МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 17-20 липня 2024 р.

Одеса
2024

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2024)

Odesa, Ukraine, July 17-20, 2024

Conference Proceedings

Odesa
2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2024)

Одеса, Україна, 17-20 липня 2024 р.

Матеріали конференції

Одеса
2024

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2024): Conference Proceedings. Odesa : Internationalhumanitarianuniversity, 2024, 180p.

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2024): Матеріали конференції. Одеса : Міжнародний гуманітарний університет, 2024, 180с.

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф ., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л. С . – д.т.н., проф ., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

СЕМЕНКО А.І. – д.т.н., проф ., Міжнародний гуманітарний університет, м.Одеса, Україна.

РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКРЕТАР

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГЛОБА Л.С. – д.т.н., проф ., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

АЛЕКСЕЄВ М.О. – д.т.н., проф., Національний технічний університет «Дніпровська політехніка», м.Дніпро, Україна.

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. –д.т.н., проф.,Міжнародний гуманітарний університет, м.Одеса, Україна.

ПРИХОДЬКО С.Б. –д.т.н., проф.,Національний університет кораблебудування ім. адмірала Макарова, м.Миколаїв, Україна.

НІКОЛЬСЬКИЙ В.В. – д.т.н., проф., Національний університет "Одеська морська академія", м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.

ЄРЕМЕНКО О.С. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

ЛЕФТЕРОВ В.О. – д.т.н., проф ., Міжнародний гуманітарний університет, м.Одеса, Україна .

МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

КЛИМАШ М.М. – д.т.н., проф., Національний університет «Львівська політехніка», м.Львів, Україна.

ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КІЛЬДЕРОВ Д.Е. – д.п.н., проф., Національний педагогічний університет імені М.П. Драгоманова

КУЧАЙ О.В., д.п.н., проф., Національний університет біоресурсів і природокористування України.

ВІТАЛЬНЕ СЛОВО ПРЕЗИДЕНТА МІЖНАРОДНОГО ГУМАНІТАРНОГО УНІВЕРСИТЕТУ СЕРГІЯ ВАСИЛЬОВИЧА КІВАЛОВА

Шановні учасники Міжнародної науково-практичної конференції «Передові технології в інформаційно-комунікаційній інженерії», вітаю Вас на святі науки, тобто на святі майбутнього, від імені всього колективу нашого університету!

Дуже складні часи переживає зараз наша Батьківщина, багато хлопців і дівчат, чоловіків і жінок, багато наших з вами колег-науковців сьогодні знаходиться в лавах Збройних сил України, дозволяючи нам працювати на перспективу, на майбутнє нашої країни, за що їм низький уклін від усіх нас.

Тема нашої конференції нерозривно пов'язана з інформаційними технологіями, які дуже щільно ввійшли в життя кожної сучасної людини. Сьогодні навіть складно уявити собі наше життя без сучасних засобів комунікації, без Інтернету, без наявності і використання різноманітних баз даних та знань тощо. Але все це має не лише позитивні наслідки, оскільки приводе до критичної актуальності питань, пов'язаних з захистом інформації, питань інформаційної безпеки. Так несанкціоновані зміни інформаційних, зокрема цифрових контентів, якщо такі не будуть вчасно виявлені, можуть привести до значимих негативних наслідків як для окремо взятої людини, банку, підприємства, так і для суспільства в цілому, в чому ми неодноразово могли переконатися останнім часом. Тому в Міжнародному гуманітарному університеті дуже велика увага приділяється питанням кібербезпеки та захисту інформації.

Для нашої країни сьогодні критично важливими є питання розвитку, вдосконалення та впровадження сучасних інформаційних технологій. Як це буде відбуватися, залежить, зокрема, і від нас з вами, особливо від нашої талановитої молоді, на яку буде покладена велика місія відбудови нашої України після Перемоги над російськими загарбниками. Може сьогодні в межах доповіді на нашій конференції з вуст того, хто ще здобуває вищу освіту, прозвучать тези, впровадження яких дозволить нам через 3-4 роки перейти на новий рівень розвитку інформаційно-комунікаційної інженерії, принаймні, мені б цього дуже хотілось.

Шановні учасники конференції, я щиро бажаю всім сили і витримки, бажаю плідної роботи, цікавих дискусій, потужних наукових результатів! Це наш з вами внесок в майбутню Перемогу! Дуже хочу, щоб через рік наступна наша конференція пройшла в мирній суверенній Україні під звуки веселих українських пісень, а не повітряної тривоги. Віримо в Перемогу! Наближаємо Перемогу! Слава Україні!

Сергій КІВАЛОВ
Президент Міжнародного гуманітарного університету, академік, доктор юридичних наук, професор, заслужений юрист України, Почесний громадянин міста Одеса

ВІТАЛЬНЕ СЛОВО РЕКТОРА МІЖНАРОДНОГО ГУМАНІТАРНОГО УНІВЕРСИТЕТУ КОСТЯНТИНА ВІКТОРОВИЧА ГРОМОВЕНКА

Щиро вітаю всіх учасників Міжнародної науково-практичної конференції «Передові технології в інформаційно-комунікаційній інженерії» в стінах Міжнародного гуманітарного університету!

Одеса в усі часи свого існування була осередком науки, залишається вона такою і сьогодні, коли Україна переживає страшні часи повномасштабної війни, розв'язаної російською федерацією. Рік тому вражі снаряди майже зруйнували одеський будинок вчених – символ науки нашого міста, з яким кожен одесит знайомиться, як тільки починає усвідомлювати себе громадянином Одеси, але вони ніколи не зможуть зруйнувати одеський характер. Навіть у таких складних умовах ми з вами продовжуємо наукову роботу, одним з доказів чого є наша конференція.

Тільки два роки в Міжнародному гуманітарному університеті працює факультет кібербезпеки, програмної інженерії та комп'ютерних наук, створення якого стало нашою відповіддю на об'єктивний виклик сучасного інформаційного суспільства, відповіддю на наявний дефіцит фахівців в галузі інформаційних технологій. Сьогодні ми вже можемо з гордістю рапортувати: наша відповідь стала гідною. На факультеті відкрито велику кількість ІТ-спеціальностей всіх трьох рівнів вищої освіти, які користуються попитом серед абітурієнтів. Міжнародний гуманітарний університет, а саме факультет кібербезпеки, програмної інженерії та комп'ютерних наук стає другим домом для все більшої кількості студентів і аспірантів. Це наш потенціал, це наш ІТ-золотий запас, одним з проявів чого є сьогоднішня наукова конференція, яка, я сподіваюся, стане зручним майданчиком для обміну результатами наукових досліджень з комп'ютерних наук, кібербезпеки, захисту інформації, програмної інженерії для фахівців не тільки України, а й зарубіжжя.

Шановні учасники конференції, щиро бажаю всім успіхів, вагомих наукових результатів! Бажаю всім витримки, нехай всі ваші рідні залишаються живими і здоровими. Віримо в наших захисників, віримо в Збройні сили України! Наближаємо нашу Перемогу! Слава Україні!

Костянтин ГРОМОВЕНКО
Ректор Міжнародного гуманітарного університету, доктор юридичних наук, професор, заслужений юрист України

ЗМІСТ

СЕКЦІЯ 4. ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

УДК 004.42

Д. Д. Плечистий, к.т.н., доцент,
О.В. Войтюк, аспірант,
Державний університет «Житомирська політехніка»

МЕТОДИ ОПТИМІЗАЦІЇ РЕКУРСИВНИХ ЦИКЛІВ В JAVASCRIPT

Метод рекурсії посідає ключову роль у вирішенні питань побудови складного користувацького інтерфейсу. При правильному налагоджені рекурсивної функції можливо досягнути бажаного результату без допомоги циклів та купи дублюючого коду. Рекурсії допомагають вирішити не тільки питання обчислень та пошуку значень, але й побудови макету додатку.

Гарним прикладом слугує вкладені списки, які мають однакову структур, стилі та правила поведінки, але різні значення та розміщення. У прикладі зі списками метод рекурсії вирішить поставлену задачу, з іншої сторони, якщо ціллю відмалювання є не прості елементи, а складні компоненти взаємодії користувача, то метод може нашкодити продуктивності додатку.

Проблема рекурсії полягає у виділенні великої частин ресурсів на обчислення, що може призвести до візуальних дефектів, таких як: заморожування процесу рендерінгу, перенавантаження стеку операцій, довга відповідь додатку на користувацькі дії.

Для вирішення проблеми методу було проаналізовано низку рішень, кожен з яких пропонує механізми покращення продуктивності за рахунок виділення пам’яті на додаткові операції.

Мемоізація

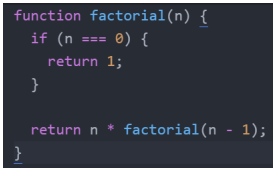
```
const memo = {};
function fibonacci(n) {
    if (n in memo) {
        return memo[n];
    }
    if (n <= 1) {
        return n;
    }
    memo[n] = fibonacci(n - 1) + fibonacci(n - 2);
    return memo[n];
}
```

(Мал. 1)

Принцип мемоізації полягає в збереженні результатів обчислень функції для уникнення повторних обчислень з тими ж вхідними даними. Це особливо корисно для рекурсивних функцій, які обчислюють однакові підзадачі багаторазово. В даному прикладі результат обчислення однієї ітерації числа Фібоначі не втрачається після обчислень, а зберігається у пам’яті, щоб при повторному виклику цієї функції спочатку перевірити наявність готового результату. Цей метод значно зменшує кількість рекурсивних викликів і покращує продуктивність за рахунок уникнення повторних обчислень.

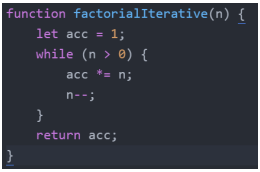
Даний метод також має свої недоліки, адже система має виділяти додаткову пам'ять, а також підтримка таких частин пам’яті може бути ускладнена великою кількістю параметрів які треба зберегти для перевірки.

Перетворення рекурсії в ітерацію



```
function factorial(n) {
  if (n === 0) {
    return 1;
  }

  return n * factorial(n - 1);
}
```

(Мал. 2)



```
function factorialIterative(n) {
    let acc = 1;
    while (n > 0) {
        acc *= n;
        n--;
    }
    return acc;
}
```

(Мал. 3)

Багато рекурсивних алгоритмів можна переписати в ітеративній формі за допомогою циклів і стеків. Це дозволяє уникнути переповнення стеку викликів і покращує використання пам'яті.

В даному прикладі рекурсія факторіала заміняється ітеративним підходом в якому обрахунки відбуваються в середині циклу. Такий підхід уникає проблему з переповненням стеку, а також є більш швидким варіантом обчислення, оскільки не потребує викликів функцій.

Паралелізація

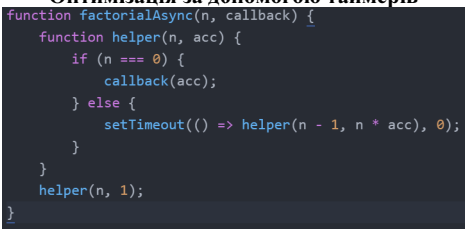
```
// Основний потік
const worker = new Worker('fibonacciWorker.js');
worker.postMessage(n);
worker.onmessage = function(event) {
    console.log(event.data); // Отримуємо результат
};

// Веб-працівник (fibonacciWorker.js)
self.onmessage = function(event) {
    const n = event.data;
    function fibonacci(n) {
        if (n <= 1) {
            return n;
        }
        return fibonacci(n - 1) + fibonacci(n - 2);
    }
    self.postMessage(fibonacci(n));
};
```

(Мал. 4)

Розділяй і володарюй - це техніка, яка дозволяє паралелізувати рекурсивні обчислення, використовуючи Web Workers для розподілу навантаження між потоками. Це особливо корисно для великих обчислень, що можуть блокувати основний потік. Основними перевагами цього методу є зниження навантаження на основний потік та можливість обробляти великі обсяги даних паралельно.

Даний метод складний у реалізації та налагодженні, адже треба додаткові витрати на передачу даних між потоками.

Оптимізація за допомогою таймерів



```
function factorialAsync(n, callback) {
    function helper(n, acc) {
        if (n === 0) {
            callback(acc);
        } else {
            setTimeout(() => helper(n - 1, n * acc), 0);
        }
    }
    helper(n, 1);
}
```

(Мал. 5)

Для довгих рекурсивних обчислень, які можуть блокувати основний потік, можна використовувати setTimeout для розбивки задачі на частини. Це дозволяє іншим завданням виконуватися між частинами обчислень, зберігаючи інтерфейс користувача чутливим. Розуміючи відмінність синхронних та асинхронних операцій можна перенаправити обчислення в стек асинхронних операцій що і видно з малюнку 5. Так як setTimeout змусить функцію перейти в стек асинхронних операцій, факторіал числа почне виконуватись на фоні, даючи можливість іншим синхронним операціям отримати пріоритет виконання.

Список використаних джерел

1. Tapas Adhikary «Synchronous vs Asynchronous JavaScript – Call Stack, Promises, and More» URL: https://www.freecodecamp.org/news/synchronous-vs-asynchronous-in-javascript/
2. Honey Sharma «Introduction to Web Workers» URL: https://medium.com/naukri-engineering/introduction-to-web-workers-3dc8c7dce0be
3. Michal Aibin, Milos Simic From «Recursive to Iterative» URL: https://www.baeldung.com/cs/convert-recursion-to-iteration
4. Germán Cocca «What is Memoization? How and When to Memoize in JavaScript» URL: https://www.freecodecamp.org/news/memoization-in-javascript-and-react/

УДК 004.91

Педяш В.В., к.т.н., доцент
Ледовський Є.В., аспірант
Думбров В.Д., студент
Міжнародний Гуманітарний Університет
vpedyash@gmail.com

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ СПАМУ В ТЕКСТОВИХ ПОВІДОМЛЕННЯХ

Анотація. *Робота присвячена аналізу сучасних методів розпізнавання спаму в текстових повідомленнях з фокусом на використання нейронних мереж. Виконано порівняння традиційних підходів до фільтрації спаму та актуальність використання методів глибокого навчання. Детально аналізуються різні архітектури нейронних мереж, включаючи рекурентні нейронні мережі (RNN, LSTM, GRU), згорткові нейронні мережі (CNN), трансформери (зокрема, BERT) та гібридні моделі. Особлива увага приділяється порівняльному аналізу цих архітектур, їх переваг та недоліків при розпізнаванні спаму.*

Розглянуто питання вибору оптимального представлення текстових даних, стратегій навчання моделей та оцінки їх ефективності.

Актуальність проблеми розпізнавання спаму в текстових повідомленнях неухильно зростає в сучасному інформаційному просторі. З розвитком цифрових комунікацій та збільшенням обсягу електронної кореспонденції, проблема небажаних та потенційно шкідливих повідомлень стає все більш гострою. Спам не лише створює незручності для користувачів, але й може нести серйозні загрози безпеці, включаючи фішинг, поширення шкідливого програмного забезпечення та крадіжку особистих даних. У зв'язку з цим, розробка ефективних методів автоматичного виявлення та фільтрації спаму є критично важливим завданням для забезпечення безпеки та комфорту користувачів цифрових платформ.

Метою даної роботи є комплексний аналіз сучасних підходів до розпізнавання спаму в текстових повідомленнях, з особливим фокусом на методи, що базуються на використанні нейронних мереж.

Задача розпізнавання спаму в текстових повідомленнях є класичним прикладом проблеми бінарної класифікації в області обробки природної мови [1]. Суть завдання полягає в автоматичному визначенні є дане повідомлення спамом чи легітимним (не спамом). Ця задача ускладнюється постійною еволюцією методів створення спаму, які стають все більш витонченими та складними для виявлення традиційними методами. Традиційні підходи до вирішення проблеми розпізнавання спаму включають використання правил на основі ключових слів, статистичних методів, таких як наївний баєсівський класифікатор, методів машинного навчання, зокрема, методу опорних векторів (SVM) та дерев рішень. Ці методи довгий час були основою систем фільтрації спаму, демонструючи достатньо високу ефективність. Однак, з ускладненням структури спаму та збільшенням обсягів даних, виникла необхідність у більш потужних та гнучких інструментах аналізу.

Нейронні мережі стали революційним проривом у вирішенні задачі розпізнавання спаму [2]. Здатність нейронних мереж автоматично визначати складні ознаки з великих обсягів даних без необхідності ручного конструювання ознак зробила їх особливо привабливими для вирішення цієї проблеми. Різні архітектури нейронних мереж, від простих багатошарових персептронів до складних рекурентних та згорткових мереж, продемонстрували високу ефективність у задачах обробки природної мови, включаючи класифікацію спаму [3].

Серед різноманітних архітектур нейронних мереж, які застосовуються для розпізнавання спаму, особливу увагу привертають рекурентні нейронні мережі (RNN), зокрема їх варіанти з довгою короткочасною пам'яттю (LSTM) та вентильним рекурентним блоком (GRU). Ці архітектури здатні ефективно обробляти послідовні дані, враховуючи зміст та семантичні зв'язки між словами в тексті, що є критично важливим для точного розпізнавання спаму [4].

Рекурентні нейронні мережі (RNN) є одними з найбільш природних архітектур для обробки послідовних даних, таких як текст. Основна ідея RNN полягає в тому, що вони мають внутрішній стан, який оновлюється при обробці кожного елемента послідовності. Це дозволяє мережі "запам'ятовувати" інформацію з попередніх кроків, що є критично важливим для розуміння змісту в текстових повідомленнях. У задачах розпізнавання спаму, RNN здатні враховувати взаємозв'язки між словами та фразами, що дозволяє їм виявляти складні паттерни, характерні для спам-повідомлень. Наприклад, RNN може навчитися розпізнавати специфічні комбінації слів або граматичні конструкції, які часто зустрічаються в спамі, навіть якщо вони розділені в тексті іншими словами. Однак, класичні RNN мають проблему зникаючого градієнта, яка обмежує їх здатність обробляти довгі послідовності. Це особливо актуально для довгих текстових повідомлень, де важлива інформація може бути розподілена на великій відстані. Для вирішення цієї

проблеми були розроблені більш складні архітектури, такі як LSTM (Long Short-Term Memory) та GRU (Gated Recurrent Unit).

LSTM є потужним варіантом рекурсивних нейромереж, який вирішує проблему зникаючого градієнта за допомогою механізму "воріт". LSTM містить спеціальні блоки пам'яті, які можуть зберігати інформацію протягом тривалого часу. Це дозволяє мережі ефективно обробляти довгі послідовності та виявляти довгострокові залежності в тексті. У задачах розпізнавання спаму, LSTM особливо ефективні для аналізу складних спам-повідомлень, які можуть містити приховані ознаки спаму, розподілені по всьому тексту. Наприклад, LSTM може навчитися розпізнавати спам, який починається з нейтрального тексту, але містить характерні ознаки спаму в кінці повідомлення.

GRU є спрощеною версією LSTM, яка також використовує механізм воріт, але має менш складну структуру. GRU зазвичай демонструє продуктивність, подібну до LSTM, але з меншою кількістю параметрів, що робить їх більш ефективними з точки зору обчислювальних ресурсів. Для задачі розпізнавання спаму, GRU може бути особливо корисними в системах реального часу, де важлива швидкість обробки повідомлень. Вони здатні ефективно виявляти ключові ознаки спаму, зберігаючи при цьому здатність аналізувати зміст повідомлення.

Згорткові нейронні мережі (CNN) спочатку були розроблені для обробки зображень, але згодом показали високу ефективність у завданнях обробки тексту, включаючи розпізнавання спаму. CNN використовують операцію згортки для виявлення локальних паттернів у вхідних даних. У завданнях аналізу тексту, CNN можуть ефективно виявляти специфічні фрази, які є характерними для спам-повідомлень. Наприклад, CNN може навчитися розпізнавати такі паттерни, як "миттєве збагачення" або "обмежена пропозиція", які часто зустрічаються в спамі.

Перевагою CNN є їх здатність автоматично вивчати ієрархічні представлення ознак. Це означає, що нижні шари мережі можуть виявляти прості паттерни (наприклад, специфічні слова або короткі фрази), тоді як вищі шари здатні розпізнавати більш складні конструкції. Однак, на відміну від RNN, CNN мають обмежену здатність враховувати довгострокові залежності в тексті. Це може бути недоліком при аналізі довгих повідомлень, де важлива інформація може бути розподілена на великій відстані.

Трансформери, зокрема модель BERT (Bidirectional Encoder Representations from Transformers), стали революційним проривом у галузі обробки природної мови. Ключовою інновацією трансформерів є механізм самоуваги, який дозволяє моделі ефективно обробляти взаємозв'язки між всіма елементами вхідної послідовності. У завданнях розпізнавання спаму, BERT та інші моделі на основі трансформерів мають кілька значних переваг. По-перше, вони здатні враховувати зміст слова з обох боків, що дозволяє більш точно інтерпретувати змістове значення слів. По-друге, попереднє навчання на величезних корпусах тексту дозволяє цим моделям мати глибоке розуміння мови, яке може бути адаптоване для конкретної задачі розпізнавання спаму. Трансформери особливо ефективні для виявлення складних форм спаму, які можуть використовувати витончені лінгвістичні конструкції або контекстно-залежні фрази. Наприклад, вони можуть краще розпізнавати спам, який намагається маскуватися під легітимне повідомлення, використовуючи тонкі нюанси мови. Однак, використання трансформерів для розпізнавання спаму має і свої проблеми. Зокрема, ці моделі зазвичай вимагають значних обчислювальних ресурсів, що може бути проблематичним для систем реального часу або для обробки великих обсягів повідомлень.

Гібридні моделі, які комбінують різні архітектури нейронних мереж, також показали високу ефективність у розпізнаванні спаму. Наприклад, комбінація CNN та LSTM дозволяє об'єднати здатність CNN виявляти локальні паттерни з можливістю LSTM обробляти довгострокові залежності. Такі гібридні моделі можуть бути особливо корисними для розпізнавання складних форм спаму, які використовують різноманітні

стратегії для обходу фільтрів. Наприклад, CNN-LSTM модель може ефективно виявляти характерні фрази спаму, одночасно враховуючи їх зміст у всьому повідомленні.

Важливим аспектом розробки систем розпізнавання спаму на основі нейронних мереж є вибір відповідної стратегії навчання. Зокрема, використання методів регуляризації, таких як дропаут (dropout) або L2-регуляризація, може значно покращити здатність моделі до узагальнення та запобігти перенавчанню. Крім того, важливо враховувати проблему незбалансованих даних, яка часто виникає в задачах розпізнавання спаму, де кількість легітимних повідомлень зазвичай значно перевищує кількість спам-повідомлень.

На основі проведеного дослідження можна зробити висновок, що застосування нейронних мереж для розпізнавання спаму в текстових повідомленнях є перспективним напрямком, який демонструє значні переваги порівняно з традиційними методами. Різні архітектури нейронних мереж, включаючи RNN, LSTM, GRU, CNN та трансформери, показують високу ефективність у вирішенні цієї задачі, кожна зі своїми унікальними перевагами. Рекурентні мережі та їх варіанти особливо ефективні для аналізу послідовної природи тексту та виявлення довгострокових залежностей, в той час як CNN здатні ефективно виявляти локальні паттерни та словесні послідовності, характерні для спаму. Трансформери, зокрема BERT, демонструють високі результати завдяки їх здатності враховувати зміст та попереднє навчання на великих фрагментах тексту. Гібридні моделі, які комбінують різні архітектури, показують потенціал для ще більш ефективного розпізнавання складних форм спаму.

Перспективними напрямками подальших досліджень є розробка методів активного та трансферного навчання, а також створення мультимодальних моделей, здатних аналізувати різні типи даних. Загалом, використання нейронних мереж відкриває нові можливості для створення більш точних, адаптивних та ефективних систем захисту від спаму, що має критичне значення для забезпечення безпеки та комфорту користувачів у сучасному цифровому просторі.

Література

1. Goldberg Y. Neural Network Methods for Natural Language Processing / Y. Goldberg. - New York City: Springer Nature, 2022. – 285 p.

2. Sabharwal M. Spam Detection in Online Social Networks Using Feed Forward Neural Network / M. Sabharwal , J. Kaur. – North Charleston: Independently Published, 2018. – 71p.

3. Conway D. Machine Learning for Email: Spam Filtering and Priority Inbox / D. Conway, J. White – Sebastopol: O'Reilly Media, Inc, 2011. – 148 p.

4. Atienza R. Advanced Deep Learning with TensorFlow 2 and Keras / R. Atienza. – Birmingham: Packt Publishing, 2020. – 513 p.

УДК 004.91

Педяш В.В., к.т.н., доцент
Петренко О.М., студент
Міжнародний Гуманітарний Університет
vpedyash@gmail.com

РОЗРОБКА РЕКОМЕНДАЦІЙНОЇ СИСТЕМИ НА ОСНОВІ ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ОНЛАЙН МАГАЗИНУ

Анотація. *У даній роботі розглядається проблема розробки та впровадження рекомендаційної системи на основі глибоких нейронних мереж для онлайн-магазину, яка використовує текстові описи товарів для надання персоналізованих рекомендацій.*

Досліджуються переваги та обмеження традиційних методів побудови рекомендаційних систем, таких як колаборативна, контентна фільтрація та обґрунтовується доцільність використання нейронних мереж для подолання цих обмежень. Описується процес розробки системи, включаючи етапи підготовки вхідних даних та їх покроковуу обробку для визначення схожості між товарами. Приділена увага до використання сучасних методів обробки природної мови для підвищення якості рекомендацій.

Використання рекомендаційних систем стало невід'ємною частиною сучасної електронної комерції. Онлайн-магазини прагнуть запропонувати своїм клієнтам персоналізований досвід покупок, що підвищує задоволеність користувачів та збільшує продажі. Актуальність використання нейронних мереж для побудови рекомендаційних систем в сучасному світі електронної комерції та цифрового контенту важко переоцінити [1, 2]. В епоху інформаційного перевантаження та величезного вибору товарів і послуг, здатність надавати персоналізовані та релевантні рекомендації стає ключовим фактором успіху для багатьох бізнесів.

Метою даної роботи є розробка та впровадження рекомендаційної системи на основі глибоких нейронних мереж для онлайн-магазину, яка використовує текстові описи товарів для надання персоналізованих рекомендацій.

Традиційні методи побудови рекомендаційних систем, такі як колаборативна фільтрація та контентна фільтрація, мають свої переваги та обмеження [3]. Колаборативна фільтрація базується на аналізі поведінки користувачів та їхніх вподобань, що дозволяє виявляти приховані закономірності та робити точні прогнози. Однак ця методика стикається з проблемою "холодного старту" для нових користувачів або товарів, а також може страждати від розрідженості даних. Контентна фільтрація, з іншого боку, фокусується на характеристиках самих товарів, що дозволяє робити рекомендації навіть для нових елементів. Проте цей метод може бути обмежений якістю та повнотою метаданих товарів, а також може призвести до надмірної спеціалізації рекомендацій, не враховуючи можливі нові інтереси користувача. Гібридні підходи, які комбінують колаборативну та контентну фільтрацію, намагаються подолати обмеження обох методів. Вони можуть забезпечити більш збалансовані та точні рекомендації, але часто вимагають складної настройки та оптимізації для досягнення оптимальних результатів.

З розвитком технологій машинного навчання, зокрема, глибоких нейронних мереж, з'явилися нові можливості для створення більш ефективних рекомендаційних систем. Глибокі нейронні мережі здатні автоматично вивчати складні нелінійні залежності з великих обсягів даних, що робить їх ідеальними для обробки різноманітної інформації, доступної в онлайн-магазинах. Вони дозволяють враховувати не тільки явні переваги користувачів, але й приховані патерни поведінки, контекстуальну інформацію та семантичні зв'язки між об'єктами. Особливу роль в цьому контексті відіграють методи обробки природної мови (NLP) та глибокого навчання, які дозволяють ефективно аналізувати текстові дані, такі як описи товарів, відгуки користувачів та контентні характеристики [4, 5]. Використання передових моделей, таких як BERT або GPT, для аналізу текстів дозволяє враховувати найтонші нюанси мови та контексту, що значно підвищує якість рекомендацій. Крім того, нейронні мережі здатні адаптуватися до змін у перевагах користувачів та тренди ринку, постійно вдосконалюючи свої прогнози на основі нових даних. Важливо також відзначити, що використання нейронних мереж дозволяє створювати гібридні рекомендаційні системи, які поєднують переваги різних підходів, таких як колаборативна фільтрація та контентно-орієнтовані методи. Це дозволяє вирішувати проблеми холодного старту, коли система стикається з новими користувачами або товарами, а також покращувати якість рекомендацій для нішевих продуктів. У контексті постійно зростаючої конкуренції за увагу користувачів, здатність надавати персоналізовані та точні рекомендації стає критичним фактором для утримання клієнтів та підвищення їх лояльності.

Побудова ефективної рекомендаційної системи на основі текстових описів товарів вимагає ретельного підходу до обробки та аналізу даних. Процес починається з підготовки текстової інформації, що включає збір описів товарів, їх очищення від непотрібних елементів та нормалізацію. Важливим етапом є лематизація або стемінг, які дозволяють привести слова до їх базової форми, що значно покращує якість подальшого аналізу. Після підготовки тексту здійснюється його векторизація, тобто перетворення слів та фраз у числові вектори. Для цього можуть використовуватися різні методи, такі як Word Embedding (наприклад, Word2Vec, GloVe або FastText).

Варто зазначити, що етап векторизації тексту є критичним для успіху всієї системи, оскільки від якості векторних представлень залежить здатність моделі виявляти семантичні зв'язки між товарами. Сучасні методи, такі як BERT, дозволяють отримувати контекстуально-залежні вектори, які враховують значення слова в конкретному контексті, що особливо важливо для аналізу складних описів товарів. Крім того, для специфічних областей може бути доцільним навчання власної моделі ембедінгів на корпусі текстів, релевантних для конкретної предметної області.

Наступним кроком є створення векторних представлень товарів на основі їх текстових описів. Це може бути здійснено шляхом простого усереднення векторів слів, що входять до опису, або більш складними методами, такими як зважене усереднення з використанням ваг TF-IDF чи застосування згорткових нейронних мереж. На основі отриманих векторних представлень будується модель, здатна визначати схожість між товарами. Ця модель може бути реалізована у вигляді багатошарового перцептрона, LSTM-мережі або використовувати архітектуру Transformer. Ключовим моментом є вибір відповідної функції втрат, яка дозволить ефективно навчити модель розрізняти схожі та несхожі товари. Після навчання моделі можна переходити до етапу визначення схожості між товарами, що зазвичай здійснюється за допомогою обчислення косинусної подібності або евклідової відстані між їх векторними представленнями.

При побудові моделі важливо враховувати не тільки текстові характеристики товарів, але й інші фактори, такі як категорії товарів, цінові діапазони, популярність серед користувачів тощо. Це дозволяє створити більш комплексну модель, яка здатна враховувати різноманітні аспекти при генерації рекомендацій. Крім того, використання методів ансамблювання, коли кілька моделей об'єднуються для отримання фінального прогнозу, може значно підвищити якість рекомендацій. Важливим аспектом є також постійна оптимізація та оновлення моделі на основі нових даних та відгуків користувачів, що дозволяє системі адаптуватися до змінних уподобань та тренди ринку.

Фінальним етапом є генерація рекомендацій на основі визначеної схожості товарів. Це може бути реалізовано шляхом пошуку найближчих сусідів у векторному просторі або застосуванням методів кластеризації для групування схожих товарів. Важливо також врахувати аспекти персоналізації, використовуючи історію взаємодій користувача для уточнення рекомендацій та забезпечити різноманітність пропозицій, уникаючи надмірної схожості рекомендованих товарів. Такий підхід дозволяє створити ефективну рекомендаційну систему, яка здатна аналізувати текстові описи товарів та надавати релевантні пропозиції користувачам, підвищуючи їх задоволеність та збільшуючи конверсію.

Важливо забезпечити прозорість роботи системи, надаючи користувачам можливість розуміти, чому їм рекомендуються ті чи інші товари, та контролювати процес персоналізації. Це не тільки підвищує довіру користувачів до системи, але й дозволяє отримувати цінний зворотний зв'язок для подальшого вдосконалення алгоритмів рекомендацій.

На основі проведеного дослідження можна зробити висновок, що використання глибоких нейронних мереж для побудови рекомендаційних систем на основі текстових описів товарів є перспективним напрямком у сфері електронної комерції. Ця технологія дозволяє подолати обмеження традиційних методів, таких як колаборативна та контентна

фільтрація, шляхом ефективної обробки великих обсягів даних та виявлення складних нелінійних залежностей. Ключовими етапами розробки такої системи є ретельна підготовка текстових даних, включаючи очищення та нормалізацію, вибір оптимального методу векторизації тексту, створення векторних представлень товарів, та побудова моделі для визначення схожості між товарами. Використання сучасних методів обробки природної мови, таких як BERT, дозволяє враховувати контекст та семантичні зв'язки в описах товарів, що значно підвищує якість рекомендацій. Важливими аспектами є також врахування додаткових факторів, таких як категорії товарів та цінові діапазони, використання методів ансамблювання для підвищення точності прогнозів, та забезпечення персоналізації та різноманітності рекомендацій. Впровадження такої системи дозволяє онлайн-магазинам підвищити задоволеність користувачів, збільшити продажі та зміцнити конкурентні позиції на ринку, при цьому важливо забезпечити прозорість роботи системи та можливість користувацького контролю для підвищення довіри та отримання цінного зворотного зв'язку.

Перспективи подальших досліджень включають інтеграцію більш просунутих технік обробки природної мови для покращення розуміння семантики товарних описів, розробку методів для ще більш ефективної обробки мультимодальних даних, та дослідження можливостей використання квантових обчислень для оптимізації певних аспектів системи. Крім того, важливим напрямком є подальше вдосконалення методів забезпечення приватності та етичності рекомендацій, а також розробка більш просунутих технік для пояснення роботи системи користувачам та бізнес-аналітикам.

Література

1. Бодянський Є. В. Аналіз та обробка потоків даних засобами обчислювального інтелекту: Монографія / Є. В. Бодянський, Д. Д. Пелешко, О. А. Винокурова, С. В.Машталір, Ю. С. Іванов. Львів : Видавництво Львівської політехніки, 2016. - 236 с.

2. Ricci F. Recommender systems handbook [3rd ed.] / F. Ricci, L. Rokach, B. Shapira. NY: Springer Science+Business Media, LLC, 2022. 1048 p.

3. Falk K. Practical Recommender Systems 1st Edition / K. Falk. NY: Manning Publications, 2019. – 432 p.

4. Jin H. Automated Machine Learning in Action / H. Jin , X. Hu. – Shelter: Manning Publications, 2022. – 338 p.

5. Atienza R. Advanced Deep Learning with TensorFlow 2 and Keras / R. Atienza. – Birmingham: Packt Publishing, 2020. – 513 p.

УДК 004.93

Педяш В.В., к.т.н., доцент
Ткач В.М., аспірант
Терновський О.Ю., студент
Міжнародний Гуманітарний Університет
vpedyash@gmail.com

ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУР ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ РОЗПІЗНАВАННЯ МЕДИЧНИХ ЗОБРАЖЕНЬ

Анотація. *Робота присвячена дослідженню трьох розповсюджених архітектур згорткових нейронних мереж (ResNet, DenseNet та VGG) при їх застосуванні для розпізнавання медичних зображень. Особлива увага приділяється аналізу ефективності цих мереж у різних медичних застосуваннях. Проводиться порівняльний аналіз архітектур за такими критеріями як кількість параметрів, обчислювальні вимоги,*

точність класифікації, а також розмір моделі. На основі проведеного аналізу надано рекомендації щодо вибору оптимальної архітектури для різних задач медичної діагностики.

Медична діагностика є однією з найважливіших галузей застосування штучного інтелекту та комп'ютерного зору. Точне та швидке розпізнавання патологій на медичних зображеннях може значно покращити якість діагностики та лікування пацієнтів. В останні роки глибокі нейронні мережі продемонстрували вражаючі результати в задачах комп'ютерного зору, зокрема в аналізі медичних зображень [1-3].

Метою даної роботи є порівняльна характеристика трьох популярних архітектур згорткових нейронних мереж ResNet, DenseNet та VGG для задачі аналізу медичних зображень на наявність патологій.

Особливістю даного напряму є те, що на прикладі конкретних медичних застосувань слід розглянути особливості кожної архітектури, переваги та недоліки, а також проаналізувати їх ефективність. При розпізнаванні медичних зображень також слід врахувати варіативність патологій, низьку якість деяких зображень та необхідність враховувати тонкі деталі. Тому вибір оптимальної архітектури нейронної мережі є критично важливим для досягнення високої точності діагностики.

Перша з досліджених архітектур ResNet (Residual Network) була запропонована в 2015 році дослідниками з Microsoft Research і швидко стала однією з найпопулярніших архітектур для задач комп'ютерного зору. Ключовою особливістю ResNet є використання так званих "залишкових блоків" (residual blocks). Ці блоки дозволяють ефективно навчати дуже глибокі нейронні мережі, вирішуючи проблему затухання градієнтів. У залишковому блоці вхідні дані передаються через кілька згорткових шарів, а потім додаються до початкового входу. Це створює "короткі шляхи" для градієнтів, що дозволяє ефективно навчати сотні шарів. ResNet може мати глибину від 18 до 152 шарів і навіть більше. Найпопулярнішими варіантами є ResNet-50 та ResNet-101. Для медичних застосувань ResNet показала високу ефективність у багатьох задачах, включаючи класифікацію рентгенівських знімків грудної клітки, виявлення пухлин на МРТ-зображеннях мозку та аналіз гістологічних зрізів. Перевагами ResNet є висока точність класифікації, здатність вивчати складні ознаки та можливість навчання дуже глибоких мереж. Недоліками можна вважати велику кількість параметрів та відносно високі обчислювальні вимоги.

Наступною архітектурою, котру також слід розглянути, є DenseNet (Dense Convolutional Network). Вона була представлена в 2017 році і запропонувала новий підхід до побудови глибоких згорткових мереж. Головна ідея DenseNet полягає в тому, що кожен шар отримує на вхід виходи всіх попередніх шарів. Це створює дуже щільну структуру зв'язків між шарами, звідки й походить назва архітектури. Така щільна структура зв'язків дозволяє ефективно повторно використовувати ознаки, вивчені на різних рівнях мережі. Це призводить до більш компактних моделей з меншою кількістю параметрів порівняно з ResNet. DenseNet також вирішує проблему загасання градієнтів, але робить це іншим способом, ніж ResNet. Завдяки прямим зв'язкам між усіма шарами, градієнти можуть легко поширюватися через всю мережу. У медичних застосуваннях DenseNet показала високу ефективність для сегментації органів на КТ-зображеннях, класифікації шкірних уражень та аналізу мамографічних знімків. Перевагами DenseNet є висока точність при меншій кількості параметрів, ефективне використання ознак та хороша узагальнююча здатність. Недоліками можна вважати складність реалізації та високі вимоги до пам'яті під час навчання.

Третьою архітектурою, яку було взято до уваги, є VGG (Visual Geometry Group). VGG була розроблена в Оксфордському університеті в 2014 році і стала однією з перших успішних глибоких згорткових мереж. VGG має простішу архітектуру порівняно з ResNet та DenseNet. Вона складається з послідовності згорткових шарів з фільтрами 3x3, за якими слідують шари максимального об'єднання та повнозв'язні шари на кінці мережі.

Ключовою особливістю VGG є використання дуже малих згорткових фільтрів (3x3) у всіх шарах. Це дозволяє збільшити глибину мережі при збереженні невеликої кількості параметрів. Найпопулярнішими варіантами VGG є VGG-16 та VGG-19, які мають відповідно 16 та 19 шарів з вагами. Незважаючи на свою відносну простоту, ці мережі показують високу точність у багатьох задачах комп'ютерного зору. У медичних застосуваннях VGG успішно використовувалася для класифікації рентгенівських знімків, виявлення діабетичної ретинопатії на знімках очного дна та аналізу ультразвукових зображень. Перевагами VGG є простота архітектури, хороша інтерпретованість вивчених ознак та висока точність на багатьох наборах даних. Недоліками є велика кількість параметрів та високі обчислювальні вимоги порівняно з більш сучасними архітектурами.

В таблиці 1 наведено порівняння трьох вищезгаданих архітектур нейронних мереж [4, 5]. Аналізуючи ключові параметри, можна помітити суттєві відмінності між цими архітектурами.

Таблиця 1 – Порівняльна характеристика архітектур нейронних мереж типу ResNet, DenseNet та VGG

Характеристика	ResNet	DenseNet	VGG
Глибина мережі	Від 18 до 152+ шарів	Змінна, зазвичай 121-201 шар	16 або 19 шарів
Кількість параметрів	Середня	Низька	Висока
Швидкість навчання	Середня	Висока	Низька
Точність класифікації	Дуже висока	Висока	Висока
Ключова особливість	Залишкові блоки	Щільні зв'язки між шарами	Малі згорткові фільтри (3x3)
Обчислювальні вимоги	Високі	Середні	Високі
Інтерпретованість	Середня	Середня	Висока
Вимоги до пам'яті	Середні	Високі	Середні
Рік розробки	2015	2017	2014
Типові медичні застосування	Класифікація рентгенівських знімків, виявлення пухлин на МРТ	Сегментація органів на КТ, аналіз мамографії	Класифікація рентгенівських знімків, аналіз УЗД

Дані з таблиці показують, що ResNet вирізняється надзвичайно високою точністю класифікації та здатністю будувати дуже глибокі мережі, але це досягається за рахунок високих обчислювальних вимог. Вона демонструє найкращий баланс між ефективністю та продуктивністю, маючи низьку кількість параметрів, високу швидкість навчання та інференсу при збереженні високої точності. VGG, хоч і має найбільшу кількість параметрів та найнижчу швидкість навчання, відзначається високою інтерпретованістю результатів та відмінною придатністю для трансферного навчання. Щодо вимог до пам'яті, DenseNet виявляється найбільш вимогливою, тоді як ResNet та VGG мають середні показники. Варто зазначити, що всі три архітектури показують високу ефективність у різних медичних застосуваннях, але кожна має свої переваги: ResNet часто обирають для задач, що вимагають найвищої точності, DenseNet - для ефективного використання обчислювальних ресурсів, а VGG - коли важлива інтерпретованість результатів. Ця порівняння демонструє, що вибір оптимальної архітектури для задач медичної візуалізації залежить від багатьох факторів і вимагає ретельного аналізу вимог конкретного проекту та доступних ресурсів, враховуючи такі параметри як точність, швидкість роботи, вимоги до пам'яті та обчислювальних ресурсів.

На основі проведеного порівняльного аналізу архітектур ResNet, DenseNet та VGG для розпізнавання медичних зображень можна зробити наступні висновки. Всі три архітектури демонструють високу ефективність у різноманітних задачах медичної візуалізації, проте мають свої особливості та сфери оптимального застосування. ResNet

вирізняється високою точністю класифікації та здатністю до навчання надглибоких мереж, що робить її відмінним вибором для складних діагностичних задач, де критично важлива максимальна точність. DenseNet пропонує найкращий баланс між точністю та обчислювальною ефективністю, що робить її привабливою для широкого спектру практичних застосувань, особливо в умовах обмежених ресурсів. VGG, незважаючи на більшу кількість параметрів, залишається цінною завдяки високій інтерпретованості результатів та відмінній придатності до трансферного навчання. Вибір оптимальної архітектури для конкретного медичного застосування повинен базуватися на ретельному аналізі специфіки задачі, вимог до точності, швидкодії та доступних обчислювальних ресурсів.

Перспективними напрямками подальших досліджень є адаптація цих архітектур під специфіку медичних даних, розробка гібридних моделей, що поєднують сильні сторони різних архітектур, а також покращення інтерпретованості та пояснюваності результатів, що критично важливо для впровадження систем штучного інтелекту в клінічну практику.

Література

1. Навчальний посібник з дисципліни Системи візуалізації та розпізнавання образів / [Смолій В.В., Савицька Я.А., Місюра М.Д., Шкарупило В.В.]. - К.: ФОП Ямчинський О.В., 2020.- 200 с.
2. Вовк С.М. Методи обробки зображень та комп'ютерний зір. Навчальний посібник / С.М. Вовк, В.В. Гнатушенко, М.В. Бондаренко – Д.:«ЛІРА», 2016. – 148 с.
3. Бодянський Є. В. Аналіз та обробка потоків даних засобами обчислювального інтелекту: Монографія / Є. В. Бодянський, Д.Д. Пелешко, О.А. Винокурова, С.В. Машталір, Ю. С. Іванов. - Львів : Видавництво Львівської політехніки, 2016. - 236 с.
4. Jin H. Automated Machine Learning in Action / H. Jin , X. Hu. – Shelter: Manning Publications, 2022. – 338 p.
5. Atienza R. Advanced Deep Learning with TensorFlow 2 and Keras / R. Atienza. – Birmingham: Packt Publishing, 2020. – 513 p.

Стрелковська І.В., д.т.н., професор, Левченко А.С, магістр 1 курсу навчання зі спеціальності 121 Інженерія програмного забезпечення
Міжнародний гуманітарний університет
i.strelkovskaya@mgu.edu.ua,

МОДЕЛЮВАННЯ ТРАФІКУ З ВИКОРИСТАННЯМ ПАКЕТУ MATLAB СЕРЕДОВИЩА SIMULINK

Анотація. *Розглянуто програмні засоби моделювання самоподібного трафіку. Визначено основні вимоги до моделювання самоподібного трафіку на базі систем масового обслуговування. Запропоновано використання розподілу Вейбула для опису вхідного потоку вимог на обслуговування. Встановлено, що доцільним для моделювання трафіку є використання програмного пакету MATLAB середовища SIMULINK. Розроблено програмну реалізацію для моделювання самоподібного трафіку в середовищі SIMULINK.*

Програмна реалізація задач моделювання трафіку сьогодні займає важливе місце серед досліджень, незважаючи на велику кількість реалізованих засобів моделювання та аналізу трафіку, серед яких можна відмітити WireShark, NS-2 та NS-3, QualNet, GPSS, OPNET, OMNET++, NetSim [1] та багато інших. Завданням таких програмних реалізацій є моделювання трафіку із заданими характеристиками та умовами його обслуговування з врахуванням встановленого закону розподілу та характеристик трафіку (інтенсивностей,

пропускних спроможностей, часу затримки та джитеру), що дозволяє встановити певні залежності між обсягом трафіку, що надходить на обслуговування в мережу, і параметрами мережі, що забезпечують ефективне використання доступних ресурсів. Використання існуючих програмних реалізацій моделювання трафіку має значні обмеження для дослідження трафіку, адже можливості моделювання часто обмежені вибором моделі трафіку, або ж спрямовані на якийсь певний різновид трафіку. Тому в роботі розглядається можливість використання імітаційного моделювання з використанням програмного пакету MATLAB на базі середовища SIMULINK для моделювання самоподібного трафіку. Важливою перевагою середовища SIMULINK є використання блоків SimEvents blockset для створення джерел потоку вимог на обслуговування з різними законами розподілу, формування черг (в тому числі пріоритетних) та дисциплін обслуговування, створення серверів та багато іншого. При цьому пакет SIMULINK дозволяє використовувати будь-які бібліотеки програмного пакету MATLAB для моделювання трафіку, а також додавати блоки, розроблені безпосередньо користувачем [1].

Сучасні дослідження трафіку комп'ютерних мереж використовують модель самоподібного трафіку, яка характеризується особливою структурою, що зберігається при багаторазовому масштабуванні та має довгострокову залежність між моментами надходження вимог на обслуговування, що визначається функцією кореляції в різні моменти часу. Потік самоподібного трафіку має післядію, бо кількість вимог на обслуговування до систбеми масового обслуговування (СМО) після часу t, залежить від кількості вимог, що надійшли до моменту часу t. Для самоподібного трафіку характерні часті «сплески» пакетів за відносно невеликого середнього рівня значень трафіку. Це значно погіршує характеристики обслуговування самоподібного трафіку, збільшуючи втрати пакетів, час затримки та джиттер пакетів. Як кількісну оцінку ступеня самоподібності трафіку визначено параметр Херста H, який має значення $0,5 < H < 1$ [1-7]. Тому важливим завданням є моделювання самоподібного трафіку, яке дозволить відтворити особливості його структури та характеристик.

Для моделювання самоподібного трафіку використано систему масового обслуговування (СМО), для якої необхідно враховувати: закон розподілу, для опису надходження проміжків між вимогами на обслуговування, що найбільш підходить для самоподібного трафіку. Частіше це закон Вейбуллу або закон Парето; закон розподілу, для опису часу обслуговування вимог в СМО; кількість серверів в СМО; довжину черги вимог на обслуговування в СМО.

Метою даної роботи є моделювання самоподібного трафіку з використанням програмного пакету MATLAB на базі середовища SIMULINK.

Розглянемо розв'язання задачі моделювання самоподібного трафіку для системи масового обслуговування виду $W_B/M/1/K$, де W_B– закон Вейбула, який описує проміжки між вимогами на обслуговування, M – експоненційний закон, який описує час обслуговування вимог в СМО, система має один сервер (однолінійна), K – довжина черги вимог.

Для моделювання СМО вважається, що [1-2]:

– потік вимог генерується за допомогою генератора вхідного потоку за розподілом Вейбула з інтенсивністю потоку λ:

$$f(x)=\begin{cases}\alpha\beta x^{\alpha-1}e^{-\beta x^{\alpha}}, & x\geq 0\\ 0, & x\leq 0\end{cases}, \qquad (1)$$

де α – параметр форми кривої розподілу Вейбулла, $0<\alpha<1$, який визначається виразом $\alpha = 2 - 2H$, де H – параметр Херста, $\beta = \left[\lambda\Gamma\left(1+\frac{1}{\alpha}\right)\right]^{\alpha}$ – параметр розподілу Вейбулла, $\beta>0$, Г – гамма-функція Ейлера виду $\Gamma(k) = \int_0^{+\infty} t^{k-1}e^{-1}dt$, λ– інтенсивність надходження вимог на обслуговування до СМО $W_B/M/1/K$;

– вимоги формують чергу, яка функціонує за принципом FIFO «перший прийшов, перший вийшов», черга дорівнює K;

– дисципліна обслуговування СМО з втратами, тобто вимога, яка не була обслуговувана, втрачається;

– сервер обслуговує вимоги та формує потік вимог, які отримали обслуговування з інтенсивністю обслуговування μ.

Блок-схему моделювання трафіку для СМО $W_B/M/1/K$ показано на рис. 1.

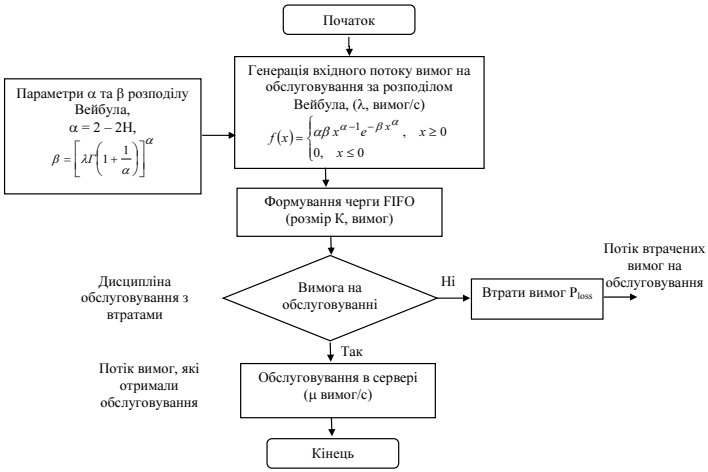


Рисунок 1 – Блок-схема моделювання трафіку для СМО $W_B/M/1/K$

Для розробки імітаційної моделі самоподібного трафіку використуємо середовище SIMULINK у програмному пакеті MATLAB [1]. Для моделювання СМО $W_B/M/1/K$ доцільно використати SimEvents blockset [1]. На першому етапі необхідно створити зовнішній генератор випадкових чисел, адже, зазвичай, можливо використовувати вже наявні генератори випадкових подій, що використовують розподіл Вейбулла, але в цьому випадку при моделюванні буде неможливо задати і надалі варіювати параметри розподілу Вейбулла. Наприклад, параметр форми кривої розподілу α та параметр Херста. Тому при моделюванні доцільно розробити генератор Generator Weibull Distribution, який генеруватиме джерела вимог на обслуговування із заданими параметрами форми кривої розподілу α і параметра розподілу Вейбулла β.

Для моделювання самоподібного трафіку використовується одне джерело, яке генерує вимоги на обслуговування за допомогою розробленого Generator Weibull Distribution, що дозволяє генерувати послідовність випадкових цифр із заданими значеннями параметрів розподілу Вейбула та інтенсивністю (λ =200 пак/с) надходження

заявок на обслуговування. Розглянемо для розподілу Вейбулла заданий параметр Херста H=0,8 і параметри α и β, відповідно, α = 0,7 і β =13,46.

Усі вимоги обслуговуються системою розподілу інформації Output Switch, час обслуговування складає μ = 120 і розподілено за допомогою експонентного закону в Single Server, який моделює генератор випадкових чисел. З урахуванням того, що СМО має чергу, заявки буферизуються у FIFO Queue з довжиною черги K = 1000 вимог та обслуговуються з дисципліною обслуговування із втратами та порядком обслуговування FIFO – «перший прийшов – перший вийшов».

На рис. 2 показано вікно для СМО виду $W_B/M/1/K$, розроблене в середовиці SIMULINK з використанням SimEvents blockset у програмному пакеті MATLAB [1].

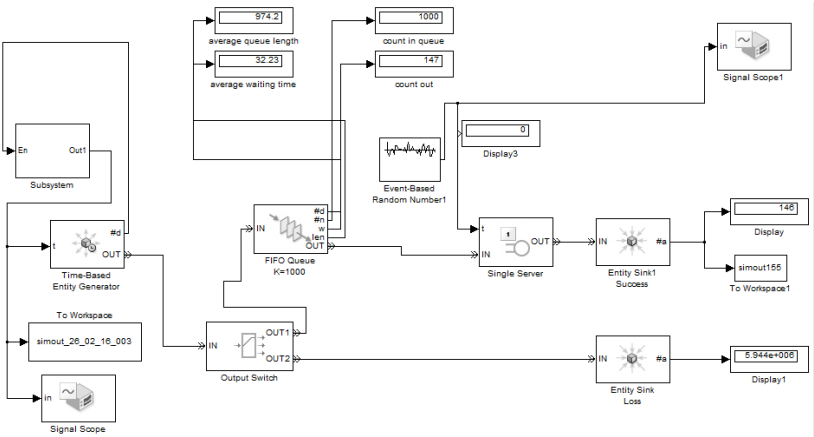


Рисунок 2 – Моделювання СМО $W_B/M/1/K$ в середовиці SIMULINK програмного пакету MATLAB

При успішному обслуговуванні вимоги підраховуються в Entity Sink Success, а при втратах, що виникають у разі переповнення буферного пристрою в Entity Sink Loss вимоги, які потрапили в Entity Sink Loss, вважаються втраченими і на обслуговування більше не надходять.

Для представлення результатів моделювання трафіку у програмі використовуються різні вікна, які показують результати для СМО виду $W_B/M/1/K$ у реальному масштабі часу. Це значення середнього часу обслуговування у вікні Average waiting time, середня довжина черги заявок у вікні Average queue length, задана довжина черги заявок у вікні Count in queue та кількість заявок із черги, які втрачені у вікні Coutnt out.

Результати моделювання трафіку для СМО виду $W_B/M/1/K$ показані на рис. 3.

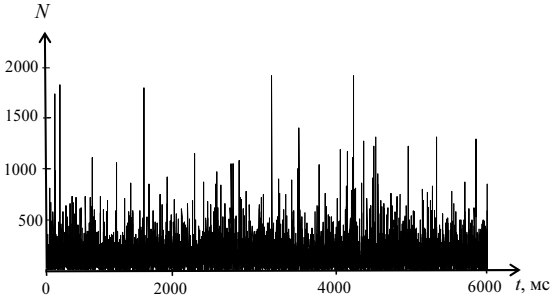


Рисунок 3 – Результати моделювання трафіку СМО виду $W_B/M/1/K$ в середовищі SIMULINK програмного пакету MATLAB

Висновки

1. Проведено моделювання самоподібного трафіку для СМО виду $W_B/M/1/K$ (W - потік запитів, які надходять, розподілених за законом Вейбула, M - час обслуговування запитів, який розподілено за експоненційним законом, система - однолінійна, довжина черги запитів - K). Вихідними даними для моделювання є значення параметра Херста H=0,6, H=0,8, H=0,9 і параметр форми кривої розподілу α = 0,7 та параметр розподілу β =13,46.

2. За допомогою програмного пакета SIMULINK у середовищі MATLAB розроблено імітаційну модель для дослідження характеристик самоподібного трафіку.

Література

1. MachWorks https://www.mathworks.com/

2. Strelkovskaya I.V. Modeling of self-similar traffic / I.V. Strelkovskaya, I.N. Solovskaya, N.V. Severin // Proceedings of the 4rd International Conference on Applied Innovations in IT (ICAIIT-2016), Vol. 1, Is. 5, Koethen, Germany, March, 10, 2016.– P. 61-64.

3. Strelkovskaya I.V. Self-similar traffic in G/M/1 queue defined by the Weibull distribution/ I.V. Strelkovskaya, T.I. Grygoryeva, I.N. Solovskaya // Radioelectronics and Communications Systems. – 2018. – V. 61, № 3 (2018). – P. 173-180.

4. Grab, E. Real-time Estimation of Traffic Self-similarity Parameter in Simulink with Wavelet Transform / E. Grab, S. Sharkovsky // Elektronika ir elektrotechnika. – 2013. – Vol. 19. – P. 88-91.

5. Rikli, N.-E. Self-similarity and stationarity of increments in VBR video / N.-E. Rikli // Journal of king saud university – Computer and information sciences. – 2019. – № 24. – P. 7-16.

6. Tomic, I., Maletic, N. Comparison of models for self-similar network traffic generation / I. Tomic, N. Maletic // X International symposium on industrtial electronics. – 2021. – P. 266-269.

7. Millan, G. A fast multifractal model for self-similar traffic flows in high-speed computer networks / G. Millan, G. Lefranc // Procedia computer science. – 2013. – Vol. 17. – P. 420-425.

СЕКЦІЯ 2. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

УДК 004.725.5

Григор'єва Т.І., кандидат технічних наук, доцент,
Міжнародний гуманітарний університет, місто Одеса
tig15090808@gmail.com
Проценко М.М.
Міжнародний гуманітарний університет, місто Одеса
protsenko.mike@gmail.com

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ ПРОЕКТУВАННЯ ВЕБ-ДОДАТКІВ З ВИКОРИСТАННЯМ TENSORFLOW.JS

Анотація. *В роботі розглядаються можливості використання бібліотеки TensorFlow.js для автоматизації процесів проектування веб-додатків. Проаналізовано ключові переваги та особливості застосування моделей машинного навчання для вирішення задач автоматизації проектування користувацьких інтерфейсів, тестування та оптимізації продуктивності веб-додатків. Запропоновано напрямки подальших досліджень в області автоматизації процесів проектування веб-додатків з використанням технологій машинного навчання.*

В сучасному світі веб-додатки відіграють все більшу роль у різних сферах життя, від бізнесу до освіти та розваг [1]. Зі зростанням складності та функціональності веб-додатків, процес їх проектування та розробки стає все більш трудомістким та часозатратним. Автоматизація процесів проектування веб-додатків дозволяє скоротити час та ресурси, необхідні для створення якісного програмного забезпечення. Одним з перспективних інструментів для вирішення цієї задачі є бібліотека TensorFlow.js [2], яка дозволяє інтегрувати моделі машинного навчання безпосередньо у веб-додатки. TensorFlow.js – це бібліотека з відкритим кодом, розроблена компанією Google, яка надає можливість виконувати машинне навчання та глибоке навчання у веб-браузері без необхідності встановлення додаткового програмного забезпечення. Вона базується на популярній бібліотеці TensorFlow, яка широко використовується для створення моделей машинного навчання на серверній стороні.

Ключовими перевагами TensorFlow.js є:

1. Можливість виконання моделей машинного навчання безпосередньо на пристрої користувача, що забезпечує конфіденційність даних та зменшує навантаження на сервер.
2. Висока швидкість роботи завдяки використанню можливостей апаратного прискорення веб-браузерів, таких як WebGL.
3. Зручність інтеграції з існуючими веб-додатками та фреймворками, такими як React, Angular, Vue.js тощо.
4. Можливість імпорту моделей, навчених з використанням інших бібліотек, таких як Keras або TensorFlow Python.

Одним з ключових етапів проектування веб-додатків є створення користувацького інтерфейсу (UI). Традиційно цей процес виконується вручну, що потребує значних затрат часу та зусиль дизайнерів та розробників. Використання TensorFlow.js дозволяє автоматизувати деякі аспекти проектування UI за допомогою генеративних моделей.

Генеративні моделі, такі як Variational Autoencoder (VAE) та Generative Adversarial Network (GAN), можуть бути навчені на існуючих прикладах UI і потім використані для генерації нових дизайнів [3]. Це дозволяє автоматизувати процес створення прототипів UI, зменшуючи час та зусилля, необхідні для їх розробки. Крім того, TensorFlow.js надає можливості для створення адаптивних користувацьких інтерфейсів, які автоматично

налаштовуються під потреби та вподобання конкретного користувача. Використовуючи моделі машинного навчання, такі інтерфейси можуть аналізувати поведінку користувача та динамічно змінювати розташування елементів, розмір шрифту, кольорову схему тощо, забезпечуючи оптимальний досвід взаємодії [4].

Тестування є невід'ємною частиною процесу розробки веб-додатків, яка забезпечує якість та надійність кінцевого продукту. Однак, ручне тестування може бути трудомістким та схильним до помилок. Використання TensorFlow.js дозволяє автоматизувати деякі аспекти тестування веб-додатків за допомогою моделей машинного навчання. Наприклад, моделі класифікації можуть бути використані для автоматичного виявлення візуальних дефектів у користувацькому інтерфейсі, таких як неправильне вирівнювання елементів, невідповідність кольорів тощо [5]. Це дозволяє швидко ідентифікувати потенційні проблеми та зменшити час, необхідний для їх виправлення. Інший підхід полягає у використанні моделей машинного навчання для генерації тестових сценаріїв на основі аналізу поведінки користувачів [6]. Такі моделі можуть автоматично генерувати набори вхідних даних та послідовності дій, які імітують реальну взаємодію користувачів з додатком, дозволяючи виявити потенційні проблеми та оптимізувати продуктивність.

Продуктивність є критичним фактором успіху веб-додатків, оскільки користувачі очікують швидкої та плавної взаємодії. TensorFlow.js надає можливості для оптимізації продуктивності веб-додатків за допомогою моделей машинного навчання. Наприклад, моделі прогнозування можуть бути використані для передбачення майбутніх дій користувача на основі його попередньої поведінки [7]. Це дозволяє завчасно завантажувати необхідні ресурси та мінімізувати час відгуку додатку. Інший підхід полягає у використанні моделей машинного навчання для автоматичної оптимізації коду веб-додатків. Такі моделі можуть аналізувати структуру та логіку програми, ідентифікувати потенційні вузькі місця та генерувати оптимізований код, що веде до підвищення продуктивності. Використання TensorFlow.js для автоматизації процесів проектування веб-додатків відкриває нові можливості для розробників. Завдяки інтеграції моделей машинного навчання безпосередньо у веб-додатки, TensorFlow.js дозволяє автоматизувати різні аспекти процесу розробки, від проектування користувацьких інтерфейсів до тестування та оптимізації продуктивності.

Таким чином, автоматизація процесів проектування веб-додатків дозволяє скоротити час та ресурси, необхідні для створення якісного програмного забезпечення, а також підвищити якість кінцевого продукту. Крім того, використання моделей машинного навчання відкриває нові можливості для персоналізації та адаптації веб-додатків під потреби конкретних користувачів. Подальші дослідження в цій області можуть бути спрямовані на розробку нових методів автоматизації проектування веб-додатків, вдосконалення існуючих моделей машинного навчання для вирішення специфічних задач, а також створення нових інструментів та фреймворків для спрощення інтеграції моделей машинного навчання у веб-додатки.

Висновки

1. TensorFlow.js відкриває нові можливості для автоматизації процесів проектування веб-додатків, дозволяючи інтегрувати моделі машинного навчання безпосередньо у веб-браузер.

2. Автоматизація проектування користувацьких інтерфейсів з використанням генеративних моделей та адаптивних підходів дозволяє скоротити час та ресурси на розробку, підвищити задоволеність користувачів та збільшити конверсію.

3. Застосування моделей машинного навчання для автоматизації тестування веб-додатків, включаючи виявлення дефектів UI та генерацію тестових сценаріїв на основі поведінки користувачів, підвищує ефективність та якість процесу тестування.

4. Оптимізація продуктивності веб-додатків за допомогою моделей прогнозування та автоматичної оптимізації коду дозволяє покращити користувацький досвід, зменшити час завантаження сторінок та підвищити конверсію.

5. Успішні приклади використання TensorFlow.js для автоматизації різних аспектів проектування веб-додатків демонструють значні переваги, такі як скорочення часу розробки, підвищення якості кінцевого продукту та збільшення задоволеності користувачів.

6. Подальший розвиток та вдосконалення технологій машинного навчання, зокрема TensorFlow.js, відкриває широкі перспективи для автоматизації процесів проектування веб-додатків та створення більш ефективних, персоналізованих та зручних для користувачів рішень.

Література

1. Gulli A., Kapoor A., Pal S. Deep Learning with TensorFlow and Keras: Regression, ConvNets, GANs, RNNs, NLP, and more with TensorFlow 2 and the Keras API, 2nd Edition / A. Gulli, A. Kapoor, S. Pal. — Packt Publishing, 2019. — 646 с.

2. Koul A., Ganju S., Kasam M. Practical Deep Learning for Cloud, Mobile, and Edge: Real-World AI & Computer-Vision Projects Using Python, Keras & TensorFlow / A. Koul, S. Ganju, M. Kasam. — O'Reilly Media, 2019. — 500 с.

3. Foster D. Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play / D. Foster. — O'Reilly Media, 2019. — 300 с.

4. Goyal A., Bengio Y., Deng L. Self-Supervised Learning: The Next Frontier in AI / A. Goyal, Y. Bengio, L. Deng. — MIT Press, 2023. — 220 с.

5. Hutter F., Kotthoff L., Vanschoren J. Automated Machine Learning: Methods, Systems, Challenges, Second Edition / F. Hutter, L. Kotthoff, J. Vanschoren. — Springer, 2022. — 350 с.

6. Sato K., Fujimaki R. Robust Optimization for Machine Learning: From Theory to Practice / K. Sato, R. Fujimaki. — Springer, 2021. — 253 с.

7. Zheng A., Casari A. Evaluating Machine Learning Models: A Beginner's Guide to Key Concepts and Pitfalls / A. Zheng, A. Casari. — O'Reilly Media, 2018. — 226 с.

УДК 608.4

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Черкас Ніката Сергійович
здобувач 1 курсу першого (бакалаврського) рівня
спеціальності 172 – Електронні комунікації та радіотехніка
Міжнародний гуманітарний університет
nikitacerkas12@gmail.com

Панков Іван Олексійович
здобувач 1 курсу першого (бакалаврського) рівня
спеціальності 123 – Комп'ютерна інженерія
Міжнародний гуманітарний університет
pankovi6287@gmail.com

Лазарєв Кіріл Олегович
здобувач 2 курсу першого (бакалаврського) рівня
спеціальності 122 – Комп'ютерні науки

Міжнародний гуманітарний університет
lazarevkirill10@gmail.com

ОСОБЛИВОСТІ ПОБУДОВИ ГОНОЧНИХ РОБОТИЗОВАНИХ МАШИНОК, ЩО ЇЗДЯТЬ ПО ЛІНІЇ

Анотація. *Метою роботи є розгляд особливостей побудови апаратної частини гоночних роботизованих машинок (болідів), що їздять по лінії, розроблених авторами статті для участі у змаганнях «E-Formula 2.0», фінал яких відбувся у Національному технічному університеті «Дніпровська політехніка» влітку 2024 року. Особливістю створеного боліду є використання недорогої елементної бази, наявної в багатьох спеціалізованих інтернет-магазинах України, зокрема використання замість популярних плат платформи «Ардуіно» більш дешевих мікроконтролерів STM8.*

Роботизовані машинки, що їздять по лінії, вже багато років залишаються популярним захопленням серед молоді, що цікавиться технологіями та інноваціями. Ці відносно прості пристрої не лише демонструють можливості сучасних технологій, а ще й слугують ефективним інструментом для навчання та досліджень. Роботи цього типу використовуються для тестування і вдосконалення технологій автономного керування, що може бути застосовано в майбутньому для безпілотних автомобілів. Вони є чудовим засобом залучення молоді до науково-технічних дисциплін, у першу чергу, завдяки своїй динамічності. Такі машинки стають невід'ємною частиною STEM-освіти, мотивуючи учнів і здобувачів до вивчення робототехніки та інноваційних технологій. В цілому, роботизовані машинки, що їздять по лінії, є не лише розвагою, але й важливим кроком у розвитку сучасних технологій та підготовці нових поколінь інженерів і програмістів.

Підтвердженням популярності цього напрямку є наявність доволі великої кількості наборів, які дозволяють зібрати перший варіант робота цього типу та дослідити його можливості. Крім того, можливість руху по лінії передбачено і в більш складних проєктах, наприклад, у наборі для складання робота-черепашки (набір KS0558 – Smart Turtle Car V3.0 від компанії Keyestudio) [1] або у наборі для складання робота-танка (набір KS0428 – DIY Mini Tank V2.0 Smart Robot car kit for Arduino STEM від компанії Keyestudio) [2].

Окремим напрямком розвитку роботизованих пристроїв, що їздять по лінії, є роботи, реалізовані у вигляді гоночних болідів. Цей напрямок дозволяє проводити змагання між різними командами, в процесі яких учасники створюють апаратне та програмне забезпечення, що дозволяє максимально швидко і точно проходити траси різного ступеня складності. Це сприяє розвитку навичок програмування, інженерного мислення та розуміння принципів автоматизації. Особливо популярні ці змагання серед школярів та здобувачів, що активно беруть участь у різноманітних конкурсах та фестивалях робототехніки. Саме такими змаганнями і стали змагання «E-Formula 2.0», фінал яких відбувся у Національному технічному університеті «Дніпровська політехніка» 6 червня 2024 року [3]. Автори цієї статті у складі команди «Траєкторія швидкості» прийняли участь у цих змаганнях із гоночним болідом, створеним власноруч.

У доповіді розглянуто особливості побудови апаратної та програмної частин гоночної роботизованої машинки, що їздить по лінії, яка прийняла участь у змаганнях «E-Formula 2.0», а також основні питання, які довелося вирішувати в процесі її створення.

Зовнішній вигляд гоночної роботизованої машинки, що їздить по лінії, створеної авторами, наведено на рис. 1. Пластикове шасі машинки складається з трьох основних частин: платформи, на якій розташовані двигуни та основна частина електронних компонентів, рухомої частини, на якій встановлений датчик лінії, та двох напрямних, призначених для з’єднання елементів в єдину конструкцію. Усі елементи шасі були спроєктовані авторами статті та надруковані на 3D-принтері. Особливістю шасі цього типу є можливість регулювання положення датчика лінії відносно платформи з колесами,

що дозволяє підібрати таке розташування датчика лінії, за якого забезпечується максимальна точність проходження траси.

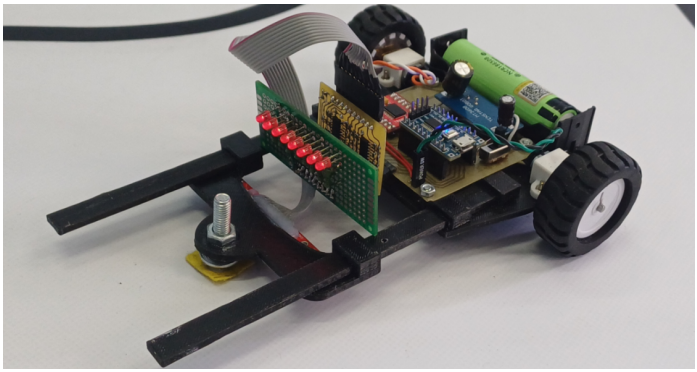


Рисунок 1 – Зовнішній вигляд гоночної роботизованої машинки, що їздять по лінії

У якості двигунів були використані колекторні мікродвигуни із вбудованим редуктором, що при напрузі живлення 6 В забезпечують швидкість обертання 1000 об/хв. із номінальним крутним моментом 0,2 кг/см [4]. Двигуни кріпляться до платформи за допомогою спеціалізованих пластикових скоб [5]. В якості рушіїв боліду були використані пластикові колеса з гумовим протектором діаметром 44 мм [6]. В якості третьої точки опори машинки був використаний металевий гвинт з напівкруглою головкою без шліцу, обертання якого дозволяло регулювати відстань між трасою та датчиками лінії.

У якості датчика лінії був використаний 8-розрядний аналоговий датчик QTR-8A, розроблений компанією Pololu [7]. Вихідні сигнали цього датчика формуються восьма оптопарами, утвореними розташованими поруч інфрачервоним світлодіодом та фототранзистором. Вихідна напруга кожного датчика пропорційна рівню освітленості і тому вона може приймати будь-яке значення в діапазоні від нуля до напруги живлення. В процесі створення машинки з'ясувалося, що цифрові порти введення-виведення мікроконтролера працюють із такими сигналами нечітко, що призводить до істотного погіршення точності проходження траси. Тому між датчиком лінії та мікроконтролером була встановлена додаткова плата, із вісьмома компараторами, охопленими позитивним зворотним зв'язком. Поріг спрацьовування компараторів змінюється за допомогою резистора R2 (рис. 2), що дозволяє швидко адаптувати датчик лінії під конкретний тип траси. Для зручності до виходів компараторів можна підключити додаткову плату, що містить вісім світлодіодів із струмообмежувальними резисторами (елементи R5, VD1 на рис. 2). Ця плата не впливає на роботу боліду, проте за її допомогою можна наочно проконтролювати правильність роботи усіх восьми каналів датчика лінії.

Сигнали з виходів датчика лінії потрапляють на мікроконтролер, який керує усіма вузлами боліду. Зазвичай для створення болідів подібного класу використовують плати, призначені для платформи «Ардуіно», наприклад, плату «Arduino Nano» [8]. Проте у гоночному боліді, що розглядається у цій статті, для керування усіма вузлами відбувається за допомогою мікроконтролера STM8S003F3P6 розташованого на спеціалізованій платі для розробки [9]. Таке рішення дозволило зменшити вартість боліду, оскільки мікроконтролери STM8, що мають приблизно такі ж самі продуктивність та функціональність як і плати «Ардуіно», але при цьому коштують щонайменше втричі дешевше.

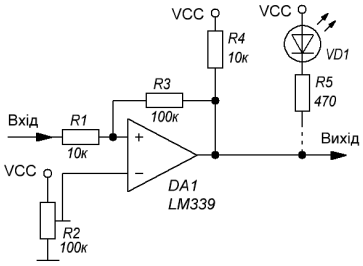


Рисунок 2 – Електрична схема одного каналу компараторів датчиків лінії

Вихідна потужність портів введення-виведення мікроконтролера недостатня для безпосереднього підключення двигунів боліду, тому для керування двигунами був використаний спеціалізований двоканальний драйвер на основі мікросхеми TB6612 [10]. Використання мікросхеми TB6612 дозволило незалежно контролювати швидкість обертання кожного з двигунів у чотирьох режимах: обертання за годинниковою стрілкою, обертання проти годинникової стрілки, вільний рух та гальмування.

Живлення машинки відбувається від однієї акумуляторної комірки NCR18650B із номінальною напругою 3,6 В. Напруга 6 В, яка необхідна для забезпечення потрібної потужності двигунів, формується за допомогою регульованого підвищувального перетворювача на основі контролера MT3608 [11]. Особливістю цієї плати є можливість стабільної роботи при наднизьких вхідних напругах (мінімальна робоча напруга – 2 В), що дозволяє розвивати необхідну потужність навіть при мінімальній кількості енергії в акумуляторі.

Основна частина електронної схеми боліду зібрана на друковані платі, розробленій та виготовленій авторами статті. Таке рішення дозволило істотно підвищити надійність збірки боліду, порівняно із монтажем на макетних платах та з'єднань за допомогою окремих провідників. Двигуни та датчик лінії підключаються до плати за допомогою роз'ємів. Акумуляторна комірка встановлюється у спеціалізований акумуляторний відсік, який підключається до основної плати за допомогою двох провідників.

Окрім модулів мікроконтролера та драйвера двигунів на основній платі також встановлений вимикач живлення та захист від неправильного становлення акумулятора (діод Шотткі, увімкнений послідовно із акумуляторною коміркою). Наявність захисту від неправильного встановлення акумулятора, як показали результати експлуатації, є дуже корисною функцією, оскільки дозволяє повністю уникати витрат часу на ремонт боліду, спричинений випадковим помилковим встановленням акумуляторної комірки.

Висновки. Результати участі у змаганнях «E-Formula 2.0» показали, що даний підхід до проєктування є цілком обґрунтованим і дозволяє досягти необхідного результату – болід впевнено проходить доволі складні траси, що містять, у тому числі, і повороти під кутом 90^0, і «перехрестя». Проте для підвищення швидкості проходження траси слід переробити його конструкцію, врахувавши наступні рекомендації.

1. Для збільшення швидкості боліду його вага повинна бути мінімальною – для цього слід максимально зменшити кількість компонентів, що використовуються, наприклад, відмовитися від використання готових модулів [7, 9 – 11] та змонтувати усі електронні компоненти на монолітній друкованій платі.

2. Режими «Реверс двигуна» (обертання в напрямку протилежному основному напрямку руху боліду), «вільне обертання» та «гальмування» на трасах, розрахованих на швидкісне проходження, є зайвими. Для швидкісного проходження траси достатньо єдиної функції – «рух у прямому напрямку» із можливістю регулювання швидкості

обертання кожного з двигунів. Це дозволить відмовитися від використання спеціалізованого драйвера [10] та керувати двигунами за допомогою двох ключів, реалізованих на польових транзисторах із ізольованим затвором (MOSFET).

3. Для контролю лінії восьми опотопар, скоріш за все, забагато. Слід спробувати контролювати лінію за допомогою трьох або максимум п'яти оптопар.

Таким чином, перший крок, який зробили автори статті, показав необхідність подальшого удосконалення створеного боліду в напрямках зменшення його ваги, спрощення конструкції, кінцевою метою яких є підвищення швидкості та точності проходження траси.

Література

1. Розумний робот-черепашка V3.0 від Keyestudio. URL: https://arduino.ua/prod2495-ymnii-robot-cherepashka-ot-keyestudio.
2. Міні-танк Робот V2.0 з Bluetooth від. URL: https://arduino.ua/prod2034-mini-tank-robot-v2-0-s-bluetooth-ot-keyestudio.
3. Фінал змагань «E-Formula 2.0». URL: https://mgu.edu.ua/tpost/dak4pfpm01-fnal-zmagann-e-formula-20.
4. Мікродвигун з редуктором 6В 1000 RPM. URL: https://arduino.ua/prod3386-mikromotor-s-redyktorom-6v-1000-rpm.
5. Кріплення для двигуна N20. URL: https://arduino.ua/prod5112-kreplenie-dlya-motora-n20.
6. Колесо пластикове N20 44мм. URL: https://arduino.ua/prod3836-koleso-dlya-modelei-i-roboplatform-serebristoe.
7. Модуль 8-ми датчиків лінії Pololu QTR-8A аналоговий. URL: https://arduino.ua/prod3696-modyl-datchikov-linii-pololu-qtr-8a-analogovii-8-shtyk.
8. Arduino Nano V3.0 AVR ATmega328P. URL: https://arduino.ua/prod166-arduino-nano-v3-0-avr-atmega328p-s-raspayannimi-razemami.
9. Плата розробника STM8S003F3P6. URL: https://arduino.ua/prod3766-plata-razrabotchika-stm8s003f3p6.
10. Драйвер двигунів двоканальний на TB6612FNG. URL: https://arduino.ua/prod2377-draiver-dvigatelei-dvyhkanalnii-na-tb6612fng.
11. Регульований підвищувальний перетворювач 2A 28В MT3608. URL: https://arduino.ua/prod1559-regyliryemii-povishaushhii-preobrazovatel-2a-28v-mt3608.

УДК 621.314

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Копитченко Олександр Вікторович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 123 – Комп'ютерна інженерія
Міжнародний гуманітарний університет

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОСЛІДЖЕННЯ РІВНЯ ПЕРЕТВОРЮВАЛЬНОЇ ПОТУЖНОСТІ ІМПУЛЬСНИХ ПЕРЕТВОРЮВАЧІВ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ

Анотація. *Метою роботи є розробка програмного забезпечення для дослідження рівня перетворювальної потужності імпульсних перетворювачів електричної енергії –*

невід'ємної частини сучасних комп'ютерних систем.Як показують результати досліджень, саме перетворювальна потужність визначає більшість питомих показників імпульсних перетворювачів електричної енергії (питома маса, питомий об'єм, питома вартість тощо). В роботі розглянуто принципи побудови та головні алгоритми програмного забезпечення для дослідження рівня перетворювальної потужності найбільш поширених типів імпульсних перетворювачів електричної енергії.

Імпульсні перетворювачі електричної енергії забезпечують функціонування інфокомунікаційних, радіотехнічних та комп'ютерних пристроїв на фізичному рівні, оскільки наявність стабільної напруги живлення є обов'язковою умовою надійної роботи будь-якого електронного вузла. Незважаючи на широке розповсюдження імпульсних перетворювачів в електронній техніці і робіт, присвячених цим типам електронних вузлів, наприклад [1, 2], наразі існує ціла низка питань, що потребують проведення додаткових досліджень, як на практичному, так і на теоретичному рівнях.

Одним з таких питань є визначення рівня перетворювальної потужності перетворювача. В роботі [3] показано, що перетворювальна потужність імпульсного перетворювача може бути менша за величину його вихідної потужності за умови, що його вхід та вихід мають електричний зв'язок, що дозволяє частині енергії, що проходить через перетворювач, переміщуватись між входом та виходом безпосередньо без будь-яких перетворень. У цьому випадку зв'язок між вихідною та перетворювальною потужностями перетворювача визначається наступною формулою [3]:

$$\begin{aligned} P_{\text{ПЕР}} &= P_{\text{ВИХ}} \ - \text{ для схем без електричного зв'язку,} \\ P_{\text{ПЕР}} &= P_{\text{ВИХ}}\left(1-\frac{V_{\text{ВХ}}}{V_{\text{ВИХ}}}\right) - \text{ для вольтододатних схем,} \\ P_{\text{ПЕР}} &= P_{\text{ВИХ}}\left(1-\frac{V_{\text{ВИХ}}}{V_{\text{ВХ}}}\right) - \text{ для вольтовіднімальних схем,} \end{aligned} \tag{1}$$

де $P_{\text{ПЕР}}$ – перетворювальна потужність перетворювача (Вт);
$P_{\text{ВИХ}}$ – вихідна потужність перетворювача (Вт);
$V_{\text{ВХ}}$ – напруга на вході перетворювача (В);
$V_{\text{ВИХ}}$ – напруга на виході перетворювача (В).

Зменшення перетворювальної потужності дозволяє зменшити кількість енергії, яку необхідно запасати в реактивних елементах силової частини перетворювача (дроселях та конденсаторах). А це, у свою чергу, дозволяє покращити усі питомі показники перетворювача (питому вагу, питомий об'єм, питому вартість тощо). Таким чином, питання визначення перетворювальної потужності перетворювача є актуальним.

Однак для практичного використання формули (1), так само як і для практичного використання інших співвідношень для розрахунку параметрів імпульсних перетворювачів, краще всього мати спеціалізоване програмне забезпечення, яке наразі відсутнє.

Метою статті є розробка програмного забезпечення для дослідження рівня перетворювальної потужності імпульсних перетворювачів електричної енергії, структурну схему якого наведено на рис. 1.

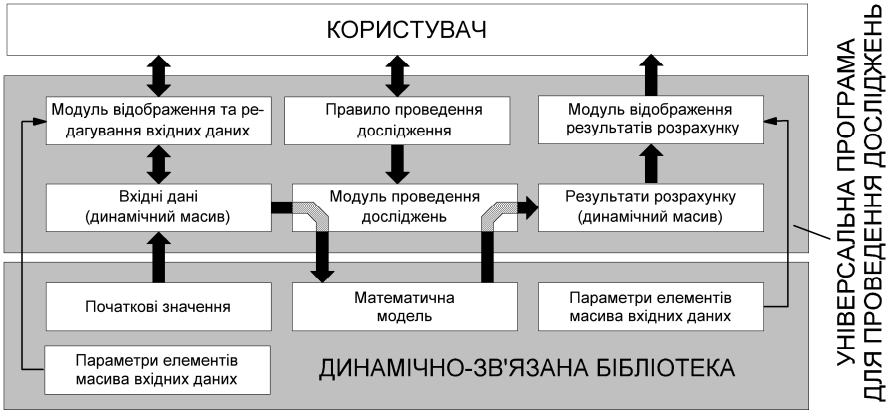


Рисунок 1 – Структурна схема програмного забезпечення

Програмне забезпечення складається із двох незалежних частин: універсальної програми для досліджень (TechProject.exe) та динамічно-зв'язаної бібліотеки (SPS.dll). Інтерфейс користувача реалізовано в універсальній частині (TechProject.exe). До переліку інтерфейсної частини програми входять модулі для відображення та редагування вхідних та вихідних даних та графічний модуль (модуль відображення результатів розрахунку).

Основними елементами, які приймають участь у проведені досліджень, є два масиви: масив вхідних даних та масив результатів розрахунку. Ці масиви є динамічними, тому кількість елементів в них залежить від того, яка математична модель використовується у динамічно-зв'язаній бібліотеці. Масив вхідних даних та результатів розрахунку передаються у математичну модель, яка на основі вхідних даних, які встановлює користувач, формує масив результатів розрахунку.

Спрощений алгоритм розрахунку параметрів імпульсних перетворювачів, у нашому випадку – величини перетворювальної потужності, наведено на рис. 2. Розрахунок починається із тестування масиву вхідних даних, яке відбувається у блоках 2 – 4. На цьому етапі перевіряється загальний розмір масиву і значення його елементів, які повинні знаходитись в певному діапазоні. Перевірка відбувається у підпрограмі TestInputArray (блок 3). У випадку виявлення помилок, наприклад, коли значення хоча б одного елементу масиву виходить за межі допустимих значень, розрахунок переривається у користувачеві формується відповідне повідомлення. Після цього у блоках 5 – 6 відбувається перевірка комбінацій значень вихідних даних. Якщо комбінація значень є помилковою, то розрахунок переривається.

Останньою перевіркою, яку потрібно зробити перед початком розрахунку, є перевірка масиву результатів обчислень, яка відбувається у блоках 8 – 10. На цьому етапі перевіряється лише розмір масиву, який повинен бути достатнім для збереження усіх розрахункових даних.

Після завершення усіх перевірок в одному з блоків 12 – 14 відбувається розрахунок параметрів перетворювача, у тому числі і рівня перетворювальної потужності, визначеної формулою (1). Вибір конкретного набору розрахункових формул залежить від типу схеми – одного із вхідних даних, значення якого перевіряється у блоці 11.

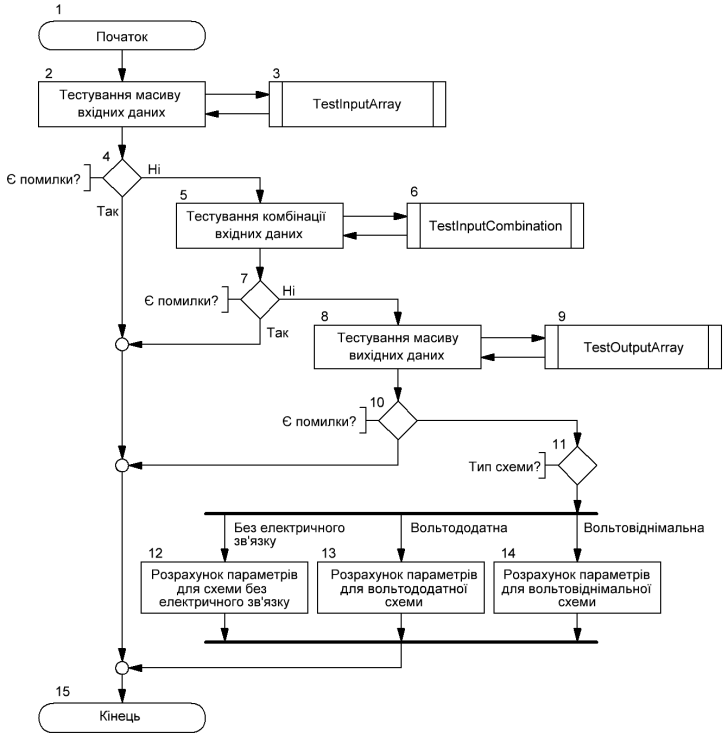


Рисунок 2 – Спрощений алгоритм розрахунку перетворювальної потужності

Висновки. Розроблене програмне забезпечення для дослідження рівня перетворювальної потужності імпульсних перетворювачів електричної енергії дозволяє розраховувати та досліджувати величину перетворювальної потужності найбільш поширених схем перетворювачів, тому його можна використовувати як при проектуванні засобів живлення інфокомунікаційних, радіотехнічних та комп'ютерних пристроїв, так і під час підготовки фахівців у галузі комп'ютерної техніки.

Література

1. Zehendner M., Ulmann M. Power Topologies Handbook. Texas Instruments, 2016.

2. K.Kit Sum Switch Mode Power Conversion Basic Theory and Design. CRC Press, 2017.

3. Kadatskui A.F., Rusu A.P. Determination of the necessary inductor core dimensions for switching electrical energy converters. *Наукові праці ОНАЗ ім. О.С. Попова*, 2018. №1. С.125–135.

УДК 004.58

Бичковський Єгор Олексійович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 122 Комп'ютерні науки
Міжнародний гуманітарний університет
egorbychkovsky@gmail.com

Науковий керівник
Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

АНАЛІЗ РИНКУ АПАРАТНОГО ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМ ТИПУ “РОЗУМНИЙ БУДИНОК” В УКРАЇНІ

Анотація.*Зроблено аналіз ринку апаратного та програмного забезпечення для систем типу “Розумний будинок” в Україні.Розглянуто сучасний стан ринку апаратного та програмного забезпечення для систем типу "Розумний будинок" в Україні. Проаналізовано основні тенденції, проблеми та перспективи розвитку цього ринку. Приділено увагу впливу світових технологічних трендів на український ринок, а також визначено ключові гравці та їх вплив на формування пропозицій для кінцевих споживачів. Особливу увагу приділено діяльності української компанії Ajax Systems, яка є одним з провідних гравців на ринку розумних систем безпеки.*

Ринок "Розумних будинків" стрімко розвивається по всьому світу, зокрема і в Україні. Впровадження інтелектуальних систем у житлові приміщення дозволяє підвищити комфорт, безпеку та енергоефективність. Основними компонентами таких систем є різноманітні датчики, контролери, інтерфейси керування та програмне забезпечення. Зростання попиту на інтелектуальні системи стимулюється збільшенням кількості новобудов та оновленням старого житлового фонду. На ринок активно виходять нові гравці, включаючи як великі міжнародні компанії, так і місцеві стартапи, що пропонують інноваційні рішення. Інтеграція з Інтернетом речей (IoT) дозволяє створювати більш складні та функціональні мережі пристроїв, а розвиток мобільних застосунків забезпечує віддалене управління системами [1].

Однак ринок стикається з певними проблемами. Висока вартість апаратного забезпечення залишається значною перешкодою для масового впровадження систем. Низька обізнаність населення про можливості та переваги "Розумного будинку" також стримує розвиток ринку. Відсутність єдиних стандартів для обладнання різних виробників ускладнює інтеграцію систем, що є додатковою проблемою [1]. Це і обумовило мету роботи, яка полягає в аналізі ринку апаратного та програмного забезпечення для систем типу “Розумний будинок” в Україні.

Серед основних гравців ринку виділяються міжнародні компанії, такі як Google (Nest), Amazon (Alexa) та Samsung (SmartThings), що пропонують повний спектр продуктів для "Розумного будинку". Водночас місцеві компанії, такі як Ajax Systems, спеціалізуються на бездротових системах безпеки та автоматизації. Перспективи розвитку ринку включають зниження цін на обладнання завдяки масовому виробництву та здешевленню технологій, підвищення обізнаності населення через рекламні кампанії та освітні програми, а також розширення функціональності систем завдяки інтеграції з новими технологіями, такими як штучний інтелект та великі дані [2].

Ajax Systems є одним з провідних українських виробників систем безпеки для "Розумних будинків". Компанія пропонує широкий спектр продуктів, включаючи охоронні датчики, контролери, інтерфейси керування та програмне забезпечення для моніторингу та керування системами. Основні продукти Ajax Systems наведені у табл. 1.

Таблиця 1 – Продукти та їх функції[3]

Продукт	Функції
Датчик руху MotionProtect	Виявляє рух людини в приміщенні, сповіщає про проникнення
Датчик диму FireProtect	Виявляє дим і різке підвищення температури, сповіщає про пожежу
Датчик затоплення LeaksProtect	Виявляє витік води, сповіщає про затоплення
Розумна розетка Socket	Дистанційне керування електроприладами, вимірювання споживання електроенергії
Центральний блок Hub	Координує роботу всіх пристроїв системи, забезпечує зв'язок з мобільним застосунком

Технічні особливості програмного забезпечення Програмне забезпечення для систем "Розумний будинок" включає кілька ключових компонентів наведені табл. 2.

Таблиця 2 – Технічна особливість та їх призначення [3]

Технічна особливість	Призначення
Хмарні сервіси	Забезпечують зберігання даних та віддалений доступ до системи через інтернет. Вони дозволяють користувачам керувати своїми пристроями з будь-якої точки світу за допомогою мобільних застосунків.
Мобільні застосунки	Призначені для зручного управління системою з мобільних пристроїв. Застосунки зазвичай пропонують інтуїтивно зрозумілий інтерфейс для налаштування та моніторингу роботи системи.
Інтерфейси програмування (API)	Дозволяють інтегрувати різні пристрої та сервіси між собою, створюючи єдину екосистему. Це забезпечує гнучкість у виборі обладнання та можливість розширення функціональності системи.
Алгоритми штучного інтелекту	Використовуються для аналізу даних з датчиків та пристроїв, забезпечуючи інтелектуальне управління системою. Наприклад, система може навчатися звичкам користувачів та автоматично налаштовувати освітлення чи опалення відповідно до їхніх уподобань.

Впровадження цих технологій дозволяє створювати інтелектуальні системи, які забезпечують високий рівень комфорту, безпеки та енергоефективності для користувачів. Розвиток програмного забезпечення та інтеграція нових технологій, таких як штучний інтелект та великі дані, відкривають нові можливості для розумних будинків, роблячи їх ще більш функціональними та зручними у використанні.

Станом на 2023 рік український ринок "Розумних будинків" демонструє значний потенціал для росту, проте потребує більшої підтримки з боку держави та інвестицій в інфраструктуру. Крім того, важливою є роль освіти та підвищення обізнаності громадян про переваги використання інтелектуальних систем. Враховуючи світові тенденції, можна очікувати, що український ринок продовжить зростати, слідуючи за глобальними технологічними трендами та впроваджуючи інноваційні рішення у повсякденне життя [4].

Висновки. Проведено аналіз ринку апаратного та програмного забезпечення для систем типу “Розумний будинок” в Україні.Ринок апаратного та програмного забезпечення для систем типу "Розумний будинок" в Україні перебуває на етапі активного розвитку. Компанія Ajax Systems відіграє важливу роль у розвитку цього ринку, пропонуючи інноваційні рішення для безпеки та автоматизації. Її продукти, такі як:

Датчик руху MotionProtect, Датчик диму FireProtect, Датчик затоплення LeaksProtect,Розумна розетка Socket, Центральний блок Hub, мають значний функціонал і мають широкий спектр застосувань. Подальший розвиток ринку залежить від інвестицій у інфраструктуру, підтримки з боку держави, а також зусиль виробників та постачальників щодо розробки та впровадження інноваційних рішень.

Література

1. Statista: "Smart Home Market Size and Forecast in Ukraine".
2. MarketsandMarkets: "Smart Home Market Size. Share. Statistics & Industry Growth Analysis Report by Product (Living Control. Security & Access Control. HVAC Control. Smart Speaker. Smart Kithen and Smart Furniture). Software and Services. Sales Channel and Region – Global Forecast to 2028".
3. Ajax Systems: "Innovative Security Solutions for the Smart Home".
4. Міністерство цифрової трансформації України: "Національна програма цифровізації".

УДК 004.05

Лень Дмитро Юрійович
магістр за спеціальністю 123 Комп'ютерна інженерія
Міжнародний гуманітарний університет
Lentjy@gmail.com
Науковий керівник
Розенвассер Денис Михайлович
кандидат технічних наук,
доцент кафедри комп'ютерних наук
Міжнародний гуманітарний університет

ДОСЛІДЖЕННЯ НАДІЙНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

***Анотація**. Дослідження надійності мереж передачі даних набуває особливої важливості в сучасному світі, де інформаційні технології стали невід'ємною частиною всіх аспектів життя. Зростаюча кількість кіберзагроз, високі вимоги до безперебійності, збільшення складності систем та розвиток критичних галузей, таких як охорона здоров'я, фінанси та енергетика, роблять надійність мереж ключовим фактором для безпечної і стабільної роботи.*

Актуальність дослідженні надійності мереж передачі даних можна розділити на декілька пунктів:

1. Високі вимоги до безперебійності роботи мереж передачі даних – це дуже важливо у наш час, тому що будь-які простої або збої можуть призвести до значних фінансових втрат, репутаційних ризиків, втрати даних, а також впливу на здоров'я та життя людей. Надійність систем передачі даних є ключовим фактором для забезпечення безперебійної роботи бізнесу під час венного стану та масових відключень світла.
2. Зростання кількості кіберзагроз не є рідкістю у наш час, з розвитком технологій та Інтернету кіберзлочинці знаходять нові шляхи для атак на комп'ютерні системи та мережі передачі даних. Забезпечення надійності мереж передачі даних стає критичним для захисту від вірусів, хакерських атак, фішингу та інших кіберзагроз.
3. З кожним роком мережі передачі даних стають все більш складними, включаючи інтеграцію з різними платформами, сервісами та пристроями. Зростаюча комплексність вимагає нових підходів до забезпечення надійності, щоб уникнути несправностей і забезпечити стабільну роботу.

4. У багатьох критичних галузях, таких як охорона здоров'я, фінанси, енергетика та транспорт, мережі передачі даних відіграють вирішальну роль. Надійність систем у цих галузях може впливати на життя людей та безпеку держави, що робить дослідження у цій сфері надзвичайно важливими.

5. Впровадження нових технологій, таких як хмарні обчислення, віртуалізація, блокчейн та квантові обчислення, змінює архітектуру комп'ютерних систем та мереж передачі даних. Це вимагає нових підходів до дослідження надійності, щоб гарантувати стабільну і безпечну роботу.

6. Інвестиції у дослідження та підвищення надійності мереж передачі даних можуть значно зменшити витрати на усунення збоїв, покращити продуктивність і конкурентоспроможність компаній. Надійні системи забезпечують довіру клієнтів і партнерів.

7. В багатьох країнах існують жорсткі вимоги та стандарти до надійності і безпеки мереж передачі даних. Наприклад, в Україні існують вимоги до надійності роботи мережі під час військового стану та список критичних точок, які мають працювати навіть в умовах планових відключень світла та повного блекаута. Дотримання цих вимог є необхідним для відповідності законодавству і уникнення штрафів.

8. Соціальна відповідальність за надійність мереж передачі даних є важливою складовою соціальної відповідальності компаній і організацій. Це включає захист приватних даних користувачів, забезпечення безпеки і добробуту суспільства, підтримку довіри до технологій, а також підтримки дієздатності критичних сервісів за будь яких умов.

Методи підвищення надійності мереж передачі даних першу чергу ґрунтуються на оцінці ризиків та факторів які можуть чинити вплив на роботу мереж передачі даних. В залежності від цих факторів треба приймати відповідні дії для підвищення надійності, наприклад:

1. Організація роботи при відсутності електроживлення. Для цього можна встановлювати батареї, генератори, сонячні панелі, або організовувати додаткові вводи живлення.

2. Резервування критично важливого обладнання, на випадок програмних чи апаратних проблем.

3. Оптимізація мереж передачі даних таким чином, щоб аварії на окремих елементах системи не впливали на загальну надійність мережі.

4. Організація роботи мережі за умов відсутності швидкого доступу для відновлення обладнання під час комендантської години чи повітряною тривоги.

5. Географічне рознесення тих вузлових центрів та критичного обладнання мережі передачі даних, які неможливо задублювати.

6. Організація віддаленого доступу до систем керування мережею на випадок неможливості фізичного доступу до обладнання та офісу.

7. Періодична зміна паролів та використання двохфакторної авторизації для унеможливлення несанкціонованого доступу.

8. Аналіз нормативно правових актів від державних органів та виконання термінових розпоряджень військових адміністрацій.

Висновки: дослідження надійності мереж передачі даних є надзвичайно актуальним і важливим фактором для забезпечення стабільного та безпечного функціонування сучасного суспільства, бізнеса та підвищення рівня життя громадян за будь-яких умов.

Література:

1. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп'ютерні мережі: [навчальний посібник]. - Львів, 2013. 373 с.

2. Попов А.Ф., Комп’ютерні системи і мережі. Чернівці, Україна: 2010.

3. Тарнавський Ю.А., Кузьменко І.М. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.

4. Жураковский Б. Ю. Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 336 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36615

5. Жураковський Б. Ю. Комп'ютерні мережі. Частина 2 Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 372 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36641

6. Alessandro Birolini. Reliability Engineering: Theory and Practice. Springer, 2017. - 651 p.

7. Alessandro Birolini. Quality and Reliability of Technical Systems: Theory, Practice, Management. Springer Science & Business Media, 2012. - 502 p.

8. Тиш Є.В. Конспект лекцій з дисципліни „Надійність, контроль, діагностика та експлуатація ЕОМ" для студентів денної форми навчання. Тернопіль, 2016.

9. Василевський О. М., Поджаренко В. О. Нормування показників надійності технічних засобів. Навчальний посібник. http://posibnyky.vntu.edu.ua/pdf/000754.pdf.

10. Надійність техніки. Оцінювання і прогнозування залишкового ресурсу (терміну служби) технічних систем. ДСТУ. http://www.immsp.kiev.ua/activity/Napriam%208_Standarty/Standart_Zalyshkovij_resurs.pdf.

11. Власенко К. В., Грудкіна Н. С. Надійність технічних систем. Методичні рекомендації до самостійної роботи. http://www.dgma.donetsk.ua/metod/vm/118.pdf.

12. Скакун М. Р., Ткаченко О. М., Лемешко А.В. Аналіз методів дослідження продуктивності комп'ютерних мереж // Телекомунікаційні та інформаційні технології. - 2021. - № 4 (73)

13. Кузьмичов А.І. Оптимізаційні моделі мережевих структур / А.І. Кузьмичов, Є.О. Додонов // Реєстрація, зберігання і обробка даних. – Т.19. - № 2. – 2017. – С. 24 – 35.

14. Кучеров Д.П. Керування перевантаженням комп'ютерної мережі. [Електронний ресурс] - https://ceur-ws.org/Vol-2067/paper10.pdf

15. iPerf - The ultimate speed test tool for TCP, UDP and SCTP. [Електронний ресурс] - https://iperf.fr/iperf-doc.php#3doc

16. Richard Sharpe, Ed Warnicke, Ulf Lamping. Wireshark User's Guide [Електронний ресурс] - https://www.wireshark.org/docs/wsug_html_chunked/

17. Комп'ютерні мережі. Частина 1. Моделювання комп'ютерних мереж: Лабораторний практикум. / Укладачі: О. С. Яценко, О. І. Яценко. – Житомир: Вид-во ЖДУ ім. І. Франка, 2022. – 76 с.

18. Платтнер Б., Чернега В. Безпровідні локальні комп'ютерні мережі: навч. посібник. К.: Кондор, 2018. – 238 с.

19. Комп'ютерні мережі навчальний посібник для виконання лабораторних робіт [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології»/ спеціалізації «Інформаційне забезпечення робототехнічних систем» / Б.Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 10,08 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. –213 с.

20. OMNET++ Simulator. https://omnetsimulator.com/

21. Абрамов В.О. Застосування комбінованих моделей комп'ютерних мереж в навчальному процесі // Кібербезпека: освіта, наука, техніка, - № 4 (4), 2019. DOI 10.28925/2663-4023.2019.4.2431

УДК 004.94

Клімішина І.В.
Міжнародний гуманітарний університет, місто Одеса

klimishyna.iryna@gmail.com
Паскаленко В.М.
Міжнародний гуманітарний університет, місто Одеса
Салагор В.І.
Міжнародний гуманітарний університет, місто Одеса

МЕТОДИ ВЕРИФІКАЦІЇ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ

Анотація. *Розглядаються методи верифікації комп'ютерних систем критичного призначення, що є життєво важливим для забезпечення їхньої надійності та безпеки. Проаналізовано методи тестування, симуляції та аналізу, які використовуються для перевірки правильності роботи систем у галузях, що потребують високого рівня надійності, таких як енергетика, медицина, транспорт і авіація. Особлива увага приділяється побудові моделей і методів автоматизованого проектування та дослідження тестопридатних цифрових систем логічного управління на базі кінцевих автоматів. Запропоновано підходи для підвищення тестопридатності систем шляхом розробки додаткових переходів у графах автоматів та впровадження вбудованих систем діагностування на етапі проектування. Розглянуто можливості застосування хмарних сервісів для автоматизованого проектування тестопридатних HDL-моделей керуючих автоматів. Використання методів тестопридатного проектування дозволяє скоротити час та витрати на технічне обслуговування, підвищити надійність та безпеку комп'ютерних систем критичного призначення.*

Комп'ютерні системи критичного призначення відіграють важливу роль у багатьох галузях, включаючи енергетику, медицину, авіацію та транспорт. Надійність і безпека цих систем є життєво важливими, оскільки помилки або збої можуть мати катастрофічні наслідки. Верифікація таких систем є важким процесом, що включає використання різних методів для забезпечення їх правильної та надійної роботи [1,2].

Верифікація комп'ютерних систем критичного призначення є ключовим етапом у забезпеченні їхньої надійності та безпеки. Використання різних методів, таких як формальні методи, тестування, симуляція та аналіз, дозволяє забезпечити всебічну перевірку систем. Діагностичні експерименти та методи тестопридатного проектування є ефективними інструментами для знаходження та виправлення помилок на різних етапах розробки і експлуатації систем логічного управління.

Для відстеження роботи автоматних систем логічного управління доцільно застосовувати або апаратні системи, які імітують алгоритм керування або діагностування, або методи тестопридатного проектування, які перетворюють керуючі автомати на легкотестовані, тобто такі, у яких витрати на проведення діагностичного експерименту є мінімальними за довжиною та часом. При проектуванні систем логічного управління на технологічній платформі ПЛІС із застосуванням САПР на базі мов опису апаратури вбудовані системи діагностування та апаратні засоби підвищення тестопридатності доцільно вводити ще на етапі побудови моделей мовами опису апаратури.

Для верифікації комп'ютерної системи критичного призначення пропонується проведення кілька діагностичних експериментів:

1. Створити кілька сценаріїв, які відображають реальні умови використання системи, і виконати їх тестування.
2. Змодельовати кілька відмов у системі для перевірки її стійкості та надійності.
3. Зібрати та проаналізувати логи системи для виявлення помилок та аномалій.

Результати діагностичних експериментів мають показати проблеми або помилки у роботі системи. Виявлені проблеми мають бути усунені, що дозволить підвищити надійність та безпеку комп'ютерної системи критичного призначення.

Таким чином, методи тестування на основі сценаріїв, симуляції відмов та аналізу логів у поєднанні з методами тестопридатного проектування є ефективними інструментами для верифікації комп'ютерних систем критичного призначення. Впровадження цих методів у процес розробки та експлуатації таких систем забезпечить їх високу надійність, безпеку та ефективність, що є життєво важливим у критичних галузях.

У сучасних критичних системах, таких як енерго- та газопостачання, застосовуються локальні системи логічного управління й регулювання. Ці системи базуються на композиції керуючого та операційного автоматів, розташованих на технологічно відокремлених об'єктах. Важливо забезпечити високу надійність та ефективність цих систем, особливо в умовах критичних режимів роботи. Для цього необхідно мати ефективні методи контролю та діагностики автоматних систем логічного управління.

Одним із перспективних підходів до підвищення надійності та зменшення витрат на технічне обслуговування систем є методи тестопридатного проектування [3,4]. Ці методи спрямовані на створення систем, які легко тестуються, що дозволяє скоротити час і ресурси, необхідні для проведення діагностичних експериментів. При проектуванні систем логічного управління на технологічній платформі ПЛІС з використанням САПР на основі мов опису апаратури важливо враховувати системи діагностування або підвищення тестопридатності апаратними засобами. Важливим і дуже актуальним науко-технічним завданням є розробка моделей і методів автоматизованого проектування та дослідження тестопридатних цифрових систем логічного управління на базі кінцевих автоматів. Метою роботи є розробка моделей і методів автоматизованого проектування та діагностування автоматних систем логічного управління на ПЛІС з використанням мов опису апаратури для скорочення часу технічного обслуговування критичних систем. Практичне значення в галузі комп'ютерної інженерії полягає у розробці тестопридатних моделей кінцевих автоматів з використанням мов опису апаратури САПР РЕП та шаблонів автоматного програмування. Для зменшення апаратурних витрат при побудові легкотестованих керуючих автоматів пропонується метод додаткових переходів у графах автоматів за допомогою процедури розрахунку тестопридатності кінцевих автоматів.

Розроблені процедури розрахунку тестопридатності кінцевих керуючих автоматів дають можливість оптимізувати створення додаткових переходів у графових моделях автоматів, що дозволяє зменшити апаратурні витрати при побудові легкотестованих керуючих автоматів. Показана можливість розробки програмного модуля із візуальним інтерфейсом для автоматизованого проектування тестопридатних HDL-моделей кінцевих керуючих автоматів. Реалізація програмного модуля пропонується у вигляді хмарного сервісу. Використання методів тестопридатного проектування дозволяє скоротити час та витрати на технічне обслуговування, підвищити надійність та безпеку комп'ютерних систем критичного призначення.

Таким чином, методи верифікації комп'ютерних систем критичного призначення є необхідним інструментом для забезпечення їх надійності та безпеки. Системи, що використовуються у таких важливих галузях, як енергетика, медицина, транспорт і авіація, потребують особливо ретельного тестування та верифікації для запобігання катастрофічним наслідкам у разі помилок або збоїв. Розробка моделей і методів автоматизованого проектування та дослідження систем логічного управління на базі кінцевих автоматів дозволяє значно підвищити ефективність та надійність цих систем. Використання мов опису апаратури для побудови моделей та впровадження вбудованих систем діагностування ще на етапі розробки, сприяє зменшенню витрат на технічне обслуговування та покращенню тестопридатності систем.

Висновки

1. Верифікація комп'ютерних систем критичного призначення є важливим завданням, яке потребує використання спеціальних моделей та методів. Діагностичні

експерименти дозволяють виявити та виправити потенційні проблеми у функціонуванні системи, що підвищує її надійність та безпеку. В роботі розглянуто кілька моделей та методів верифікації, а також наведено приклад їх застосування для системи управління повітряним рухом.

2. Запропоновані методи тестопридатного проектування забезпечують створення систем, які легко тестуються, що знижує час і ресурси, необхідні для проведення діагностичних експериментів. Зокрема, побудова додаткових переходів у графових автоматів за допомогою процедур розрахунку тестопридатності дозволяє зменшити апаратурні витрати при створенні керуючих автоматів.

Література

1. Мірошник М. А. Обробка подій у цифрових пристроях реального часу. / Мірошник М. А., Шкіль О.С., Рахліс Д.Ю., Пшеничний К. Ю., Мірошник А. Н. / Збірник наукових праць «Вісник ЧДТУ», 2023, №2., с.50-57.

2. Шкарупило В.В. Сценарії, методи та засоби формальної верифікації артефактів процесу проєктування систем критичного призначення: монографія В.В. Шкарупило, І.В. Блінов. — Вінниця: ГО «Європейська наукова платформа», 2021. — 104с.

3. Негуриця Д. С. Адаптивність та адаптованість програмного забезпечення систем критичного призначення / Д. С. Негуриця // Радіоелектронні і комп'ютерні системи. - 2014. - № 6. - С. 48-52.

4. Давидов В. В. Моделі та методи підвищення безпеки програмного забезпечення (монографія). Харків, 2021. 146 с.

УДК [004.7+004.8]:621.31

М. О. Лановський
магістр спеціальності 123 – Комп'ютерна інженерія
Міжнародний гуманітарний університет
lanovskiy@gmail.com
Науковий керівник: ***О. П. Русу***
кандидат технічних наук, доцент
кафедри комп'ютерних наук
Міжнародний гуманітарний університет
м. Одеса, Україна

ВПРОВАДЖЕННЯ «РОЗУМНИХ» ТЕХНОЛОГІЙ В СИСТЕМИ ЕНЕРГЕТИЧНОГО МЕНЕДЖМЕНТУ ВІТЧИЗНЯНИХ ПІДПРИЄМСТВ

Анотація. *Розглянуто визначення традиційних та «розумних» мереж, роль енергетичного менеджменту в енергоефективності підприємства та переваги «розумної» системи енергоменеджменту. Визначено ключовий елемент для трансформації традиційних мереж в «розумні» – мікромережа та її складові. Виявлено не розв'язані питання, пов'язані з впровадженням «розумних» технологій.*

Актуальність теми. Для підприємств, які прагнуть оптимізувати енергоспоживання та зменшити операційні витрати, інтеграція систем енергоменеджменту стає необхідним кроком на шляху підвищення продуктивності. Це питання особливо актуальне й для українських підприємств, де дефіцит енергоресурсів та економічні виклики вимагають впровадження прогресивних рішень. Стрімкий розвиток «розумних» технологій (зокрема smart grid), дослідження методів керування мікромережею (microgrid), розповсюдження рішень Інтернету речей – це відкриває перспективні підходи до підвищення стійкості та ефективності енергетичних систем [1–3].

Мета роботи. Розгляд потенційних переваг та недоліків впровадження технологій «розумного» енергоменеджменту. Основна увага приділяється: цифровізації енергетичної мережі підприємства, надання інструментів «розумного» керування джерелами енергії та викликам з впровадження «розумної» мережі.

У роботі будуть вирішені такі **завдання**: визначення традиційних та «розумних» електричних мереж; визначення ролі систем енергетичного менеджменту; визначення мікромереж; розгляд проблем інтеграції «розумних» мереж.

Виклад основного матеріалу.Традиційна електрична мережа являє собою мережу електростанцій, ліній електропередач та розподільчих систем, які використовуються для виробництва, передачі та розподілу електроенергії відповідно. Враховуючи нинішній енергетичний дефіцит нашої країни та враховуючи постійну потребу в більш ефективному та надійному енергопостачанні підприємств, потребується перехід до «розумних» мереж (smart grid), які бурхливо досліджуються та розвиваються [3–5].

«Розумна» мережа – це вдосконалена електрична інфраструктура, яка контролює та оптимізує використання електроенергії за допомогою цифрових технологій. Вона сприяє трансформації енергетичного сектору, надає можливість швидко реагувати на відключення або обмеження основних ліній живлення, розподіляти пікове навантаження та оперативно реагувати на несправності в мережі. Шляхом використання «розумних» лічильників, відновлюваних джерел енергії разом з впровадженням системи зберігання енергії, а також інтеграції «розумної» системи енергоменеджменту, «розумна» мережа надає можливість скоротити втрати енергії, підвищити надійність електропостачання та знизити витрати на споживану електроенергію [3,4].

Енергетичний менеджмент – набір заходів, спрямованих на економію енергетичних ресурсів: моніторинг енергоспоживання; аналіз показників, результати якого використовуються як основа для розроблення нових енергетичних бюджетів; розроблення енергетичної політики; планування нових енергоощадних заходів і под. [6].

«Розумна» система енергоменеджменту – це цифрова (комп'ютерна) система, що надає можливість відстежувати, контролювати, вимірювати та оптимізувати енергоспоживання. Така система поєднує в собі елементи, що споживають електроенергію (наприклад, опалення, вентиляція та кондиціонування, освітлення та виробниче обладнання), з лічильниками, датчиками та іншими інтелектуальними або комунікаційними пристроями, які відстежують стан, вимірюють та агрегують дані всередині системи. Система енергетичного менеджменту може зв'язуватися з комунальним підприємством або оператором основної мережі для, наприклад, закупівлі енергії за дешевшим тарифом, для передачі надлишкової енергії в рамках програм операторів енергосистеми, для реагування на обмеження споживаної енергії тощо [4,5,7].

Важливою складовою для досягнення енергоефективності та успішної трансформації наявних мереж в «розумні» мережі є мікромережі. Мікромережа (microgrid) – це локальна електрична мережа, що діє як єдиний і контрольований об'єкт. Вона складається з: - енергетичних генераторів (дизельних генераторів, сонячних батарей, вітрогенераторів тощо); - систем зберігання енергії, які знижують пікові навантаження, згладжують вироблення відновлюваних джерел енергії; - споживачів/навантажень; - точки з'єднання мікромережі та основної мережі, що охоплює різноманітне силове обладнання та пристрої для розподілу електроенергії, управління та захисту обох мереж; - системи енергетичного менеджменту, яка отримує інформацію від джерел генерації, накопичувачів енергії, споживачів та основної мережі.

Використання мікромережі дозволяє правильно розподілити, синхронізувати, балансувати використання енергетичних ресурсів та досягнути часткову або повну енергетичну незалежність об'єкта живлення. Мікромережі зазвичай підключаються до основної енергосистеми, але можуть від'єднуватися від неї, щоб обслуговувати споживачів під час відключень або в періоди обмежень [8,9].

Однією з головних проблем у впровадження технологій «розумних» мереж є потреба в значних початкових капіталовкладеннях для побудови необхідної інфраструктури та систем. Комунальні підприємства, малі та середні підприємства стикаються зі значними витратами на модернізацію наявних електромереж, що стає бар'єром для швидкого впровадження «розумних» технологій.

Додатковою перешкодою для впровадження цих технологій є складність інтеграції різних компонентів і систем у цілісну та сумісну мережу; відсутність стандартизації. Різні технології можуть бути несумісні в рамках однієї мережі. Забезпечення зв'язку та обміну даними між різними пристроями може стати складним завданням, що вимагає ретельного планування та координації усіх сторін, залучених до процесу модернізації електромережі.

Не менш важливою є проблема «холодного» старту: запуск мікромережі без підключення до основних ліній. На частоту та напругу системи може вплинути різке споживання струму на перших етапах запуску мережі в енергонезалежному режимі, що призводить до відключення генераторів та загальної зупинки системи [8].

Висновки. Враховуючи нинішні реалії нашої країни – дефіцит енергоресурсів та економічні виклики – зростання споживання електроенергії та необхідність стабільного і надійного її постачання в енергосистему підприємств зумовлює перехід з традиційної енергетичної мережі до «розумної».

Важливим елементом «розумних» мереж є мікромережі, які складаються з енергетичних генераторів, систем зберігання енергії, споживачів, точки з'єднання з основною мережею. Ядром «розумної» мережі (та мікромережі) є «розумна» система енергоменеджменту – цифрова (комп'ютерна) система, яка допомагає скоротити втрати енергії, підвищити надійність електропостачання, оперативно реагувати на зміни в системі та знизити витрати на споживану електроенергію.

Однак, враховуючи бурхливий розвиток «розумних» технологій, донині залишаються відкритими важливі питання, пов'язані з потребою значних капіталовкладень, відсутністю стандартизації, сумісності компонентів та проблемою «холодного» старту мікромережі.

Література

1. Самойленко М.Ю. Принципи застосування технології Інтернет речей у сучасному світі техніки // Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. 2020. Вип. 31 (70), № 6 Частина 1. С. 142–148.

2. Ukraine Fights To Build More Resilient, Renewable Energy System in Midst of War | News | NREL. URL: https://www.nrel.gov/news/features/2023/ukraine-fights-to-build-a-more-resilient-renewable-energy-system-in-the-midst-of-war.html (дата звернення: 14.07.2024).

3. Saleem M.U. et al. Integrating Smart Energy Management System with Internet of Things and Cloud Computing for Efficient Demand Side Management in Smart Grids // Energies 2023, Vol. 16, Page 4835. Multidisciplinary Digital Publishing Institute, 2023. Вип. 16, № 12. С. 4835.

4. Pawar P., Vittal K P. Design and development of advanced smart energy management system integrated with IoT framework in smart grid environment // J Energy Storage. Elsevier, 2019. Вип. 25. С. 100846.

5. Smart energy management for industrials | Deloitte Insights. URL: https://www2.deloitte.com/xe/en/insights/industry/power-and-utilities/smart-energy-management.html (дата звернення: 15.07.2024).

6. Енергоменеджмент | ДЕРЖПРОДСПОЖИВСЛУЖБА. URL: https://dpss.gov.ua/diyalnist/enerhomenedzhment (дата звернення: 15.07.2024).

7. Mischos S., Dalagdi E., Vrakas D. Intelligent energy management systems: a review // Artif Intell Rev. Springer Nature, 2023. Вип. 56, № 10. С. 11635–11674.

8. Uddin M. et al. Microgrids: A review, outstanding issues and future trends // Energy Strategy Reviews. Elsevier, 2023. Вип. 49. С. 101127.

9. Wu H., Li H., Gu X. Optimal energy management for microgrids considering uncertainties in renewable energy generation and load demand // Processes. MDPI AG, 2020. Вип. 8, № 9.

УДК 004.7

Педяш В.В., к.т.н., доцент
Сулейманов С.С., студент
Міжнародний Гуманітарний Університет
s.suleymanov09121998@gmail.com

ДОСЛІДЖЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ КОРПОРАТИВНИХ МЕРЕЖ ПРИ ВПРОВАДЖЕННІТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Анотація. *Дане дослідження присвячене аналізу енергоефективності корпоративних мереж при впровадженні технологій Інтернету речей, з особливим фокусом на системи управління освітленням. Розглянуто актуальність проблеми оптимізації енергоспоживання в умовах зростаючої складності корпоративної інфраструктури. Проаналізовано потенціал інтеграції систем автоматичного управління будівлями з IoT-технологіями для створення комплексних рішень енергоменеджменту. Досліджено сучасні технології управління освітленням, зокрема аналогове управління 1-10 В та цифровий протокол DALI, та їх роль у підвищенні енергоефективності. Окреслено перспективні напрямки подальших досліджень у галузі енергоефективних IoT-рішень для корпоративних мереж.*

У сучасному світі питання енергоефективності набуває все більшої актуальності, особливо в контексті корпоративних мереж та великих підприємств. З розвитком технологій Інтернету речей (IoT) з'являються нові можливості для оптимізації енергоспоживання та підвищення загальної ефективності роботи корпоративних систем [1-2]. Однак, впровадження IoT-технологій у корпоративні мережі породжує ряд викликів, пов'язаних з інтеграцією, безпекою та управлінням великими обсягами даних.Актуальність дослідження енергоефективності корпоративних мереж при впровадженні технологій Інтернету речей обумовлена зростаючою потребою в оптимізації енергоспоживання в умовах глобальної енергетичної кризи та підвищення цін на енергоносії. Корпоративні мережі, які охоплюють великі офісні будівлі, виробничі приміщення та data-центри, є значними споживачами енергії. Тому пошук шляхів підвищення їх енергоефективності є критично важливим завданням для сучасного бізнесу.

Проблема полягає в тому, що традиційні методи управління енергоспоживанням в корпоративних мережах часто виявляються неефективними в умовах зростаючої складності інфраструктури та збільшення кількості пристроїв. Впровадження технологій IoT відкриває нові можливості для моніторингу та оптимізації енергоспоживання, але вимагає комплексного підходу до інтеграції та управління.

Метою даного дослідження є аналіз можливостей підвищення енергоефективності корпоративних мереж шляхом впровадження технологій Інтернету речей. У рамках дослідження планується розглянути існуючі підходи до енергоменеджменту в корпоративних мережах, оцінити потенціал IoT-технологій для оптимізації енергоспоживання, а також розробити рекомендації щодо ефективної інтеграції IoT-рішень в існуючу інфраструктуру.

Одним з ключових аспектів дослідження є аналіз доцільності впровадження систем автоматичного управління будівлями (Building Management Systems, BMS) та їх інтеграції з технологіями IoT. BMS представляють собою комплексні рішення для контролю та управління інженерними системами будівель, включаючи системи опалення, вентиляції,

кондиціонування, освітлення та безпеки.Інтеграція BMS з технологіями IoT дозволяє створити єдину екосистему "розумної будівлі", де всі системи працюють узгоджено та ефективно. IoT-датчики, розміщені по всій будівлі, збирають дані про температуру, вологість, освітленість, присутність людей та інші параметри. Ці дані в режимі реального часу передаються до центральної системи управління, яка аналізує їх та приймає рішення щодо оптимізації роботи всіх підсистем.

Особливу увагу в рамках дослідження планується приділити системі освітлення як одній з ключових підсистем будівлі, що має значний потенціал для оптимізації енергоспоживання. Сучасні технології управління освітленням дозволяють значно знизити витрати на електроенергію за рахунок автоматичного регулювання яскравості та кольорової температури світла в залежності від зовнішніх умов та присутності людей.

Однією з найпоширеніших технологій управління освітленням є аналогове управління за допомогою сигналу 1-10 В. Ця технологія дозволяє плавно регулювати яскравість світильників шляхом зміни напруги в діапазоні від 1 до 10 вольт. Перевагами даної технології є простота реалізації та сумісність з широким спектром світлодіодних драйверів.Система управління освітленням 1-10 В працює наступним чином: контролер посилає аналоговий сигнал напруги до світлодіодного драйвера, який відповідно змінює струм, що подається на світлодіоди. При напрузі 1 В світильник працює на мінімальній яскравості (зазвичай близько 10% від максимальної), а при 10 В - на максимальній яскравості.Однак, технологія 1-10 В має ряд обмежень. Зокрема, вона не дозволяє здійснювати індивідуальне управління окремими світильниками в групі та не передбачає зворотного зв'язку від світильників до контролера. Крім того, для реалізації цієї технології потрібно прокладати додаткові кабелі управління, що може бути проблематичним у випадку модернізації існуючих систем освітлення.

Альтернативою аналоговому управлінню є цифровий протокол DALI (Digital Addressable Lighting Interface). DALI - це стандартизований протокол зв'язку для систем освітлення, який дозволяє здійснювати двонаправлений обмін даними між контролером та світильниками. Кожен пристрій в системі DALI має унікальну адресу, що дозволяє індивідуально керувати кожним світильником або групою світильників.Протокол DALI забезпечує більш гнучке та точне управління освітленням порівняно з технологією 1-10 В. Він підтримує до 64 індивідуальних адрес на одній шині та дозволяє створювати до 16 груп світильників. Крім регулювання яскравості, DALI підтримує додаткові функції, такі як автоматичне тестування аварійного освітлення, зберігання сценаріїв освітлення та звітування про стан світильників.Важливою перевагою протоколу DALI є можливість інтеграції з системами автоматизації будівель та IoT-платформами. Це дозволяє створювати комплексні рішення для управління освітленням, які враховують дані з різних датчиків (присутності, освітленості, температури) та можуть бути частиною загальної стратегії енергоменеджменту будівлі.

Порівнюючи технології 1-10 В та DALI з іншими рішеннями для управління освітленням, можна відзначити, що вони займають проміжне положення між простими аналоговими системами та більш складними цифровими протоколами, такими як DMX512 або KNX. Технологія 1-10 В залишається популярною завдяки своїй простоті та низькій вартості, особливо для невеликих проектів. DALI, у свою чергу, пропонує більш широкі можливості при помірній складності реалізації.

На відміну від бездротових технологій управління освітленням, таких як Zigbee або Bluetooth Low Energy, DALI та 1-10 В є дротовими рішеннями, що забезпечує більшу надійність та стабільність роботи. Це особливо важливо для корпоративних мереж, де надійність та безпека є ключовими вимогами.Впровадження систем управління освітленням на базі технологій 1-10 В або DALI в корпоративних мережах дозволяє досягти значної економії електроенергії. За різними оцінками, економія може складати від 30% до 75% порівняно з традиційними системами освітлення без можливості регулювання. Це досягається за рахунок автоматичного димування світильників в

залежності від рівня природного освітлення, відключення освітлення в приміщеннях, де немає людей, та оптимізації роботи освітлення відповідно до графіку роботи офісу.

Інтеграція систем управління освітленням з технологіями IoT відкриває додаткові можливості для підвищення енергоефективності. Наприклад, використання IoT-датчиків присутності та руху дозволяє створювати більш точні та гнучкі сценарії роботи освітлення. Аналіз даних про використання приміщень, зібраних за допомогою цих датчиків, може допомогти оптимізувати розклад роботи офісу та більш ефективно використовувати простір [3].Крім того, інтеграція систем освітлення з іншими підсистемами будівлі через IoT-платформу дозволяє реалізувати комплексні стратегії енергозбереження. Наприклад, система може автоматично знижувати яскравість освітлення при підвищенні температури в приміщенні, щоб зменшити навантаження на систему кондиціонування.

Важливим аспектом впровадження IoT-технологій в системи управління освітленням є забезпечення кібербезпеки. Оскільки світильники та контролери освітлення стають частиною корпоративної мережі, вони можуть стати потенційною точкою входу для кіберзлочинців. Тому при проектуванні таких систем необхідно передбачати механізми шифрування даних, автентифікації пристроїв та сегментації мережі.Важливо відзначити, що впровадження технологій IoT в системи управління освітленням та інші підсистеми будівлі вимагає комплексного підходу та врахування специфіки конкретного об'єкта. Необхідно провести детальний аудит існуючої інфраструктури, оцінити потенціал енергозбереження та розробити стратегію поетапного впровадження нових технологій.

При виборі конкретних технічних рішень для управління освітленням в корпоративних мережах слід враховувати не тільки їх функціональність та енергоефективність, але й сукупну вартість володіння. Це включає в себе витрати на придбання обладнання, його встановлення, налаштування, обслуговування та можливу модернізацію в майбутньому.Також важливо забезпечити сумісність обраних рішень з існуючими системами автоматизації будівлі та корпоративною IT-інфраструктурою. Це дозволить уникнути створення ізольованих "островів автоматизації" та забезпечити ефективне управління всіма системами будівлі з єдиного центру [4].

Окремої уваги заслуговує питання навчання персоналу роботі з новими системами управління освітленням та іншими IoT-рішеннями. Ефективність впровадження нових технологій значною мірою залежить від того, наскільки добре співробітники розуміють принципи їх роботи та можуть використовувати всі їх можливості. Для корпоративних мереж важливо також розглянути можливості інтеграції систем управління освітленням з системами управління робочими місцями (Workplace Management Systems). Це дозволить оптимізувати використання офісного простору та забезпечити комфортні умови роботи для співробітників при мінімальних витратах енергії.

При проектуванні систем управління освітленням на базі IoT-технологій важливо враховувати можливості масштабування та адаптації системи до змін у структурі організації та використанні приміщень. Гнучкість та модульність архітектури системи дозволить легко додавати нові функції та інтегрувати нові пристрої в майбутньому.

На основі проведеного дослідження можна зробити висновок, що впровадження технологій Інтернету речей в системи управління освітленням корпоративних мереж має значний потенціал для підвищення енергоефективності та оптимізації використання ресурсів. Інтеграція систем автоматичного управління будівлями з IoT-технологіями дозволяє створити єдину екосистему "розумної будівлі", що забезпечує комплексний підхід до енергоменеджменту. Сучасні технології управління освітленням надають широкі можливості для оптимізації енергоспоживання та підвищення комфорту користувачів, однак їх впровадження вимагає комплексного підходу, що враховує питання безпеки, масштабованості та інтеграції з існуючою інфраструктурою.

Перспективи подальших досліджень у цій галузі включають розробку більш ефективних алгоритмів прогнозування потреб в освітленні, дослідження можливостей

інтеграції систем управління освітленням з іншими "розумними" системами будівлі, вивчення впливу "людиноцентричного освітлення" на продуктивність праці, а також розробку нових стандартів та протоколів для забезпечення сумісності IoT-пристроїв. Важливим напрямком є також дослідження методів підвищення кібербезпеки IoT-систем у корпоративних мережах та розробка стратегій циркулярної економіки для мінімізації екологічного впливу цих технологій.

Література

1. Азаров О. Д. Комп'ютерні мережі : підручник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук та ін. − Вінниця : ВНТУ, 2020. − 378 с.
2. Карпенко М. Ю. Конспект лекцій з курсу «Комп'ютерні мережі» / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2019. – 99 с.
3. Блозва А.І. Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька // - К.: Компрінт, 2017.- 821с.
4. Тарбаєв С.І. Проектування інфокомунікаційних мереж. Навчальний посібник. – Київ: ННІТІ ДУТ, 2019. – 186 ст.

УДК 621.314

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Мись Олександр Миронович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 122 Комп'ютерні науки
Міжнародний гуманітарний університет

ДИНАМІЧНО-ЗВ'ЯЗАНА БІБЛІОТЕКА ДЛЯ РОЗРАХУНКУ ПЕРЕТВОРЮВАЧІВ НАПРУГИ ДЛЯ КОМП'ЮТЕРНОГО ОБЛАДНАННЯ

Анотація. *Розглянуто спосіб використання технології динамічного зв'язку програмних модулів для створення програмного застосунку, призначеного для розрахунку перетворювачів напруги для комп'ютерного обладнання. Розроблена динамічно-зв'язана бібліотека підтримує вісім найбільш поширених схем силової частини перетворювачів та дозволяє розраховувати усі необхідні параметри та характеристики. Головною перевагою розробленого програмного застосунку є можливість легкої інтеграції із системами автоматизованого проєктування комп'ютерного обладнання.*

Перетворювачі електричної енергії є невід'ємною частиною сучасних комп'ютерних засобів. Частіше за все, комп'ютерне обладнання містить перетворювачі, що збільшують, зменшують або змінюють полярність (інвертують) рівень первинної напруги, використання яких обумовлене особливостями сучасних електронних компонентів, джерел електричної енергії, а також жорсткими вимогами до технічних параметрів комп'ютерного обладнання – у першу чергу, до рівня енергозбереження.

Незважаючи на те, що особливості проєктування перетворювачів напруги доволі широко висвітлені у відомій літературі [1], і наразі існує певна кількість спеціалізованого програмного забезпечення, призначеного для їх розрахунку і дослідження [2], готові програмні модулі, які можна було б швидко інтегрувати в системи автоматизованого

проєктування комп'ютерних засобів, наразі відсутні. Цей і обумовило мету роботи, яка полягає в розробці програмного модуля для розрахунку перетворювачів напруги, головною особливістю якого є проста інтеграції в системи, призначені для автоматизованого проектування комп'ютерного обладнання.

На сьогоднішній день існує певна кількість методів практичної реалізації відомих математичних моделей, за допомогою яких можна проєктувати перетворювачі напруги. Найбільш простим рішенням є створення прикладних файлів (модулів) у програмних пакетах, призначених для математичних розрахунків або моделювання електричних схем, наприклад, Mathcad, LabView, або Proteus. Головною перевагою такого підходу є наявність потужного дослідницького інструментарію, за допомогою якого можна швидко досягти поставленої мети. Однак отриманий файл можна використовувати тільки в материнському програмному середовищі, тому інтеграція створеного застосунку з іншими системами автоматизованого проєктування буде утрудненою.

Іншим рішенням поставленої задачі є створення окремого спеціалізованого програмного забезпечення із власним інтерфейсом та віртуальними інструментами для проєктування. Завдяки наявності повного доступу до вихідного коду можна реалізувати інтерфейс з будь-якою існуючою системою автоматизованого проєктування, що є безсумнівною перевагою такого підходу. Проте через необхідність залучення для подібного проєкту цілої команди висококваліфікованих фахівців-програмістів часові та фінансові витрати на його реалізацію будуть найбільшими.

Найбільш придатним варіантом вирішення поставленої задачі є створення спеціалізованого програмного модуля без власного інтерфейсу і мінімальною кількістю додаткових інструментів. При такому підході, з одного боку, не потрібно витрачати час та кошти на створення складних у розробці користувацьких інтерфейсів, а з іншого – забезпечити необхідну якість та точність розрахунків.

Найбільш придатною технологією для вирішення поставленої задачі є технологія динамічного зв'язку програмних модулів, яка використовується в операційних системах Windows. При використання цієї технології прикладний програмний модуль реалізовується у вигляді динамічно-зв'язаної бібліотеки (DynamicLinkLibrary, DLL). Така технологія активно використовується в операційних системах Windows, оскільки за допомогою динамічного зв'язкуможна зменшити витрати оперативної пам'яті як програмних застосунків, так і операційної системи.

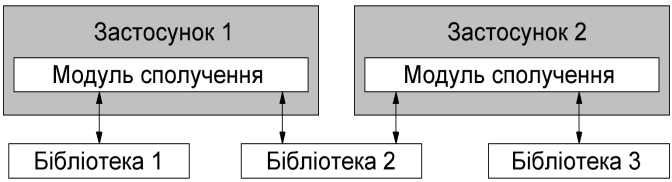


Рисунок 1 – Технологія динамічно-зв'язаних бібліотек

Головною перевагою створення модулю для розрахунку перетворювачів напруги у вигляді динамічно-зв'язаної бібліотеки є малі фінансові та часові витрати на створення кінцевого програмного застосунку. У цьому випадку, уся увага програміста приділяється реалізації прикладних математичних функцій, без відволікання на типові задачі, які вже реалізовані у системі автоматизованого проєктування комп'ютерного обладнання.

Наразі створено програмне забезпечення, яке підтримує вісім найбільш поширених схем перетворювачів (понижувальна, підвищувальна, інвертувальна, із прямим та зворотним увімкненням діода, із виводом середньої точки трансформатора, підмостова та мостова) з можливістю модифікації кожної схеми, у тому числі і з можливістю

використання автотрансформаторного увімкнення дроселя. За допомогою створеної бібліотеки можна розрахувати усі головні параметри перетворювача: регулювальні характеристики, миттєві, середні та діючі значення напруг та струмів в усіх елементах силової частини (накопичувальні дроселі, комутувальні елементи, вхідні та вихідні конденсатори), величину статичних та динамічних втрат енергії в елементах силової частини, а також енергетичні характеристики (потужність втрат, коефіцієнт корисної дії тощо).

Висновки.Створена динамічно-зв'язана бібліотека для розрахунку перетворювачів напруги може стати простим та корисним інструментом для проєктування комп'ютерного обладнання, що відповідає усім сучасним нормам. Головною перевагою розробленого програного забезпечення є можливість легкої інтеграції із існуючими системами автоматизованого проєктування комп'ютерного обладнання, яке забезпечується використанням технології динамічного зв'язку програмних модулів.

Література

1. Zehendner M., Ulmann M. Power Topologies Handbook. Texas Instruments, 2016. 216c.

2. Kadatskyy A.F., Rusu A.P. Determination of the necessary inductor core dimensions for switching electrical energy converters.*Наукові праці ОНАЗ ім. О.С. Попова*. 2018. №1. С.125-134.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056.5

Філіпенко Н.О., бакалавр Національного університету «Одеська політехніка»
filipenko.8895204@stud.op.edu.ua
Науковий керівник:
Кобозєва А.А., д.т.н., проф..

РОЗРОБКА СТЕГАНОГРАФІЧНОГО МЕТОДА, ЗАСНОВАНОГО НА ЗБУРЕННЯХ СИНГУЛЯРНИХ ЧИСЕЛ БЛОКІВ КОНТЕЙНЕРА

Анотація: *Представлено новий стеганографічний метод, спрямований на подолання основного недоліку традиційного методу модифікації найменшого значущого біту (LSB-методу), який залишається найпоширенішим на сьогодні, - чутливості до атак проти вбудованого повідомлення. Стійкість запропонованого методу досягається шляхом використання для стеганоперетворення області сингулярного розкладання матриць блоків контейнера, де вбудова додаткової інформації відбувається в найбільші сингулярні числа.*

З розвитком цифрових технологій і зростанням обсягів інформації, що передається, зберігається, оброблюється, питання її захисту стає усе більш актуальним. Сучасний захист інформації передбачає комплексність та системність при його організації та включає нормативно-правові, організаційні, фізичні, криптографічні та інші засоби для його організації.

На сьогоднішній день провідні позиції в інформаційній безпеці займає стеганографія, де приховується сам факт наявності секретного повідомлення. Серед значної кількості існуючих стеганографічних методів, що використовуються в сучасних стеганографічних системах, залишається метод модифікації найменшого значущого біту (LSB) завдяки його простоті, можливості забезпечення великої пропускної спроможності прихованого каналу зв'язку при збереженні надійності сприйняття формованого стеганоповідомлення, порівняно малій обчислювальній складності. Але LSB-метод є нестійким до будь-яких атак проти вбудованого повідомлення, що не дозволяє використовувати його у тих випадках, де такі атаки в каналі зв'язку є ймовірними, залишаючи актуальним питання підвищення стійкості відповідної стеганографічної системи, зокрема шляхом розробки нових стеганометодів, що використовують ідеї LSB-методу.

Метою роботи є підвищення стійкості стеганографічної системи до атак проти вбудованого повідомлення шляхом розробки стеганографічного методу, заснованого на принципах роботи методу модифікації найменшого значущого біта.

Об'єктом дослідження є процеси стеганографічного вбудування даних у цифрові зображення.

Предметом дослідження є методи вбудовування даних на основі збурення сингулярних чисел блоків.

Останнім часом для рішення задач захисту інформації добре зарекомендував себе загальний підхід до аналізу стану інформаційних систем (ЗПАІС), заснований на матричному аналізі та теорії збурень [1], згідно з яким будь-які перетворення інформаційної системи, зокрема системи захисту інформації, частковим випадком якої є стеганографічна система, формально представляються у вигляді сукупності збурень сингулярних чисел і сингулярних векторів (блоків) матриці, що ставиться у відповідність інформаційній системі. Саме цей підхід використано в роботі для розробки стеганографічного методу.

Ідея розробки полягає в тому, щоб застосувати метод LSB не в просторовій області контейнера, як передбачає його класичний варіант, а в області сингулярного розкладання матриці (чи блоків матриці) контейнера, в якості чого в роботі використовується цифрове зображення (ЦЗ), використовуючи для стеганоперетворення найбільш стійке до збурних дій сингулярне число, отримане в результаті сингулярного розкладання. В якості додаткової інформації (ДІ), що є результатом роботи прекодера стеганографічної системи з повідомленням, що передається по прихованому каналу зв'язку, в роботі розглядається бінарна послідовність, сформована випадковим чином. Моделювання атак проти вбудованого повідомлення відбувається шляхом накладання шуму, що є традиційним в обробці цифрових зображень, зокрема процес стеганоперетворення також можна розглядати як результат накладання деякого шуму на контейнер. В роботі в якості збурних дій не розглядаються пуассонівський шум та шум «сіль-перець», оскільки їх застосування приводе до порушення надійності сприйняття стеганоповідомлення, що не є припустимим для самого порушника, а використовуються гауссівський і мультиплікативний шуми з різними параметрами.

Основні кроки запропонованого стеганометоду виглядають наступним чином.

Вбудова додаткової інформації

Крок 1. ЦЗ з матрицею F розбивається стандартним чином на непересічні $l \times l$-блоки, довільний з яких позначимо B.

Крок 2. (*Вбудова додаткової інформації*)

Для кожного блоку B, задіяного в процесі стеганоперетворення у відповідності з секретним ключем:

2.1. Побудувати сингулярне розкладання [2]

$$B = USV^T, \qquad (1)$$

де U, V - ортогональні $l \times l$-матриці лівих і правих сингулярних векторів блоку B, $S = diag(\sigma_1, \sigma_2, ..., \sigma_l)$ - діагональна матриця сингулярних чисел, за допомогою якого визначити сингулярні числа σ_1, … , σ_l B;

2.2. Нехай p - черговий біт ДІ, який вбудовується в черговий блок B. Для цього σ_1 округлюється до найближчого цілого числа, переводиться в двійкову систему числення. Четвертий з кінця біт в двійковому представленні σ_1 замінюється на p, після чого модифіковане бінарне представлення повертається в десяткову форму. Отримаємо збурене значення максимального сингулярного числа блоку - $\overline{\sigma}_1$.

2.3. (*Відновлення блоку $\overline{B}$ стеганоповідомлення*)

$$\overline{B} = U\overline{S}V^T$$

де $\overline{S} = diag(\overline{\sigma}_1, \sigma_2, ..., \sigma_l)$.

Результат – стеганоповідомлення з матрицею $\overline{F}$.

Декодування додаткової інформації

Крок 1. ЦЗ-стеганоповідомлення з матрицею $\overline{\overline{F}}$, для якої в загальному випадку $\overline{\overline{F}} \neq \overline{F}$, оскільки стеганоповідомлення ймовірно піддається атаці проти вбудованого повідомлення, розбивається стандартним чином на непересічні $l \times l$-блоки, довільний з яких позначимо $\overline{\overline{B}}$.

Крок 2. (*Декодування додаткової інформації*)

Для кожного блоку $\overline{\overline{B}}$, задіяного в процесі стеганоперетворення у відповідності з секретним ключем:

2.1. Побудувати сингулярне розкладання (1): $\overline{\overline{B}} = \overline{\overline{U}}\,\overline{\overline{S}}\,\overline{\overline{V}}^T$, за допомогою якого визначити сингулярні числа $\overline{\overline{\sigma}}_1$, $\overline{\overline{\sigma}}_2$, …, $\overline{\overline{\sigma}}_l$;

2.2. Нехай $\overline{p}$ - черговий біт додаткової інформації, який декодується з чергового блоку $\overline{\overline{B}}$. Для цього $\overline{\overline{\sigma}}_1$ округлюється до найближчого цілого числа, переводиться в двійкову систему числення; $\overline{p}$ покладається рівним четвертому з кінця біту в двійковому представленні $\overline{\overline{\sigma}}_1$.

Результат – бітова послідовність, що відображає додаткову інформацію.

Отримана послідовність бітів порівнюється з оригінальною послідовністю, що була вбудована. Помилки декодування визначаються як відсоток невідповідних бітів між отриманою послідовністю і оригінальною.

Оцінка ефективності розробленого методу відбувалася шляхом обчислювального експерименту, в якому було задіяно 100 ЦЗ в різних форматах збереження, отриманих професійними та непрофесійними відеокамерами, різної освітленості, контрастності тощо. Отримані наступні оцінки ефективності: в умовах накладання на формовані стеганоповідомлення гауссівського шуму кількість помилок при декодуванні ДІ при дисперсії $D \le 0.0009$ не перевищує 41% , при накладанні мультиплікативного шума при $D \le 0.0009$ - не перевищує 22%.

Висновки. В роботі вирішено важливу практично-прикладну задачу підвищення стійкості стеганографічної системи до атак проти вбудованого повідомлення шляхом розробки нового стеганографічного методу, заснованого на принципах роботи LSB-методу та результатах аналізу властивостей збурень сингулярних чисел блоків матриці цифрового зображення в умовах додаткових збурних дій.

В ході розробки стеганографічного методу були отримані наступні результати:

- Визначена область блоків зображення-контейнера для вбудови ДІ – максимальні сингулярні числа, отримані шляхом сингулярного розкладання, яка дала можливість підвищити стійкість розробленого методу до атак проти вбудованого повідомлення в порівнянні з LSB-методом;
- Обгрунтована доцільність моделювання атак проти вбудованого повідомлення за допомогою накладання шумів з різними параметрами та обрані самі шуми: гауссівський та мультиплікативний;
- Обгрунтована локалізація четвертого з кінця біта двійкового представлення округленого до найближчого цілого числа значення максимального сингулярного числа блоку цифрового зображення для вбудови біта ДІ, що дало можливість забезпечити як стійкість до атак проти вбудованого повідомлення формованого стеганоповідомлення, так і його надійність сприйняття;
- Практично підтверджено гіпотезу про важливість вибору формату зображення-контейнера. Формат TIFF забезпечує високу точність та стійкість до шумів, тоді як формат JPEG є більш економічним з точки зору обсягу збережених даних, але виявляється більш чутливим до додавання шуму. Різниця похибок при декодуванні ДІ для контейнерів у форматі JPEG та TIFF - 7%.

В найгіршому випадку ($D = 0.0009$) ефективність декодування ДІ в розробленому методі в порівнянні з методом LSB, і , як наслідок, стійкість стеганографічної системи до атак проти вбудованого повідомлення, підвищена в умовах гауссівського шуму на 18%, в умовах мультиплікативного – на 56%.

Література
1. Кобозєва А.А., Хорошко В.О. Аналіз інформаційної безпеки: монографія. К.: ДУІКТ, 2009. 251 с.
2. Bergman C. Unitary embedding for data hiding with the SVD / C.Bergman, J.Davidson // Security, steganography and watermarking of multimedia contents VII, SPIE. — 2005. — Vol.5681. — P.619—630.

УДК 004.056.5

Колесник І.О., бакалавр Національного університету «Одеська політехніка»
diguerra523@gmail.com
Науковий керівник:
Кобозєва А.А., д.т.н., проф..

РОЗРОБКА ТЕОРЕТИЧНОГО БАЗИСУ СТЕГАНОМЕТОДУ, ЗАСНОВАНОГО НА ЗБУРЕННЯХ СИНГУЛЯРНИХ ЧИСЕЛ

Анотація: *Ефективність забезпечення захисту інформації, зокрема стеганографічного, головним чином залежить від теоретичного базису, який покладений в основу використовуваних методів та алгоритмів. В роботі з метою створення теоретичного базису стеганографічного методу, стійкого до атак проти вбудованого повідомлення, проведені дослідження властивостей сингулярних чисел блоків матриці цифрового зображення в умовах додаткових збурних дій. Визначені сингулярні числа блоків цифрового зображення, які мають найменшу чутливість до змін вхідних даних. Збурення саме цих сингулярних чисел в результаті стеганоперетворення повинно забезпечити стійкість до збурних дій відповідного стеганографічного методу*

З кожним днем разом з поширенням та впровадженням інформаційних технологій у всі сфери життя суспільства, створення значного обсягу конфіденційних та критично важливих даних у цифровому вигляді зростає пріоритет задач інформаційної безпеки, зокрема стеганографії. Ефективність забезпечення захисту інформації в будь-якій галузі, головним чином залежить від того теоретичного базису, який покладено в основу використовуваних методів та алгоритмів. Огріхи в теоретичному базисі можуть призвести до недієздатності використовуваного методу в критичний момент і, як наслідок, до катастрофічних наслідків як для окремої людини, фірми, підприємства, так суспільства в цілому. Основна увага в роботі при розробці базису приділяється забезпеченню стійкості відповідного методу до атак проти вбудованого повідомлення.

Серед цифрових контентів на сьогодні найбільше поширення отримали цифрові зображення (ЦЗ), які використовуються в роботі, та цифрові відео, при цьому очевидно, що цифрове відео може розглядатися як послідовність кадрів-зображень, що робить можливим застосовувати отримані для зображень результати для відео послідовностей.

Метою роботи є розробка теоретичного базису, що забезпечить для стеганографічних методів, розроблених на його основі, стійкість до атак проти вбудованого повідомлення, шляхом дослідження властивостей сингулярних чисел блоків матриці ЦЗ в умовах додаткових збурних дій.

Об’єктом дослідження є процес забезпечення нечутливості цифрового контенту до збурних дій.

Предметом дослідження є характер збурень сингулярних чисел блоків цифрового зображення в умовах стеганографічних атак проти вбудованого повідомлення.

Для задач стеганографії добре зарекомендував себе загальний підхід до аналізу стану інформаційних систем (ЗПАІС), заснований на матричному аналізі та теорії збурень [1], відповідно з яким будь-які зміни, що відбуваються з системою, зокрема системою захисту інформації, формально можуть бути представлені у вигляді сукупності збурень

повного набору формальних параметрів – сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) матриці, що ставиться у відповідність інформаційній системі. ЗПАІС є перспективним і таким, удосконалення якого дасть можливість покращити властивості тих систем захисту інформації, зокрема стеганографічних систем, які на ньому базуються. Одним з напрямів такого удосконалення є детальне дослідження властивостей сингулярних чисел в сенсі їх чутливості до збурних дій, що робиться в роботі.

Поняття стійкості стеганоалгоритму до атак проти вбудованого повідомлення нерозривно пов'язано з поняттям чутливості параметрів, що визначають контейнер, стеганоповідомлення, до збурних дій. Від характеру реакції цих параметрів на збурну дію (атаку проти вбудованого повідомлення) буде залежати ефективність декодування вбудованої інформації, кількість помилок, що виникають в результаті змін в матриці стеганоповідомлення при атаці.

Всі СНЧ будь-якої матриці F, зокрема матриці цифрового зображення, є нечутливими до збурних дій, чи добре обумовленими, у відповідності з формулою [2]:

$$\max_i \left|\sigma_i(F) - \sigma_i(F + \Delta F)\right| \le \left\|\Delta F\right\|_2 \qquad (1)$$

де $\sigma_i(F)$, $\sigma_i(F + \Delta F)$ - СНЧ поданої F та збуреної $F + \Delta F$ матриць відповідно, ΔF – матриця збурення, $\|\cdot\|_2$ – спектральна матрична норма.

Але все ж таки різні СНЧ матриці/блоку матриці ЦЗ будуть реагувати по-різному на одну й ту саму збурну дію, не перевищуючи величини $\left\|\Delta F\right\|_2$, залишаючи актуальною задачу виявлення найстійкіших з них.

Зазначимо, що останнім часом переважна більшість розроблюваних стеганографічних методів є блоковими, тобто такими, що здійснюють вбудову/декодування додаткової інформації поблоково. Це дає можливість забезпечити порівняно незначну обчислювальну складність методу у випадку його послідовної реалізації, а також дає простий спосіб розпаралелювання такого методу, оскільки обробка кожного блоку відбувається незалежно. Враховуючи цей факт, подальше дослідження проводиться для блоків матриці ЦЗ, отриманих шляхом її стандартної розбивки.

В ході дослідження було проведено обчислювальний експеримент, в якому було задіяно 100 оригінальних ЦЗ різного формату (з втратами (JPEG) та без втрат (TIFF)), різного розміру, отриманих професійними та непрофесійними відео камерами. В ході експерименту матриця F оригінального ЦЗ розбивалася на неперетинні $l \times l$-блоки. Для кожного блоку окремо будувалося сингулярне розкладання [2]:

$$B = USV^T, \qquad (2)$$

де U, V - ортогональні $l \times l$-матриці лівих і правих СНВ блоку B, $S = diag(\sigma_1, \sigma_2, ..., \sigma_l)$ - діагональна матриця сингулярних чисел; в результаті якого отримувалися СНЧ блоку $\sigma_1,\ \sigma_2, ..., \sigma_l$. Після отримання СНЧ оригінальне ЦЗ піддавалося збурній дії, в якості якої в роботі використовувалися різні шуми (гауссівський, мультиплікативний) з різними параметрами. Використання саме шумів, зокрема гауссівського, є традиційним при моделюванні збурних дій на ЦЗ, навіть стеганоперетворення. В ході експерименту збурене зображення зберігалося в форматі без втрат, після чого розбивалося на $l \times l$-блоки, для кожного з яких будувалося сингулярне розкладання (2), за допомогою якого визначалися СНЧ кожного блоку ЦЗ після атаки: $\overline{\sigma}_1,\ \overline{\sigma}_2, ..., \overline{\sigma}_l$. Збурення $\Delta\sigma_i$ для кожного СНЧ в кожному блоці визначалося за формулою: $\Delta\sigma_i = \left|\sigma_i - \overline{\sigma}_i\right|$, $i = \overline{1,l}$, після чого розраховувалися середні значення $\Delta\sigma_i$ по всім блокам ЦЗ.

В результаті експерименту встановлено:

- Найбільш стійкими до збурних дій в блоках ЦЗ є максимальне СНЧ σ_1 і декілька (два σ_{l-1}, σ_l) найменших СНЧ, які встановлюють найбільш сприятливу зону (НСЗ) для вбудови додаткової інформації при стеганоперетворенні, стійкому до атак проти вбудованого повідомлення;
- Характер зміни середніх значень збурень СНЧ блоків не залежить
  - від формату ЦЗ,
  - від конкретних характеристик ЦЗ,
  - від характеристик збурної дії, якій піддається ЦЗ,
  - від розміру *l* використовуваного блоку,

тобто НСЗ для будь-якого ЦЗ-контейнера (з втратами, без втрат) при довільній збурній дії визначається як σ_1, σ_{l-1}, σ_l.

Важливо, що означена картина характеру збурень СНЧ в цілому зберігається для кожного блоку ЦЗ: звісно кількісно залежність $\Delta\sigma_i$ від номеру *i* може відрізнятися від залежності для середніх значень, але якісно зберігається та ж сама концепція – найменших змін зазнають перше та декілька останніх СНЧ.

Висновки. В роботі визначено найбільш сприятливу для вбудови додаткової інформації при стеганоперетворенні, стійкому до атак проти вбудованого повідомлення, зону, яка є актуальною для будь-якого ЦЗ-контейнера (з втратами, без втрат) при довільній збурній дії: СНЧ σ_1, σ_{l-1}, σ_l блоків ЦЗ, отриманих шляхом стандартної розбивки.

Отримані результати свідчать про те, що використання НСЗ є перспективним для розробки нових стеганометодів.

Література

3. Кобозєва А.А., Хорошко В.О. Аналіз інформаційної безпеки: монографія. К.: ДУІКТ, 2009. 251 с.
4. Demmel J. Computing the singular value decomposition with high relative accuracy / J.Demmel, M.Gu, S.Eisenstat, I.Slapnicar, K.Veselic // Linear Alg. Appl. — 1999. — Vol.299. — P. 21—80.

УДК 004.056.5

Єнакієв Б.Г., бакалавр Національного університету «Одеська політехніка»
yenakiiev.8864773@stud.op.edu.ua
Науковий керівник:
Кобозєва А.А., д.т.н., проф..

РОЗРОБКА МЕТОДУ ВИЯВЛЕННЯ ФОТОМОНТАЖУ В ЦИФРОВИХ ЗОБРАЖЕННЯХ

Анотація: *Проблема виявлення неоригінальних цифрових контентів, зокрема зображень, що є результатом фотомонтажу, залишається актуальною. В роботі представлений новий експертний метод, який на основі аналізу властивостей матриці найменших сингулярних чисел блоків, що ставиться у відповідність цифровому зображенню, дає змогу відокремити оригінальне зображення від такого, цілісність якого порушена, а також локалізувати область зображення, що містить в собі «вклейку» - частину іншого зображення. Представлений метод базується на встановлених відмінностях властивостей матриці найменших сингулярних чисел блоків для цифрових зображень, що зберігаються в різних форматах – з втратами та без втрат.*

Запропонований метод забезпечує підвищення ефективності виявлення наявності фотомонтажу в порівнянні з сучасним аналогом.

Ми живемо в надзвичайно цифровізованому світі, і часом буває складно відрізнити брехню від реальності. Зараз Україна знаходиться у стані війни проти агресії Росії, і ця проблема стала ще більш актуальною на фоні поширення різноманітних фото- та відеофейків, довіра яким може створювати хибне розуміння світу та ситуації загалом.

Одним з найпоширеніших на сьогодні та таким, що легко реалізується за допомогою існуючих графічних редакторів (PhotoShop, Gimp та ін..) способів фальсифікації – порушення цілісності цифрових зображень є фотомонтаж [1], коли одне цифрове зображення (ЦЗ) створюється з декількох. Не дивлячись на те, що задача виявлення фотомонтажу є предметом дослідження вчених в галузі інформаційної безпеки по всьому світу, вона не є остаточно вирішеною, не існує універсальних експертних методів, які в змозі навіть детектувати наявність «чужерідної» частини – вклейки у будь-якому випадку фотомонтажу.

Метою роботи є підвищення ефективності процесу виявлення порушення цілісності цифрового зображення шляхом розробки методу виявлення факту фотомонтажу.

Об'єктом дослідження є процеси порушення цілісності в ЦЗ.

Предметом дослідження є методи виявлення фотомонтажу в ЦЗ.

В роботі передбачається, що фотомонтаж формується наступним чином. Використовуються два ЦЗ в різних форматах збереження: з/без втрат. Одне з них відіграє роль основного, а друге такого, з якого береться частина, яка переноситься на перше зображення, створюючи на ньому заміщуючу область – вклейку. Для виявлення результатів фотомонтажу в таких умовах ключовим моментом є наявність інструменту для відокремлення ЦЗ в різних форматах збереження.

Не обмежуючи спільності міркувань, для простоти подальшого викладу будемо вважати, що формально будь-яке ЦЗ під час експертизи представляється одною матрицею яскравості пікселів *F*. Якщо ЦЗ є кольоровим, то, залежно від схеми збереження, *F* може бути або матрицею яскравості (YUV), або одною з матриць кольорів (RGB). Матриці *F* поставимо у відповідність матрицю *M* найменших сингулярних чисел блоків (МНСБ) за наступним правилом. Матриця *F* розбивається попередньо на $l \times l$-блоки. Враховуючи, що найпопулярнішими і найпоширенішими алгоритмами стиску є JPEG та JPEG2000, а задача полягає в розпізнаванні цих алгоритмів і відокремленні від алгоритмів збереження ЦЗ без стиску, в роботі $l = 8$.

В МНСБ *M*, розмір якої $\left[\frac{n}{8}\right] \times \left[\frac{n}{8}\right]$, кожний елемент відповідає блоку ЦЗ, визначає кількість сингулярних чисел (СНЧ) у відповідному блоці *B*, менших заданого порога *T*. При цьому СНЧ *B* визначаються за допомогою сингулярного розкладання:

$$B = U \Sigma V^T, \qquad (1)$$

де U, V - ортогональні матриці, стовпці яких u_i, v_i, $i = \overline{1,8}$, визначають ліві і праві сингулярні вектори *B* відповідно, а $\Sigma = diag(\sigma_1, \sigma_2, ..., \sigma_8)$, де $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_8 \geq 0$ - СНЧ. СНЧ разом з відповідними лівим і правим сингулярними векторами (σ_i, u_i, v_i), $i = \overline{1,8}$, утворюють сингулярні трійки для блоку ЦЗ.

Відомо, що стиск ЦЗ з втратами приводить до зменшення/знищення високочастотної (можливо, і середньочастотної, що залежить від коефіцієнту стиску) складової зображення. При цьому високочастотним складовим відповідають, головним чином, сингулярні трійки зображення (σ_i, u_i, v_i) з найменшими СНЧ, то стиск приводе до

зменшення найменших СНЧ ЦЗ (блоків ЦЗ), можливо, аж до нуля. Хоча на практиці «чистих» нулів, як правило, не буде, оскільки в процесі обчислень, які відбуваються з дійсними СНЧ в системі чисел з плаваючою точкою, виникає обчислювальна похибка, і відповідні СНЧ будуть порівнянними з похибкою округлення, що повинно відбитися на значеннях МНСЧ. Очевидно, що МНСЧ для ЦЗ у різних форматах зберігання (з/без втрат) будуть відрізнятися одна від одної: для блоків ЦЗ в форматі без втрат їх, як правило, менше, ніж в блоках ЦЗ в форматі з втратами.

Основні кроки методу виявлення фотомонтажу виглядають наступним чином:

Крок 1. Матриця F ЦЗ розміром $n \times m$, що піддається експертизі цілісності, розбивається стандартним чином на непересічні 8×8-блоки B_{ij}, де i - номер блокового рядка, j - номер блокового стовпця, на перерізі яких знаходиться блок, $i = \overline{1, \left[\frac{n}{8}\right]}$, $j = \overline{1, \left[\frac{m}{8}\right]}$ (відлік починається з лівого верхнього кута).

Крок 2. (Побудова матриці M найменших сингулярних чисел блоків).

Для визначення елемента m_{ij} $i = \overline{1, \left[\frac{n}{8}\right]}$, $j = \overline{1, \left[\frac{m}{8}\right]}$ матриці M розміру $\left[\frac{n}{8}\right] \times \left[\frac{m}{8}\right]$:

2.1. Побудувати сингулярне розкладання (1) для відповідного блоку $B_{ij}: B_{ij} = U \Sigma V^T$ з якого визначити СНЧ B_{ij}: $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_8 \geq 0$.

2.2. Визначити кількість $K \in \{0,1,2,3,4,5,6,7,8\}$ СНЧ B_{ij}, для яких має місце: $\sigma_i < T$, де T – порогове значення, що визначається експериментальним шляхом.

2.3. Визначення елемента m_{ij}: $m_{ij} = K$.

Крок 3. Визначити: $X_a = \max\limits_{i,j} m_{ij}$ - максимальне значення елементів МНСЧ *M*.

Крок 4. З матриці M найменших сингулярних чисел формується множина X елементів, значення яких дорівнюють X_a.

Крок 5. Перевірка загальної кількості елементів множини X

Якщо

$|X| < 5$,

де $|X|$ - потужність множини X,

то ЦЗ не містить вклейку, *кінець експертизи* (перехід на крок 10)

Крок 6. Побудовафрагментів O матриці M – околів кожного значення $m_{ij} \in X$.

Крок 7. З побудованих на кроці 6 визначитифрагмент $\overline{O}$, який має найбільшу кількість елементів множини *X*.

Крок 8. Розрахунок значень *S*та *P* для подальшого аналізу обраного фрагменту $\overline{O}$:

$S = |A_1 - A_2|$,

де A_1 – середнє арифметичне значень елементів матриці M, A_2 – середнє арифметичне значень елементів фрагменту O;

$$P = \frac{X_l}{X_g} \cdot 100\%$$

де X_l – кількість елементів X_a у фрагменті O, X_g – кількість елементів X_a у матриці M.

Крок 9. (Експертний висновок)

Якщо

$$S > 0.2$$

То Ідентифіковано вбудований фрагмент
кінець експертизи (перехід на крок 10)

Якщо

$$P > 60\%$$

То Ідентифіковано вбудований фрагмент
кінець експертизи (перехід на крок 10)

Якщо

$$(S < 0.2)\&(P < 60\%)$$

То ЦЗ чисте

Крок 10. Кінець експертизи

Експериментально встановлене порогове значення становить: T=0.3.

Для оцінки ефективності розробленого метода виявлення фотомонтажу був проведений обчислювальний експеримент, в якому було задіяно 100 оригінальних ЦЗ, отриманих як професіональними, так і не професіональними відеокамерами, які піддавалися фотомонтажу. Оригінальні і спотворені ЦЗ піддавалися експертизі за допомогою розробленого методу. Кількісними результатами проведення експерименту стали помилки 1-го (спотворене ЦЗ ідентифікувалося як оригінальне) і 2-го (оригінальне ЦЗ ідентифікувалося як спотворене) роду. Для порівняльної оцінки ефективності був обраний сучасний метод-аналог, запропонований в [2], оскільки він має подібну до розробленого область застосування і схожий математичний апарат, заснований на аналізі СНЧ блоків матриці ЦЗ.

Результати проведеного обчислювального експерименту представлені в табл.1 (тут помилки 1-го і 2-го роду для методу [2] рахувалися як середні значення відповідних помилок для всіх розглянутих в роботі [2] варіантів, де фотомонтаж був побудований з ЦЗ в різних (з/без втрат) форматах збереження).

Табл.3.1. Показники ефективності розробленого методу

Метод	Помилки 1-го роду (%)	Помилки 2-го роду (%)
Метод, запропонований в [2]	23	3
Розроблений метод	14	8

Висновки. В роботі вирішена важлива науково-практична задача підвищення ефективності процесу виявлення порушення цілісності ЦЗ шляхом розробки методу виявлення факту фотомонтажу. Метод розроблений на основі аналізу властивостей МНСЧ, множини X елементів МНСЧ, що мають максимальні значення, та околів елементів з множини X.

Показники ефективності запропонованого методу становлять: 14 і 8% - помилки 1-го і 2-го роду відповідно, що дозволило підвищити ефективність виявлення результатів фотомонтажу на 39% (в сенсі помилок 1-го роду) в порівнянні з сучасним аналогом, що має аналогічну область застосування та схожий математичний базис (заснований на аналізі СНЧ блоків).

В ході розробки метода виявлення фотомонтажу в ЦЗ досліджено властивості матриці найменших сингулярних чисел блоків, що ставиться у відповідність ЦЗ, для різних форматів (з втратами, без втрат) збереження, в результаті чого обґрунтовано і практично підтверджено:

- значення елементів МНСЧ для ЦЗ в форматі з втратами в сукупності перевищують значення елементів МНСЧ для ЦЗ в форматі без втрат;
- гістограми значень елементів МНСЧ для зображень без втрат не можуть мати моду, що перевищує 2; гістограми значень елементів МНСЧ для зображень з втратами не можуть мати моду, що дорівнює 0;
- у випадку моди гістограми значень елементів МНСЧ 1 або 2 висновок про формат ЦЗ залежить від максимального значення МНСЧ.

Література

1. Moghaddasi Z., Jalab H.A., Noor R.M. Image splicing forgery detection based on low-dimensional singular value decomposition of discrete cosine transform coefficients. *Neural Computing and Applications*. 2019. 31. P. 7867–7877.

2. Зорило В.В. Метод підвищення ефективності виявлення порушення цілісності цифрового зображення: дис. канд. техн. наук: 05.13.21/ Зорило Вікторія Вікторівна. – К., 2013. – 127 с.

UDC 004.056.55

CRYPTOGRAPHIC PROTOCOL KEY EXCHANGE ON EXTENDED FIELD ELLIPTIC CURVESKOBLITZ

Onatskiy Oleksiy,
Candidate of technical sciences, associate professor,
International Humanitarian University, Odessa, Ukraine
onatsky@meta.ua
Zharova Oksana,
Candidate of physical and mathematical sciences, associate professor,
Odessa polytechnic state university, Odessa, Ukraine
Ksenia.gds@gmail.com
Dygalo Yevhen,
Professional qualification computer system analyst,
Information technology development studio, Kyiv, Ukraine
dygaloevg@gmail.com

Abstract. *One of the methods for increasing the cryptographic strength of asymmetric encryption algorithms is to increase the size of parameters when performing modular transformations (of the order of 1024 or more bits), which in turn leads to an increase in the computational complexity of cryptographic transformations and a decrease in encryption speed. The resolution of this contradiction was found through the implementation of asymmetric encryption algorithms on elliptic curves in Galois fields. The article proposes a cryptographic key exchange protocol based on an extension of Koblitz elliptic curve fields.*

Key distribution is the most responsible key management process. The following requirements apply to it:
1) efficiency and accuracy of distribution;
2) secrecy of key distribution.

Distribution of keys between users is implemented by two methods [1]:
1) by building one or more Key Distribution Center (KDC). The disadvantage is that the KDC knows who and what keys are assigned. This makes it possible to read all the messages that are in the IS, which affects the protection of the system against criminal actions;
2) direct exchange of keys between users. The challenge here is to identify and authenticate users.

In both cases, the validity of the communication session must be guaranteed.

The aim of the article is to develop a cryptographic protocol key exchangeonelliptic curvesKoblitz defined over the extension fields $GF(2^m)$.

In cryptosystems over the extended field $GF(2^m)$, the equation EC has the form [1 – 3]:

$$y^2 + xy \equiv \left(x^3 + ax^2 + b\right) \bmod \left(f(x), 2\right) \quad (1)$$

for non-supersingular curves, denote $[E(a,b), f(x)]$.

In the equation (1) if $a \in (0, 1)$ and $b = 1$, it is called Koblitz curves or anomalous binary curves. Therefore, the Koblitz curves are defined over $GF(2^m)$ by following equations:

$$y^2 + xy \equiv \left(x^3 + x^2 + 1\right) \bmod \left(f(x), 2\right);$$
$$y^2 + xy \equiv \left(x^3 + 1\right) \bmod \left(f(x), 2\right).$$

Let us define an addition operation for points from the elements of the field $GF(2^m)$. Let the coordinates of the two point's $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, be known, then the addition of $P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ is determined as follows [1 – 3]:

1) if the points P and Q belong to a non-supersingular curve, then

$$\begin{cases} x_3 \equiv \left(\lambda^2 + \lambda + x_1 + x_2 + a\right) \bmod \left(f(x), 2\right); \\ y_3 \equiv \left[\lambda\left(x_1 + x_3\right) + x_3 + y_1\right] \bmod \left(f(x), 2\right), \end{cases}$$

where $\lambda \equiv \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right) \bmod \left(f(x), 2\right)$;

2) for a $2P = 2(x_1, y_1) = (x_3, y_3)$ point that belongs to a non-supersingular curve,

$$\begin{cases} x_3 \equiv \left(\lambda^2 + \lambda + a\right) \bmod \left(f(x), 2\right); \\ y_3 \equiv \left[x_1^2 + (\lambda + 1)\, x_3\right] \bmod \left(f(x), 2\right), \end{cases}$$

where $\lambda \equiv \left(x_1 + \dfrac{y_1}{x_1}\right) \bmod \left(f(x), 2\right)$.

Consider the cryptographic protocol key exchange on EC Koblitz defined over the extension fields $GF(2^m)$, which is shown in Fig. 1.

Let $E(a, 1)$, $a \in (0, 1)$ be an elliptic curve of the field $GF(2^m)$; G – a point of this curve; n – the group order of the curve; $f(x)$ – primitive polynomial of degree m over the field $GF(2)$; k_a, k_b – the session (or personal) keys of users A and B; r_a, r_b – random number of users A and B.

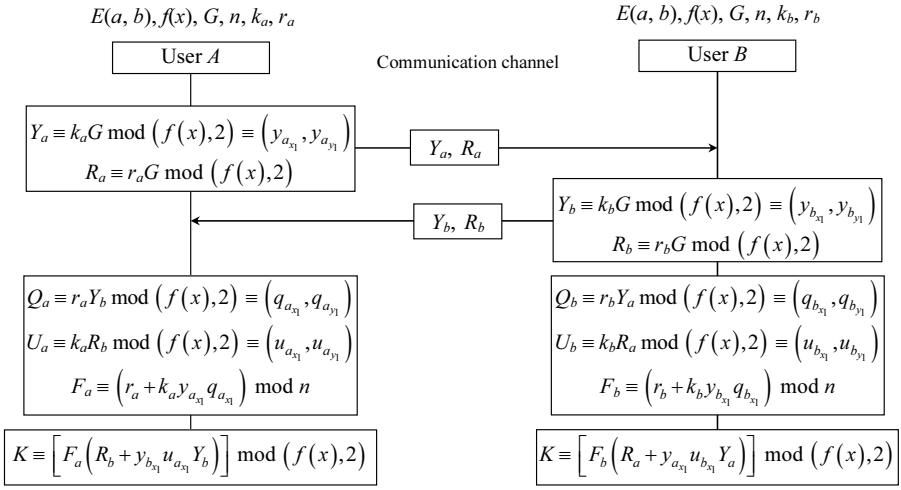


Figure 1 – Cryptographic protocol key exchange on EC

User*A* calculates the value of the public key Y_a and a random value R_a, which it sends to user*B* (calculation shown Fig. 1). User*B* calculates the value of the public key Y_b and a random value R_b, which it sends to user*A* (calculation shown Fig. 1). User*A* additionally calculates the values Q_a, U_a, F_a (calculation shown Fig. 1), which are needed to calculate the shared secret key *K*.User*B* also additionally calculates the values Q_b, U_b, F_b (calculation shown Fig. 1). Users *A* and *B* calculates shared secret key *K* (calculation shown Fig. 1).

Now users*A* and *B* have a secret key *K*known only to them, which can be used to send messages via any number of secure private-key cryptosystems.

Completeness of the cryptographic protocol key exchange:

$$K \equiv \left[F_a\left(R_b + y_{b_{x_1}} u_{a_{x_1}} Y_b\right)\right] \bmod \left(f(x),2\right) \equiv$$

$$\equiv \left[\left(r_a + k_a y_{a_{x_1}} q_{a_{x_1}}\right)\left(r_b G + k_b y_{b_{x_1}} u_{a_{x_1}} G\right)\right] \bmod \left(f(x),2\right) \equiv$$

$$\equiv \left[r_a r_b G + r_a k_b y_{b_{x_1}} u_{a_{x_1}} G + k_a r_b y_{a_{x_1}} q_{a_{x_1}} G + k_a k_b y_{a_{x_1}} y_{b_{x_1}} q_{a_{x_1}} u_{a_{x_1}} G\right] \bmod \left(f(x),2\right);$$

$$K \equiv \left[F_b\left(R_a + y_{a_{x_1}} u_{b_{x_1}} Y_a\right)\right] \bmod \left(f(x),2\right) \equiv$$

$$\equiv \left[\left(r_b + k_b y_{b_{x_1}} q_{b_{x_1}}\right)\left(r_a G + k_a y_{a_{x_1}} u_{b_{x_1}} G\right)\right] \bmod \left(f(x),2\right) \equiv$$

$$\equiv \left[r_a r_b G + k_a r_b y_{a_{x_1}} u_{b_{x_1}} G + r_a k_b y_{b_{x_1}} q_{b_{x_1}} G + k_a k_b y_{a_{x_1}} y_{b_{x_1}} q_{b_{x_1}} u_{b_{x_1}} G\right] \bmod \left(f(x),2\right).$$

Let's prove the equality of values $q_{a_{x_1}} = u_{b_{x_1}}$, $q_{b_{x_1}} = u_{a_{x_1}}$:

$$Q_a \equiv r_a Y_b \bmod \left(f(x),2\right) \equiv r_a k_b G \bmod \left(f(x),2\right) \equiv \left(q_{a_{x_1}}, q_{a_{y_1}}\right);$$

$$U_b \equiv k_b R_a \bmod \left(f(x),2\right) \equiv k_b r_a G \bmod \left(f(x),2\right) \equiv \left(u_{b_{x_1}}, u_{b_{y_1}}\right);$$

$$Q_a = \left(q_{a_{x_1}}, q_{a_{y_1}}\right) = U_b = \left(u_{b_{x_1}}, u_{b_{y_1}}\right) \Rightarrow q_{a_{x_1}} = u_{b_{x_1}};$$

$$Q_b \equiv r_b Y_a \bmod \left(f(x), 2\right) \equiv r_b k_a G \bmod \left(f(x), 2\right) \equiv \left(q_{b_{x_1}}, q_{b_{y_1}}\right);$$

$$U_a \equiv k_a R_b \bmod \left(f(x), 2\right) \equiv k_a r_b G \bmod \left(f(x), 2\right) \equiv \left(u_{a_{x_1}}, u_{a_{y_1}}\right);$$

$$Q_b = \left(q_{b_{x_1}}, q_{b_{y_1}}\right) = U_a = \left(u_{a_{x_1}}, u_{a_{y_1}}\right) \Rightarrow q_{b_{x_1}} = u_{a_{x_1}}.$$

Thus we get

$$K \equiv \left[r_a r_b G + r_a k_b y_{b_{x_1}} u_{a_{x_1}} G + k_a r_b y_{a_{x_1}} q_{a_{x_1}} G + k_a k_b y_{a_{x_1}} y_{b_{x_1}} q_{a_{x_1}} u_{a_{x_1}} G\right] \bmod \left(f(x), 2\right) \equiv$$

$$\equiv \left[r_a r_b G + k_a r_b y_{a_{x_1}} u_{b_{x_1}} G + r_a k_b y_{b_{x_1}} q_{b_{x_1}} G + k_a k_b y_{a_{x_1}} y_{b_{x_1}} q_{b_{x_1}} u_{b_{x_1}} G\right] \bmod \left(f(x), 2\right).$$

Example of the calculation key exchange protocol on over the extended field $GF(2^m)$ curves Koblitz.

Let a non-supersingular elliptic curve $E(0, 1)$ over the extended field $GF(2^{11})$ and a primitive polynomial $f(x) = x^{11} + x^2 + 1$ over the field $GF(2)$ be given, which has the form

$$y^2 + xy \equiv \left(x^3 + 1\right) \bmod \left(100000000101,\ 2\right);$$

the group order of the curve $n = 1012$; generating point $G = (111101111, 1000011111)$; user A – session (or personal) key $k_a = 639$ and random number $r_a = 258$; user B – session (or personal) key $k_b = 701$ and random number $r_b = 453$.

All calculations on the elliptic Koblitz curve are performed in binary form, but to reduce the representation of binary numbers we will use hexadecimal form numbers. Thus we have:
$n = 1012_{10} = 3F4_{16}$; $G = (111101111, 1000011111)_2 = (1EF, 21F)_{16}$;
$f(x) = 100000000101_2 = 805_{16}$; $k_a = 639_{10} = 27F_{16}$; $r_a = 258_{10} = 102_{16}$; $k_b = 701_{10} = 2BD_{16}$;
$r_b = 453_{10} = 1C5_{16}$.

All calculations key exchangeprotocol is presented in Tab. 1.

Table 1 – Example of the calculation key exchange protocol

Value	Description	Result
Y_a	27F (1EF, 21F) mod (805, 2)	(5EF, 6BC)
R_a	102 (1EF, 21F) mod (805, 2)	(7FB, 7B9)
Y_b	2BD(1EF, 21F) mod (805, 2)	(78E, 79B)
R_b	1C5 (1EF, 21F) mod (805, 2)	(10B, 2D0)
Q_a	102 (78E, 79B) mod (805, 2)	(28D, 5BC)
U_a	27F (10B, 2D0) mod (805, 2)	(78E, 15)
F_a	(102 + 27F · 5EF · 28D) mod 3F4	4B
Q_b	1C5 (5EF, 6BC) mod (805, 2)	(78E, 15)
U_b	2BD (7FB, 7B9) mod (805, 2)	(28D, 5BC)
F_b	(1C5 + 2BD · 78E · 78E) mod 3F4	DD
K user A	4B [(10B, 2D0) + 78E · 78E(78E, 79B)] mod (805, 2)	(7D6, 1F5)
K user B	DD [(7FB, 7B9) + 5EF · 28D(5EF, 6BC)] mod (805, 2)	(7D6, 1F5)

Now users A and B have a secret key

$$K = (7D6, 1F5)_{16} = (11111010110, 111110101)_2 = (2006, 501)_{10}.$$

Conclusions. The proposed protocol significantly reduces the size of parameters and increases the cryptographic strength (the computational complexity of hacking) through the use of elliptic Koblitz curve (calculations are performed in binary form). To implement the proposed protocol, we can use the recommended elliptic curves according SEC 2: Recommended Elliptic Curve Domain Parameters [4]. Software verification of the key exchange protocol and stability of the protocol against attacker attacks was performed using the OFMC and CL-AtSe AVISPA software back-ends [5, 6]. As a result of checking the proposed key exchange protocol, no known attacks were found.

References:

1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія, Харків: Видавництво «Форт», 2012. – 880 с.
2. Hankerson D., Menezes A., Vanstone S., Hankerson D. Guide to Elliptic Curve Cryptography. Springer-Verlag, 2004. – 358 p.
3. Washington L. C. Elliptic curves: number theory and cryptography. 2nd edition. Taylor & Francis Group, 2008. – 524 p.
4. SEC 2: Recommended Elliptic Curve Domain Parameters. [Electronic resource] – Mode of access: https://www.secg.org/ SEC2-Ver-1.0.pdf
5. AVISPA. [Electronic resource] – Mode of access: https://www.avispa-project.org/
6. Security Protocol Animator. [Electronic resource] – Mode of access: https://www.irisa.fr/ celtique/genet/span/

УДК 004 .056

Черемнов Максим Вікторович
аспірант,
Міжнародного гуманітарного університету
м. Одеса, Україна
cheremnovmaksym@gmail.com

ДОСЛІДЖЕННЯ МЕТОДІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Анотація. *Останніми роками біометричні методи автентифікації привернули значну увагу через їхній потенціал забезпечувати підвищену безпеку та зручність порівняно з традиційними механізмами автентифікації. Це дослідження вивчає різні методи біометричної автентифікації, їхні базові технології, сильні та слабкі сторони, а також їх застосування в різних секторах.*

Біометричне розпізнавання відноситься до автоматичного розпізнавання осіб на основі їхніх фізіологічних та/або поведінкових характеристик. Широкий спектр систем потребує надійних схем розпізнавання особи для підтвердження або визначення особи особи, яка запитує їхні послуги. Мета таких схем полягає в тому, щоб забезпечити доступ до наданих послуг законним користувачам, а не будь-кому іншому.

Не можна заперечувати інтеграцію біометричних систем у суспільство. Міжнародні аналітики очікують, що потреба в біометрії зросте в усіх галузях промисловості, а спектр її застосування розшириться.

Розвиток біометричних технологій ідентифікації особистості є актуальним, оскільки стає все більше предметів та потоків інформації, які необхідно захищати від несанкціонованого доступу. Йдеться про системи голосування, обробку електронних

платежів, кримінальне правосуддя, системи контролю доступу, системи ідентифікації особистості, інформаційну безпеку, облік робочого часу та реєстрацію відвідувачів, різноманітні соціальні проекти, що вимагають ідентифікації учасників, а також ініціативи цивільної ідентифікації (наприклад, перетин державного кордону). та надання віз для закордонних поїздок).

Які біологічні вимірювання можна вважати біометричними? Будь-які фізіологічні та/або поведінкову характеристику можна використовувати як біометричну характеристику, якщо вона задовольняє наступні вимоги [3]:

- Універсальність: у кожної людини повинна бути своя характеристика;
- Відмінність: будь-які дві особи повинні бути достатньо різними з точки зору характеристики;
- Постійність: характеристика має бути достатньо інваріантною (стосовно відповідності критеріїв) протягом певного періоду часу;
- Колекційність: характеристику можна виміряти кількісно.

Однак у практичній біометричній системі (тобто системі, яка використовує біометричні дані для особистого визнання), існує низка інших питань, які слід розглянути, зокрема:

- Продуктивність, яка стосується досяжної точності та швидкості розпізнавання, ресурсів необхідних для досягнення бажаної точності та швидкості розпізнавання;
- Прийнятність, що вказує на те, наскільки люди готові прийняти у використання конкретний біометричний ідентифікатор у повсякденному житті;
- Обхід, який відображає, наскільки легко систему можна обдурити за допомогою шахрайських методів.

Ідентифікація за відбитками пальців є найстарішим методом і найбільш широко використовується в багатьох сферах. У кожної людини є власні, неповторні відбитки пальців. Порівняння ідентифікованого відбитку пальця зеталонними що допомогає в ідентифікації особи. Коефіцієнт відповідності повинен бути не менше ніж 65% або більше [1].

Нижче наведена схема процесу біометричної автентифікації шляхом розпізнавання відбитку пальця (Рис 1). У процесі перевірки відбиток пальця людини перевірено з бази даних за допомогою алгоритмів відповідності. Також це відоме як (1:1) порівняння. Це порівняння з відбитком пальця заявника проти відбитка пальця запису (реєстрації), спочатку особа реєструє свій відбиток пальця в системі верифікації та результат показує, чи відбиток пальця, який взято з користувача зіставляється зі сховищем відбитків пальців як шаблоном бази даних або не збігається. У разі процесу ідентифікації отриманий відбиток пальця від однієї людини порівнюється з усіма відбитками пальців, які зберігаються в базі даних. Також це відоме як (1:N) відповідність. він використовується в процесі розшуку злочинців[6].

Автентифікація за відбитками пальців пропонує поєднання безпеки, зручності та економічності, що робить її популярним вибором для перевірки особи в різних програмах. Однак це не без труднощів, включаючи чутливість навколишнього середовища, ризики безпеки, проблеми конфіденційності та потенційні проблеми з точністю. Збалансування цих плюсів і мінусів має вирішальне значення для ефективного й етичного впровадження систем автентифікації за відбитками пальців.

Технологія розпізнавання облич за останні роки привернула значну увагу та отримала широке поширення, змінивши протоколи безпеки, процеси автентифікації користувачів і соціальні програми. Ця технологія використовує унікальні особливості людських облич для ідентифікації та верифікації осіб, пропонуючи поєднання безпеки та зручності.

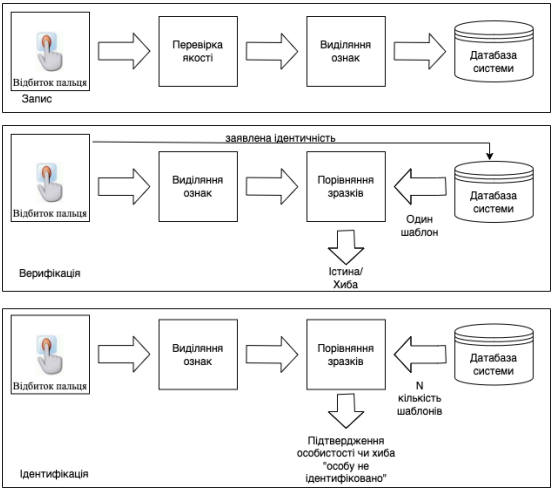


Рис. 1. Блок-схеми процесу запису, верифікації та ідентифікації показані з використанням чотирьох основних модулів біометрична система, тобто датчик, вилучення ознак, відповідник і системна база даних

Локальний бінарний шаблон (далі LBP) стає популярною технікою для представлення обличчя, а також для зображення в цілому. LBP — це не параметричне ядро, яке підсумовує локальну просторову структуру зображення. Крім того, він інваріантний до монотонних перетворень сірого, отже, представлення LBP може бути менш чутливим до змін освітлення[4].

Для ідентифікації обличчя LBP має ряд переваг. Стійкість до коливань освітлення є однією з ключових переваг. Порівнюючи інтенсивність кожного пікселя з інтенсивністю його сусідів, LBP створює бінарний шаблон, який значною мірою не реагує на зміни освітлення. Через це LBP особливо корисний у налаштуваннях із непостійним освітленням. Для додатків реального часу вкрай важливо, щоб підхід був легко реалізованим і обчислювально ефективним. Це корисно для розрізнення облич через його дискримінаційну силу та здатність захоплювати дрібнозернисті особливості текстури.

Однак LBP має свої недоліки. Метод може бути чутливим до шуму, який може вплинути на згенеровані бінарні шаблони, що призведе до зниження точності зображень із шумами. Хоча LBP добре фіксує локальну інформацію про текстуру, він може втратити глобальну просторову інформацію, яка є вирішальною для цілісного розпізнавання обличчя. Вектори ознак, створені LBP, можуть бути великими, що робить зберігання та обчислення більш інтенсивними. Крім того, незважаючи на те, що LBP стійкий до незначних змін поз, він може боротися зі значними змінами виразу обличчя, екстремальних поз або оклюзій. Незважаючи на ці обмеження, LBP залишається цінним інструментом у сфері розпізнавання обличчя, який часто використовується в поєднанні з іншими методами для підвищення загальної продуктивності.

Ще одним з популярних технік які допомагають в розпізнаванню обличчя є кореляційні фільтри. Кореляційні фільтри успішно застосовано до проблеми автоматичного розпізнавання цілей. Найбільший базовим кореляційним фільтром є узгоджений просторовий фільтр (далі MSF), чия імпульсна характеристика (у 2D, функція поширення точок). перевернута версія еталонного зображення. Тоді як MSF добре працює

при виявленні опорного зображення, пошкодженого адитивним білим шумом, він працює погано, коли посилання зображення з'являється зі спотвореннями[5].

Кореляційні фільтри пропонують кілька переваг у обробці зображень і задачах комп'ютерного зору. Однією з їхніх головних сильних сторін є ефективність і швидкість завдяки використанню методів швидкого перетворення Фур'є (FFT), які дозволяють обробляти в реальному часі навіть великі набори даних. Це робить кореляційні фільтри особливо придатними для додатків, які потребують швидкого розпізнавання образів, таких як відстеження об'єктів у відеопотоках або системи розпізнавання обличчя в реальному часі. Крім того, кореляційні фільтри стійкі до коливань освітлення, пози та шуму, що робить їх ефективними в різноманітних умовах навколишнього середовища, де такі варіації є звичайними. Вони перевершують сценарії, коли швидке й точне виявлення або зіставлення шаблонів має вирішальне значення, забезпечуючи надійні результати з мінімальними обчислювальними витратами.

Однак кореляційні фільтри мають певні обмеження. Вони можуть бути чутливими до розбіжностей між шаблоном і вхідним зображенням, що призводить до зниження точності, якщо вони не вирівняні належним чином під час попередньої обробки. Базові кореляційні фільтри також можуть мати проблеми зі значними варіаціями в масштабі, обертанні або нежорстких деформаціях, якщо вони спеціально не розроблені або доповнені додатковими методами для вирішення таких проблем. Крім того, зберігання кількох шаблонів або фільтрів для різних об'єктів або осіб може вимагати значних ресурсів пам'яті, особливо у великих системах із великими базами даних.

Біометричне розпізнавання осіб виявляється дієвим інструментом для забезпечення безпеки та зручності в різних галузях, від систем контролю доступу до соціальних проектів. Використання фізіологічних та поведінкових характеристик, таких як відбитки пальців, обличчя та кореляційні фільтри, дозволяє ефективно ідентифікувати особу з мінімальними обчислювальними витратами.

Проте існують виклики, такі як потреба в постійному удосконаленні точності та швидкості систем, а також управлінням конфіденційністю та захистом даних. Важливо збалансувати переваги з обмеженнями кожного біометричного методу для ефективного впровадження в різні сфери життя.

Майбутнє біометричних технологій обіцяє подальший розвиток у всіх галузях промисловості, що потребує надійності ідентифікації та безпеки даних. Врахування і здійснення адекватних заходів безпеки та захисту приватності є критичними для успішного впровадження цих технологій у майбутньому.

Список літератури

1. Бугаєнко Х.А. Аналіз трьох біометричних методів автентифікації особи [Електронний ресурс] / Х.А. Бугаєнко, І.Д. Горбенко // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2. – С. 262–266. – Режим доступу : http://nbuv.gov.ua/UJRN/Prre_2012_11_2_27

2. Нечипоренко О. В. Біометрична ідентифікація і автентифікація особі за геометрією обличчя. [Електронний ресурс] / Нечипоренко О. В., Корпань Я.В. – 2016. – URL: https://www.researchgate.net/publication/321423112_Biometricna_identifikacia_i_avtentifikacia_osobi_za_geometrieu_oblicca

3. Anil K. Jain, Arun Ross and Salil Prabhakar. An Introduction to Biometric Recognition // IEEE Transactions on Circuits and Systems for Video Technology. – Том 14. – Вип. 1. URL: https://www.researchgate.net/publication/3308596_An_Introduction_to_Biometric_Recognition

4. Marcel S. On the recent use of local binary patterns for face authentication / Sebastien Marcel, Yann Rodriguez, Guillaume Heusch // International journal of image and video

processing, Special issue on facial image processing. URL: http://www.idiap.ch/~marcel/professional/publications/marcel-ijivp-2007.pdf

5. Savvides M. Face Verification using Correlation Filters / Marios Savvides, B.V.K. Vijaya Kumar, Pradeep Khosla // Electrical and Computer Eng. Dept, Carnegie Mellon University Pittsburgh, U.S.A. URL: http://www.ece.cmu.edu/~kumar/Biometrics_AutoID.pdf

6. Mouad .M.H.Ali. Overview of Fingerprint Recognition System // Mouad .M.H.Ali, Vivek H. Mahale, Pravin Yannawar, A. T. Gaikwad // International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). – 2016. – URL: https://www.researchgate.net/publication/310953762_Overview_of_Fingerprint_Recognition_System

Ковальчук Д. А.
здобувач вищої освіти третього (освітньо-наукового рівня)
спеціальності 125 Кібербезпека
Науковий керівник: Йона Л. Г.
Міжнародний гуманітарний університет м. Одеса, Україна
denys.kovalchuk1@gmail.com

ПЕРСПЕКТИВИ КІБЕРБЕЗПЕКИ: ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ЗАХИСТУ ДАНИХ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

Анотація *Даний огляд описує еволюцію штучного інтелекту в кібербезпеці, починаючи зі спроб впровадження машинного навчання для виявлення загроз до сучасних розробок від корпорацій глобального рівня та великих мовних моделей. Обговорюються переваги та виклики такого застосування, включаючи потребу у великих обсягах даних, захист від атак на моделі та питання зберігання даних користувачів для збереження їх конфіденційності (GDPR). Описується роль інтердисциплінарності в розвитку цих технологій і важливість етичних питань. Текст корисний для тих, хто цікавиться новітніми технологіями кібербезпеки та їх впливом на безпеку мереж і захист особистих даних.*

Історія і перспективи розвитку

Штучний інтелект у сфері кібербезпеки виник від перших спроб застосування машинного навчання для виявлення кіберзагроз. У 2010 році компанія IBM випустила QRadar, систему, яка застосовувала алгоритми машинного навчання для аналізу мереж та виявлення потенційних загроз. Це було одним із перших комерційних рішень, які продемонстрували переваги штучного інтелекту в кібербезпеці. В наступні роки було створено безліч інших технологій, що використовували різні аспекти машинного навчання для підвищення рівня кібербезпеки.

Значущою подією стало впровадження "імунної системи" компанією Darktrace у 2013 році. Ця система використовувала машинне навчання для постійного оновлення своїх моделей і забезпечення ефективного захисту від нових атак. Розвиток штучного інтелекту в галузі кібербезпеки демонструє, як швидко адаптуються технології та методи захисту у відповідь на зростаючі загрози.

Перше використання штучного інтелекту (ШІ) в галузі кібербезпеки стикалося з технологічними та обчислювальними викликами. Проте зі зростанням обчислювальної потужності та вдосконаленням алгоритмів машинного навчання, можливості ШІ в цій сфері значно розширилися. У кінці 2010-х років почали розвивати рішення, що використовували глибоке навчання для аналізу обсягів даних та виявлення складних патернів, що свідчать про кіберзагрози. Це значно покращило точність та швидкість

виявлення загроз, зменшивши кількість помилкових сигналів і підвищивши ефективність систем кібербезпеки.

Також, одним із ключових етапів в історії розвитку штучного інтелекту в сфері кібербезпеки було впровадження великих мовних моделей (LLM). Ці моделі використовувалися для аналізу текстових даних з різних джерел, зокрема журнали безпеки, повідомлення користувачів та дані з соціальних мереж. Приміром, у 2018 році компанія Google представила модель BERT, яка стала основою для багатьох сучасних систем аналізу текстових даних. Використання таких моделей значно поліпшило виявлення фішингових атак та інших загроз, що базуються на текстових даних.

Прогрес у розвитку штучного інтелекту в галузі кібербезпеки був досягнутий завдяки співпраці між вузами, промисловістю та урядами. Багато наукових досліджень було зосереджено на створенні нових алгоритмів машинного навчання та їх впровадженні в реальні системи кібербезпеки. Наприклад, нещодавно університет Карнегі-Меллон розробив нову модель для виявлення внутрішніх загроз, яка поєднувала методи машинного навчання з психологічним аналізом поведінки користувачів. Ця модель значно підвищила точність виявлення загроз і зменшила кількість помилкових спрацьовувань.

У 2022 році Microsoft представила свою систему Multi-Factor Authentication (MFA), яка використовує штучний інтелект для поєднання біометричних даних, поведінкових патернів і інших факторів для забезпечення надійної автентифікації користувачів. Ця система значно підвищила рівень безпеки, зменшивши ймовірність несанкціонованого доступу до облікових записів і забезпечивши ефективний захист особистих даних користувачів.

Щодо найближчих перспектив та, штучний інтелект у кібербезпеці може самостійно вчитися і адаптуватися до нових способів атак, змінюючи свої методи захисту, щоб ефективно впроваджувати стратегії проти нових загроз. Системи на базі штучного інтелекту постійно оновлюють свої моделі, щоб відповідати змінам у тому, як зловмисники ведуть себе, що забезпечує високий рівень безпеки навіть у досить динамічному кіберпросторі.

Проте, використання штучного інтелекту в кібербезпеці має свої складнощі. Один із головних викликів полягає у необхідності мати великі обсяги якісних даних для тренування і покращення моделей. Це може стати проблемою для організацій, які не мають достатньо даних або не мають ресурсів для їх обробки. Крім того, алгоритми штучного інтелекту можуть бути вразливими до атак, коли зловмисники намагаються маніпулювати даними для обману системи.

Ще однією проблемою є етичні та конфіденційні аспекти. Використання штучного інтелекту для моніторингу мережевої активності може порушувати приватність користувачів. Важливо знаходити баланс між забезпеченням безпеки і збереженням особистої інформації. Так, в 2016 році Європейський Союз прийняв Загальний регламент про захист даних (GDPR), який встановлює строгі вимоги щодо обробки персональних даних, що стосуються і використання технологій штучного інтелекту в кібербезпеці.

Успішне впровадження штучного інтелекту в кібербезпеку вимагає взаємодії різних наукових напрямів. Важливо залучати експертів з комп'ютерних наук, математичного аналізу, психології та юриспруденції для створення складних і ефективних систем захисту. Наприклад, дослідження, проведене у 2021 році університетом Карнегі-Меллон, показало, що поєднання різних методів машинного навчання з психологічним аналізом поведінки користувачів суттєво підвищує ефективність виявлення внутрішніх загроз.

Алгоритми штучного інтелекту можуть стати уразливими до атак на штучний інтелект, які відомі як атаки на моделі. Це означає, що зловмисники можуть спеціально змінювати дані, щоб перехитрити систему. Навіть невеликі зміни у вхідних даних можуть призвести до неправильної класифікації загрози або до помилкових позитивних виявлень. Це є серйозною проблемою, оскільки такі атаки можуть значно підірвати ефективність

систем кібербезпеки, що використовують штучний інтелект, зробивши їх менш надійними у виявленні та нейтралізації загроз.

Не дивлячись на вищепераховані труднощі машинне навчання стає необхідним інструментом у сучасній кібербезпеці, завдяки своїй здатності до аналізу величезних обсягів даних та виявленню складних залежностей і шаблонів. Використання алгоритмів машинного навчання дозволяє автоматизувати виявлення загроз і реагування на них у реальному часі, що значно підвищує ефективність захисту мереж та систем. Перспективи використання цих технологій включають розвиток систем, які можуть самостійно навчатися і адаптуватися до нових видів загроз, а також створення інтелектуальних систем з вбудованою здатністю передбачення майбутніх атак і попередження їх. Це відкриває широкі можливості для забезпечення високого рівня кібербезпеки в умовах постійно змінюваного кіберпростору.

Висновки

Штучний інтелект у кібербезпеці відіграє ключову роль у сучасному цифровому середовищі, де зростаючі загрози вимагають інноваційних заходів захисту. З огляду на еволюцію цієї технології, варто зазначити, що початкові застосування машинного навчання для виявлення кіберзагроз вже перетворились на потужні системи, які автоматизують і підвищують ефективність захисту мереж і даних.

Прогрес у цій галузі підкреслює необхідність інтеграції різних дисциплін, включаючи комп'ютерні науки, математичний аналіз, психологію та юриспруденцію. Такий підхід дозволяє створювати комплексні системи захисту, які ефективно протистоять сучасним і майбутнім кіберзагрозам.

Однак, використання штучного інтелекту в кібербезпеці також зустрічає виклики. Наприклад, потреба у великих обсягах якісних даних для тренування моделей і вразливість до атак на штучний інтелект, коли зловмисники можуть маніпулювати даними для обману систем.

Також важливо враховувати етичні аспекти і конфіденційність при застосуванні штучного інтелекту в кібербезпеці. Існує постійна необхідність у забезпеченні балансу між збереженням приватності користувачів і забезпеченням ефективної безпеки.

Загалом, штучний інтелект в кібербезпеці є суттєвим напрямом розвитку, що відкриває широкі перспективи для створення надійних систем захисту, які активно адаптуються до нових загроз і забезпечують безпеку даних у сучасному цифровому світі.

Список використаних джерел

1. Fei Hu, Xiali Hei. “AI, Machine Learning and Deep Learning: A Security Perspective”.
2. Mark Stamp, Corrado Aaron Visaggio, Francesco Mercaldo, Fabio Di Troia. “Artificial Intelligence for Cybersecurity”.
3. Hamid Jahankhani, Babak Akhgar, Peter Cochrane, Mohammad Dastbaz “Policing in the Era of AI and Smart Societies”.
4. Laurent Gil, Allan Liska. “Security with AI and Machine Learning”.
5. Yulei Wu, Jingguo Ge, Tong Li. “AI and Machine Learning for Network and Security Management”.

УДК 004.77:004.9(477)

Кандидат юридичних наук Лефтеров Лев Васильович
Департамент кіберполіції Національної поліції України
lev.lefterov@cyberpolice.gov.ua

Науковий керівник
Йона Лариса Григорівна, к.т.н., доцент
Міжнародний гуманітарний університет
yonalarisa66@gmail.com

ОПТИМІЗАЦІЯ ТА ПІДВИЩЕННЯ БЕЗПЕКИ VPN-ТЕХНОЛОГІЙ У СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Анотація. *У статті досліджується роль і ефективність VPN-технологій у забезпеченні безпеки інформаційних комунікацій. Обговорюються сучасні методи оптимізації VPN для підвищення їх продуктивності та безпеки. Особлива увага приділяється протоколам шифрування, новітнім технологіям захисту даних та інтеграції VPN з хмарними сервісами.*

У сучасному світі інформаційно-комунікаційні системи стали невід'ємною частиною щоденного життя. Вони забезпечують зв'язок між людьми, обмін даними, доступ до інформаційних ресурсів та багато інших важливих функцій. Проте, з розвитком технологій виникають і нові загрози, пов'язані з безпекою інформації.

Безпека інформаційних комунікацій є критично важливою з кількох причин. По-перше, вона забезпечує конфіденційність даних, тобто захист від несанкціонованого доступу до приватної та конфіденційної інформації. По-друге, важливим аспектом є цілісність даних, яка запобігає несанкціонованим змінам або пошкодженню даних під час їх передачі. Третім важливим елементом є доступність даних, що забезпечує доступ до інформації лише авторизованим користувачам, коли це необхідно [1].

Додатково, безпека інформаційних комунікацій включає захист від кіберзагроз, знижуючи ризик атак зловмисників, таких як перехоплення даних, віруси, фішинг та інші види кіберзлочинів.

У цьому контексті VPN (Virtual Private Network) є одним з основних інструментів для забезпечення безпеки інформаційних комунікацій. VPN дозволяє створити захищене з'єднання через загальнодоступну мережу, таку як Інтернет. Це досягається за допомогою шифрування даних та створення тунелів, що захищають інформацію від перехоплення та несанкціонованого доступу [2].

Як зазначено вище основні функції VPN включають шифрування даних, приховування IP-адреси, забезпечення безпечного доступу до корпоративних ресурсів та захист від цензури та обмежень доступу. Шифрування даних використовує спеціалізовані протоколи для захисту інформації під час її передачі через Інтернет, забезпечуючи конфіденційність і захист від прослуховування. Приховування IP-адреси маскує справжню IP-адресу користувача, надаючи йому анонімність та захист від відстеження. Забезпечення безпечного доступу до корпоративних ресурсів дозволяє співробітникам безпечно підключатися до корпоративних мереж з будь-якого місця, забезпечуючи безпечний доступ до внутрішніх ресурсів компанії.

Розглянемо основні типи та технології VPN.

1. Site-to-Site VPN – тип мережі, що з'єднує дві або більше локальних мереж через Інтернет, створюючи єдину віртуальну мережу. Це рішення часто використовують для з'єднання офісів компанії в різних географічних місцях. Site-to-Site VPN забезпечує зручність у централізованому управлінні мережами і захист переданих даних, але налаштування може бути складним і залежить від стабільності Інтернет-з'єднання.

2. Remote Access VPN – забезпечує індивідуальним користувачам захищений доступ до корпоративної мережі з будь-якої точки світу через Інтернет. Цей тип VPN відзначається гнучкістю у доступі та високим рівнем безпеки, що є важливим для віддаленої роботи. Однак, він може бути залежним від якості Інтернет-з'єднання і може мати проблеми з продуктивністю при великій кількості користувачів.

3. SSL VPN – це технологія віддаленого доступу на основі протоколу SSL. На відміну від інших поширених технологій VPN, таких як IPSec VPN, що захищають дані на основі IP-адреси, SSL VPN шифрує дані програми. Це робить SSL VPN більш точним, ніж IPSec VPN.

4. MPLS VPN – використовує технологію Multiprotocol Label Switching (MPLS) для забезпечення високошвидкісного та надійного з'єднання між офісами компанії. Це рішення забезпечує високу продуктивність, масштабованість і надійність, але може бути дорогим і складним у налаштуванні та управлінні [3].

В залежності від конкретних типів приватних мереж використовуються різні мережеві протоколи підключення. Загальновідомими протоколами, які реалізують функції VPN, є OpenVPN, IPsec, WireGuard, L2TP/IPsec та PPTP. Кожен з цих протоколів має свої технічні характеристики, переваги і недоліки.

OpenVPN є відкритим програмним забезпеченням, яке реалізує VPN з використанням протоколів SSL/TLS для шифрування. Цей протокол забезпечує високий рівень безпеки завдяки застосуванню потужних методів шифрування і аутентифікації. OpenVPN відрізняється гнучкістю у налаштуванні і підтримує широкий спектр платформ, включаючи Windows, macOS, Linux та мобільні операційні системи. Проте, його впровадження може бути ускладнене через можливі проблеми з продуктивністю на старих або малопотужних пристроях. Врахування цих аспектів є важливим при виборі OpenVPN як рішення для забезпечення захисту інформаційних комунікацій [4].

Ipsec (Internet Protocol Security) являє собою набір протоколів, що забезпечують захист IP-комунікацій через шифрування і аутентифікацію. IPsec забезпечує високий рівень безпеки завдяки використанню сучасних алгоритмів шифрування, а також сумісність з різними платформами та пристроями, включаючи мережеві маршрутизатори і комп'ютери. Однак, налаштування IPsec може бути складним і вимагати детального знання специфікацій протоколу, а також можуть виникати проблеми з сумісністю різних реалізацій. Тому важливо ретельно підходити до налаштування і інтеграції IPsec у існуючі мережі.

WireGuard є новітнім протоколом VPN, розробленим з акцентом на простоту, швидкість і високий рівень безпеки. WireGuard відзначається високою продуктивністю завдяки спрощеній архітектурі і ефективному використанню ресурсів. Протокол є простим у налаштуванні і використанні, що робить його привабливим вибором для багатьох сценаріїв. Однак, його обмежена підтримка на деяких платформах і відносна новизна можуть вплинути на його тестування в реальних умовах. Зважаючи на це, необхідно оцінювати можливості WireGuard у контексті конкретних вимог і середовища експлуатації [4].

L2TP/Ipsec (Layer 2 Tunneling Protocol) є комбінацією протоколів L2TP і IPsec, що забезпечує захищені VPN-з'єднання через комбінацію тунелювання і шифрування. Цей протокол забезпечує високий рівень безпеки і сумісність з багатьма операційними системами і пристроями. Однак, його налаштування може бути складним, а подвійне шифрування може вплинути на продуктивність з'єднання. Тому при виборі L2TP/IPsec слід враховувати можливий компроміс між рівнем безпеки і продуктивністю [4].

PPTP є одним з найстаріших протоколів VPN, що використовує методи тунелювання для створення захищених з'єднань. Простота налаштування і висока швидкість є основними перевагами PPTP. Проте, рівень безпеки цього протоколу значно нижчий порівняно з сучасними рішеннями, і він уразливий до багатьох атак. Це робить PPTP менш придатним для використання в умовах високих вимог до безпеки [4].

Шифрування є основним механізмом захисту даних, що передаються через мережі. Сучасні методи шифрування можна класифікувати на симетричні та асиметричні. Симетричні методи шифрування, такі як Advanced Encryption Standard (AES), використовують один і той же ключ для шифрування і розшифрування даних. AES забезпечує високий рівень безпеки і є стандартом для шифрування даних у багатьох

сучасних системах VPN. Асиметричні методи шифрування, наприклад, RSA, використовують пару ключів – публічний і приватний, що дозволяє забезпечити безпечний обмін ключами і автентифікацію користувачів. Хоча асиметричне шифрування забезпечує вищий рівень безпеки при обміні даними, воно може бути менш ефективним у порівнянні з симетричними методами у плані швидкості [5].

Важливо зазначити, що шифрування даних є лише однією частиною загальної стратегії захисту інформації. Наступним важливим аспектом є автентифікація користувачів, яка грає ключову роль у забезпеченні безпеки систем. Одним з найбільш ефективних методів підвищення рівня безпеки є мультифакторна автентифікація (MFA).

Мультифакторна автентифікація (MFA) є додатковим рівнем безпеки, що використовується для підтвердження особи користувача. MFA зазвичай поєднує два або більше з наступних факторів: знання (пароль), володіння (апаратний токен або мобільний пристрій) і властивості (біометричні дані). Використання MFA суттєво підвищує рівень захисту, знижуючи ймовірність несанкціонованого доступу до системи навіть у разі компрометації пароля. У контексті VPN, MFA може бути інтегрована в процес аутентифікації для забезпечення додаткового рівня безпеки при доступі до корпоративних ресурсів [6].

Оптимізація продуктивності VPN є критичним аспектом для забезпечення ефективної роботи мережі і задовільного досвіду користувачів. Основні виклики продуктивності VPN включають зниження швидкості з'єднання, затримки та перевантаження мережевих ресурсів. Для подолання цих проблем використовуються різні техніки оптимізації, серед яких виділяються управління якістю обслуговування (QoS), балансування навантаження та стиснення даних. QoS дозволяє пріоритизувати трафік в мережі, забезпечуючи необхідну пропускну здатність для критичних додатків і знижуючи затримки для важливих даних. Це досягається шляхом налаштування мережевих пристроїв для віддання переваги певним типам трафіку, що дозволяє підтримувати високу продуктивність VPN. Балансування навантаження є ще однією важливою технікою, яка дозволяє рівномірно розподілити навантаження між кількома серверами або вузлами. Це допомагає запобігти перевантаженню окремих компонентів мережі і забезпечує більш стійке і швидке з'єднання для користувачів. Стиснення даних використовується для зменшення обсягу даних, що передаються через VPN, що може суттєво знизити затримки і підвищити швидкість з'єднання. Стиснення зменшує навантаження на мережу та забезпечує ефективніше використання пропускної здатності [7].

Віртуальні приватні мережі є невід'ємною частиною архітектури безпеки для хмарних середовищ. Використання VPN у хмарних середовищах дозволяє забезпечити захищене з'єднання між локальними інфраструктурами і хмарними ресурсами. Це дозволяє компаніям безпечно підключатися до своїх хмарних сервісів, зберігати дані і здійснювати обробку інформації без ризику несанкціонованого доступу. VPN забезпечує шифрування даних під час передачі, що захищає інформацію від потенційних загроз, таких як перехоплення або зловмисні атаки [8].

Однією з основних переваг використання VPN у хмарних середовищах є можливість забезпечення єдиного захищеного каналу для всіх комунікацій між локальними системами і хмарними сервісами. Це особливо важливо для організацій, що працюють з чутливими даними або мають високі вимоги до безпеки. Інтеграція VPN з хмарними платформами також дозволяє гнучко масштабувати інфраструктуру, забезпечуючи зростаючу безпеку у відповідності до змінюваних потреб бізнесу.

Захист даних при передачі між хмарними та локальними мережами є критичним аспектом забезпечення безпеки інформаційних систем. Хоча хмара пропонує численні переваги у вигляді масштабованості і доступності ресурсів, передача даних між локальними системами та хмарними сервісами може створювати ризики для безпеки. Використання VPN у цьому контексті забезпечує додатковий рівень захисту, за рахунок шифрування даних, що передаються між різними середовищами [1].

Коли дані передаються через VPN, вони проходять через захищений тунель, що перешкоджає їх перехопленню або зміні сторонніми особами. Це особливо важливо для передачі конфіденційної інформації або при виконанні транзакцій, що потребують високого рівня захисту. VPN також дозволяє встановлювати контроль доступу до ресурсів, забезпечуючи, щоб лише авторизовані користувачі могли отримати доступ до чутливих даних і систем.

Попри численні переваги, впровадження та використання VPN стикається з кількома суттєвими викликами. Один з основних викликів пов'язаний із забезпеченням продуктивності при високих обсягах трафіку. Шифрування та тунелювання можуть впливати на швидкість з'єднання і загальну ефективність мережі, що може стати проблемою для організацій з високими вимогами до швидкості і продуктивності.

Ще одним викликом є складність налаштування та управління VPN. Хоча сучасні рішення намагаються спростити цей процес, налаштування VPN може бути досить складним і вимагати спеціалізованих знань. Проблеми з сумісністю різних протоколів і технологій також можуть створювати труднощі в процесі інтеграції VPN у існуючі інформаційні системи.

Забезпечення безпеки також є постійним викликом, оскільки постійно з'являються нові загрози і уразливості. Постійний моніторинг і оновлення систем безпеки є необхідними для підтримання надійного захисту. В умовах швидко змінюваного технологічного середовища, забезпечення актуальності і ефективності заходів безпеки є постійним завданням.

Загалом, технології VPN мають важливе значення для забезпечення безпеки інформаційних систем та приватності даних. Подальший розвиток цих технологій обіцяє підвищення рівня захисту та ефективності, зокрема через інтеграцію з новими технологіями та вдосконалення протоколів шифрування. Однак впровадження та використання VPN стикаються з кількома викликами, такими як забезпечення продуктивності, складність налаштування та управління, а також постійні загрози безпеці. Тому організації повинні постійно вдосконалювати свої рішення у сфері VPN, щоб адаптуватися до нових умов і забезпечувати високий рівень захисту даних.

Література

1. Mytko A., Pakholchuk I. Безпека інформаційних систем організацій. Міжнародні відносини, суспільні комунікації та регіональні студії. 2017. № 1. С. 89–96. URL: https://doi.org/10.29038/2524-2679-2017-01-89-96 (дата звернення: 11.06.2024).

2. Vacca J. Virtual private networks. Network design. 2000. С. 323–337. URL: https://doi.org/10.1201/9781420093759.ch24 (дата звернення: 01.07.2024).

3. Організаційна структура технічного захисту інформації на мережевому рівні з використанням технології vpn / О. Гавриш та ін. Вісник Черкаського державного технологічного університету. 2023. № 3. С. 5–15. URL: https://doi.org/10.24025/2306-4412.3.2023.284551 (дата звернення: 29.06.2024).

4. Antoniuk J., Plechawska-Wójcik M. Comparative analysis of VPN protocols. Journal of computer sciences institute. 2023. Т. 27. С. 138–144. URL: https://doi.org/10.35784/jcsi.3315 (дата звернення: 30.06.2024).

5. Краліна Г., Баков Н. Шифрування: типи та алгоритми. Specialized and multidisciplinary scientific researches. 2020. URL: https://doi.org/10.36074/11.12.2020.v2.36 (дата звернення: 04.07.2024).

6. Дунь О. В., Дунь А. В., Dun O. V. Адаптивна автентифікація даних : thesis. 2009. URL: http://essuir.sumdu.edu.ua/handle/123456789/5957 (дата звернення: 04.07.2024).

7. QoS-Classifier for VPN and Non-VPN traffic based on time-related features / J. A. Caicedo-Muñoz та ін. Computer networks. 2018. Т. 144. С. 271–279. URL: https://doi.org/10.1016/j.comnet.2018.08.008 (дата звернення: 05.07.2024).

8. Баглай Р. О. Загрози безпеки хмарних технологій для банків. Системи обробки інформації. 2018. Вип. 1 (152). С. 127–135.

УДК 004.45+004.49

Воробйов І.В., магістр
Науковий керівник: Глоба Л.С., д.т.н., проф.
КПІ ім. Ігоря Сікорського, Київ
vorobjov.ivan@gmail.com

ТИПОЛОГІЯ ПОДІЙ У ЯДРІ LINUX ЯК ОСНОВА ДЛЯ АНАЛІЗУ ЗЛОВМИСНОЇ АКТИВНОСТІ

Анотація. *У сучасному світі пристрої на базі ядра Linux широко використовуються (понад 60% вбудованих систем та 70% мобільних пристроїв мають такі системи). За останні роки значно зросла кількість виявлених вразливостей у різних системах (з близько 5000 у 2013 році до понад 26000 у 2023 році). Забезпечення безпеки Linux систем стає надзвичайно важливою задачею для забезпечення стабільної роботи цих пристроїв. Реагування на виклики в системі може ґрунтуватися на різних подіях і патернах поведінки в системі. У даній статті розглядаються різноманітні типи подій, які можна аналізувати в системі Linux, види вразливостей та робиться спроба класифікувати події за типом зловмисної активності.*

Операційні системи на базі Linux мають значну частку ринку вбудованих систем, яка оцінюється приблизно в 50-60% завдяки своїй гнучкості та надійній підтримці. У сфері смартфонів домінує Android, Linux-базована ОС, яка займає понад 70% глобального ринку [1]. Однак за останні кілька років значно збільшилася кількість виявлених вразливостей у різних системах, з близько 5000 у 2013 році до понад 26000 у 2023 році [2]. Ростуча кількість атак та широке розповсюдження систем, заснованих на ядрі Linux, призводять до підвищення уваги до безпеки цієї системи.

Стандартною практикою для детектування зловмисної активності є аналіз різних подій, які генерує система. Ми можемо виділити значну кількість різних подій та патернів у системі, проте обробка та аналіз їх на пристроях є нетривіальною задачею через обмежені обчислювальні можливості вбудованих систем. Виникає протиріччя, коли для якісного детектування потрібно використовувати максимальну кількість різноманітних подій, але для функціонування системи та задоволення потреб користувачів це необхідно робити з мінімальними затримками. Для вирішення цієї дилеми пропонується класифікувати події в системі Linux за типами, відповідно до різних можливих атак. Далі у тезах будуть описані види подій у системі Linux, типи вразливостей та запропоновано варіант типізації подій.

Розглянемо події, які можуть бути детектовані та проаналізовані в системі Linux [3, 4]. Одним з перших та основних механізмів взаємодії з системою є системні виклики (syscalls). Прикладами можуть бути: fork() - створення нового процесу, execve() - завантаження та виконання нового виконуваного файлу, kill() - надсилання сигналу процесу, та багато інших. Ці системні виклики є критичними для функціонування системи та часто є мішенню для зловмисних дій, таких як експлуатація вразливостей або спроби несанкціонованого доступу. Аналіз патернів викликів системних функцій може допомогти виявити підозрілі або аномальні дії, що є важливим для забезпечення безпеки системи. Хоча більшість подій може бути зведена до конкретного системного виклику, цей підхід є занадто широким. Тому варто виділити також інші події. Події, пов'язані з файловими операціями, є критичними для функціонування системи. Вони включають створення та видалення файлів, зміну прав доступу та власника, а також зміну цілісності файлу. Події, пов'язані з операціями в мережі, також важливі для аналізу безпеки. Вони включають

створення та закриття з'єднань, надсилання та отримання даних. Події, пов'язані з операціями з пам'яттю, включають відображення файлу у пам'ять, виділення пам'яті та доступ до заблокованих ділянок. Ці події можуть вказувати на спроби експлуатації вразливостей у пам'яті або маніпуляції з пам'яттю системи. Активність процесів також є критичною для аналізу безпеки. Вона включає створення нових потоків та зміну пріоритетів процесів. Аналіз цих подій дозволяє більш точно ідентифікувати потенційні загрози та аномалії, що сприяє підвищенню рівня безпеки системи Linux. Завдяки такому підходу можна забезпечити ефективний моніторинг і своєчасне реагування на можливі загрози, забезпечуючи стабільну та безпечну роботу системи.

Існує велика кількість зловмисних програм, включаючи віруси, трояни, черв'яки, шпигунське програмне забезпечення, руткіти, рекламне програмне забезпечення, шифрувальники [5], бекдори. Одним із найпоширеніших є віруси, які приєднуються до інших програм або файлів і поширюються при їх виконанні. Віруси можуть пошкоджувати дані, видаляти файли або навіть змінювати конфігурацію системи, завдаючи значної шкоди комп'ютерній інфраструктурі. Іншим поширеним типом зловмисного коду є трояни, які маскуються під легітимне програмне забезпечення. Вони не розповсюджуються самостійно, але можуть надавати зловмисникам доступ до системи користувача, викрадати конфіденційні дані або виконувати інші шкідливі дії. Шпигунське програмне забезпечення збирає інформацію про користувача без його відома або згоди, відстежуючи дії користувача або збираючи дані з веб-браузера, що може призвести до викрадення особистих даних. Руткіти надають зловмисникам привілейований доступ до системи і приховують свою присутність, змінюючи системні файли або конфігурації. Рекламне програмне забезпечення відображає небажану рекламу на комп'ютері користувача, що може порушувати приватність користувача і уповільнювати роботу системи. Шифрувальники (ransomware) шифрують файли на комп'ютері користувача або блокують доступ до системи, вимагаючи викуп за розблокування або розшифрування, що може мати серйозні наслідки для користувачів і організацій. Бекдори дозволяють зловмисникам обійти нормальні механізми аутентифікації і отримати несанкціонований доступ до системи, забезпечуючи можливість для подальших атак. Окрім цього, існують вразливості, які дозволяють підвищити привілеї у системі, надаючи користувачам доступ до ресурсів, до яких вони не повинні мати доступ. Також існують вразливості, що можуть призвести до відмови в обслуговуванні, роблячи систему недоступною для користувачів.

Розглядаючи взаємозв'язок між подіями у системі та типами атак, можна спостерігати різноманітні сценарії. Системні виклики використовуються для широкого спектру операцій і часто складно піддаються аналізу через велику кількість некласифікованих подій. Дії з файловою системою можуть вказувати на наявність шифрувальника або руткіта. Аномалії в мережевих операціях можуть свідчити про наявність троянських програм чи бекдорів. Аналіз доступу до пам'яті може допомогти виявити складні атаки, які характерні для руткітів.

Проте встановлення чіткого співвідношення між подіями в системі та типами атак здається не завжди можливе, оскільки атаки часто використовують різні методи та техніки. Тому краще аналізувати не окремі події, а їх зіставлення та взаємозв'язки, що можуть вказувати на конкретні методи або техніки атаки, а не на саму атаку в цілому. Крім того, багато з цих подій не є унікальними для зловмисного використання і відбуваються в межах нормального функціонування системи. Це підкреслює важливість аналізу патернів подій та вторинних ознак для виявлення потенційних загроз та аномалій.

Висновки

У результаті аналізу типології подій у ядрі Linux для виявлення зловмисної активності виявлено, що багато з подій, що фіксуються в системі, мають широкий спектр застосування, що ускладнює їхнє однозначне класифікування. Більшість цих подій відбуваються як в нормальних, так і в потенційно зловмисних сценаріях. Зловмисне

використання системи складається з послідовності дій, які використовують різні техніки та методи для досягнення своїх цілей. Це робить важливим аналіз не окремих подій, а їх комбінацій та патернів, що вказують на специфічні техніки атаки, а не лише на вразливості системи. Отже, пряме зіставлення події з типом вразливості – є необґрунтованим, для ефективного виявлення зловмисної активності необхідно переходити від класифікації окремих подій до аналізу їх зіставлень та типів, що відображають використані техніки.

Література

1. Mobile & Tablet Operating System Market Share Worldwide | Statcounter Global Stats. StatCounter Global Stats. URL: https://gs.statcounter.com/os-market-share/mobile-tablet/worldwide/#yearly-2024-2024-bar .
2. 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is | Qualys Security Blog. Qualys Security Blog. URL: https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one .
3. Castrovilli, M., & Bini, E. (2024). SlackCheck: A Linux Kernel Module to Verify Temporal Properties of a Task Schedule. In 36th Euromicro Conference on Real-Time Systems (ECRTS 2024). Schloss Dagstuhl–Leibniz-Zentrum für Informatik.
4. Love, R. (2010). Linux kernel development. Pearson Education.
5. Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. Network security, 2016(9), 5-9.

УДК _____ *Пахолюк Олег Ігорович*
Аспірант, спеціальність 125 «Кібербезпека та захист інформації»,
Бондар Владислав Миколайович,
Магістр, спеціальність 125 - «Кібербезпека та захист інформації»
Науковий керівник
Йона Лариса Григорівна, к.т.н., доцент
Міжнародний гуманітарний університет
yonalarisa66@gmail.com

АНАЛІЗ КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ПРИЗНАЧЕННЯМ

***Анотація**. Дослідження включає аналіз* криптографічних *методів захисту інформації за призначенням, зокрема систем, що виконують процедури підтвердження справжності.*

Питання забезпечення захисту інформації – це одне з найактуальніших питань сьогодення. Захист основних властивостей інформації, що захищається, а саме конфіденційності, цілісності та доступності забезпечується різноманітними криптографічними методами.

Отже, захист інформації від несанкціонованого ознайомлення неавторизованим користувачем, тобто конфіденційність інформації, забезпечується криптографічним перетворенням відкритого тексту шляхом шифрування та передаванням його у вигляді криптограми.

Захист інформації від навмисної модифікації неавторизованим користувачем, тобто цілісність інформації, забезпечується криптографічним перетворенням шляхом створення цифрового підпису та процедурою верифікації документу.

Захист інформації від неможливості отримання доступу до неї та її використання, тобто забезпечення доступності інформації, забезпечується шляхом підтримання системи

в робочому стані для надання користувачу можливості користування нею в межах відповідних повноважень.

У зв'язку з тим, що сказано вище, можна дійти висновку, що для вирішення різноманітних завдань використовуються різні алгоритми криптографічного перетворення інформації. Дійсно, криптографічні алгоритми поділяються за призначенням.

Так, симетричні алгоритми використовуються для шифрування інформації. Це обумовлено тим, що симетричні системи для шифрування та розшифровування тексту використовують один спільний секретний ключ, внаслідок чого працюють швидше, ніж асиметричні двоключові системи.

Прикладом симетричних криптосистем можуть бути алгоритми блочного шифрування; DES; 3-DES; ДСТУ ГОСТ 28147-2009; IDEA; AES; ДСТУ 7624:2014 «Калина» тощо [1].

До симетричних криптографічних перетворень можнатакож віднести й геш-функції, оскільки в ключових функціяхгешуваннявикористовуютьсясиметричнікриптографічніперетвореннята ключі. Геш-функції призначені для перетворення довільного обсягу даних у фіксовану довжину геш-код, що дає можливість використовувати їх для перевірки цілісності даних та застосовувати в алгоритмах електронного підпису.

Прикладом криптографічних геш-функцій можуть бути ДСТУ 7564:2014 «Купина», MD5; SHA-1; SHA-256 тощо.

У таблиці 1 показано призначення симетричних алгоритмів та рівняння шифрування у них.

Таблиця 1 – Призначення симетричних криптосистем

Симетричні криптосистеми			
Шифрування			
Вид перетворення	**Ключі, що використовуються**	**Рівняння зашифровування**	**Рівняння розшифровування**
зашифровування та розшифровування	Спільний **закритий** (секретний) ключ $\mathbf{к}_з$	$\mathbf{C = Eк}_з\mathbf{(M)}$, де **C**-криптограма, **M**-відкритий текст, $\mathbf{E}к_з$(M)-функція зашифровування секретним ключем	$\mathbf{M = Dк}_з\mathbf{(C)}$, де **M**-відкритий текст, **C** криптограма, $\mathbf{D}к_з$(C) - функція розшифровуванн секретним ключем

Проте, є асиметричні системи, які також можуть шифрувати інформацію, але цей процес буде проходити повільніше, ніж у симетричних алгоритмів. Це відбувається тому, що на відміну від симетричних систем зі спільним секретним ключем, в асиметричних системах застосовується два ключа (один ключ відкритий та другий - секретний ключ). Довжина цих ключів має бути дуже великою, щоби не було можливості підібрати ключ методом перебору. Саме тому перетворення шифрування криптосистемами з відкритим ключем використовується тільки для невеликих повідомлень (приміром, для ключових послідовностей). При шифруванні повідомлення відправник використовує відкритий ключ, а одержувач повідомлення використовує відповідний секретний ключ.

Прикладом асиметричних криптосистем з режимом шифрування може бути алгоритм RSA, Ель Гамаля Меркли-Хеллмана, Шамира, тощо.

У таблиці 2 (a,b,c) показано призначення асиметричних алгоритмів. У таблиці 2,а показані правила перетворення при процедурі шифрування.

Таблиця 2,а – Призначення асиметричних криптосистем, процедура шифрування

Асиметричні криптосистеми			
Шифрування			
Вид перетворення	**Ключі, що використовуються**	**Рівняння зашифровування**	**Рівняння розшифровування**
зашифровування *та* ***розшифровування***	***відкритий*** *ключ* $\boldsymbol{к_в}$*;* *та* ***закритий*** *ключ* $\boldsymbol{к_з}$	$\mathbf{C = Eк_в (M)}$, де **C**-криптограма, **M**-відкритий текст, $\mathbf{Eк_в}$(M)-функція зашифровування відкритим ключем	$\mathbf{M = Dк_з (C)}$, де **M**-відкритий текст, **C** криптограма, $\mathbf{Dк_з}$(C) **-** функція розшифровування секретним ключем

Крім того, асиметричні системи вирішують питання розподілу ключів.

У таблиці 2,b показані правила перетворення при процедурі розподілу ключів.

При використанні асиметричних криптографічних методів, розподіл відкритих ключів користувачам та видача секретних ключів здійснюється через центри розподілення ключів (ЦРК). Оскільки кількість абонентів мережі постійно зростає, розподіл секретних ключів по відкритому каналу зв'язку за допомогою ЦРК став проблемним для забезпечення надійного та довготривалого обміну секретними ключами. Ця проблема була вирішена алгоритмом Діффі-Хеллмана.

Вчені Діффі та Хеллман продемонстрували як використовувати в асиметричних алгоритмах функцію дискретного піднесення до степеня.

Необоротність перетворювання в цьому разі забезпечується тим, що легко обчислити показникову функцію в кінцевому полі Галуа, яке складається з p елементів (p – просте число чи просте в будь-якому степені).

Обчислювання логарифмів в таких полях – більш трудомістка операція. Приміром, якщо для прямого перетворювання 1000-бітових простих чисел треба 2000 операцій, то для оберненого перетворювання (обчислювання логарифму в полі Галуа) треба біля 10^{30} операцій.

Користувачі отримують спільний секретний ключ, обчислюючи його з отриманих відкритих ключів, при цьому використовується незахищений канал зв’язку. Абоненти мають свої приватні ключі, перевіряють правильність обчислення та проходять додаткову автентифікацію, щоби бути впевненими, що відкритий ключ був відправлений саме від того користувача, хто має брати участь в цьому сеансі зв’язку. Щоби зловмисник не зміг скористатися перехопленим ключем, можна цей відкритий ключ захистити своїм електронним підписом. Цей процес необхідно виконувати, якщо між відправником повідомлення та одержувачем немає можливості передачі асиметричних ключів шляхом збереження конфіденційності. Цей метод дає можливість обчислити спільний секретний ключ на кожний сеанс зв’язку, що дуже зручно для користувачів.

Таблиця 2, b – Призначення асиметричних криптосистем, процедура розподілу ключів

Асиметричні криптосистеми			
Розподілення ключів			
Вид перетворення	**Ключі, що використо вуються**	**Створення ключа користувачем А**	**Створення ключа користувачем В**
Створення спільного секретного ключа (метод Діффі-Хеллмана)	***закритий*** ключ користувача А, $\mathbf{к_а}$; та ***закритий***ключ користувача В $\mathbf{к_в}$.	**К = $y_в^{Ка}$ (modN),** де К - спільний секретний ключ, $\mathbf{y_в} = g^{Кв}$ modN - відкрите число користувача В; g – мантіса N - модуль	**К = $y_а^{Кв}$ (modN),** де К - спільний секретний ключ, $\mathbf{y_а} = g^{Ка}$ modN - відкрите число користувача А; g – мантіса N-модуль

Недоліком алгоритма Діффі–Хеллмана є відсутність гарантованої нижньої оцінки трудомісткості зламування ключа. Окрім того, залишається проблема автентифікації, тому що є небезпека імітування користувача.

Основним призначенням несиметричних криптосистем є проведення процесу автентифікації документів. Підтвердження справжності здійснюється перетворенням документу шляхом його стиснення та подальшого використання секретного ключа для створення підпису під відкритим текстом. Тобто підпис ставиться не під самим документом, а під результатом його перетворення (гешем). В такий спосіб процес роботи асиметричних систем пришвидшується і це дає можливість використання таких якостей двоключових систем, як надійність та зручність.

Прикладом асиметричних криптосистем, що використовуються для автентифікації документів можуть бути алгоритми RSA, Ель Гамаля, DSA, GQ(Guillou-Qisquater),Шнорра,Нуберга-Рюппела(Nyberg-Rueppel),тощо [2].

У таблиці 2,с показані правила перетворення при процедурі автентифікації документу.

Докласукриптосистемзвідкритим ключем належать також криптосистеминаеліптичнихкривих(EllipticCurveCryptography–ECC).Безпека таких алгоритмів базуєтьсяздебільшогонаскладностірозв'язуваннязадачі дискретного логарифмування у групі точок еліптичної кривої (EllipticCurveDiscreteLogarithmProblem–ECDLP)надкінцевимполем.Порівняно з іншими асиметричними алгоритмами, криптосистеми на еліптичних кривих характеризуються потужною криптостійкістю. Розв'язанняпроблемиECDLPєбільшскладним,ніжвирішенняпроблемидискретного логарифмування(DiscreteLogarithmProblem–DLP).

Укриптографіїзазвичайвикористовуються еліптичні криві в кінцевих полях. Для точок на еліптичній кривій вводитьсяоперація додавання, яка є альтернативою операція множення у асиметричних криптосистемах RSAтаЕль-Гамаля. Також слід зазначити, що перевагоюкриптосистемнаеліптичнихкривихєвисокашвидкістьопрацьовуванняінформації.

Таблиця 2,с – Призначення асиметричних криптосистем, процедура автентифікації документу.

Асиметричні криптосистеми			
Автентифікація документу			
Вид перетворення	Ключі, що використо вуються	Створення підпису	Перевірка підпису
створення підпису *та* *перевірка підпису* (алгоритм RSA)	*закритий*ключ $к_з$ *та* *відкритий*ключ $к_в$	$S = m^{Кз}$, де S -підпис, m = F(M), результат гешування відкритого тексту М	• $m' = S^{Кв}$, де m' – відновлений геш з підпису S за допомогою відкритого ключа. • m'' = F(M), результат гешування відкритого тексту М • Порівняння m' = m''

Прикладом використання криптосистем на еліптичних кривих в Україні є ДСТУISO/IEC15946-1:2019«Інформаційнітехнології.Методизахисту.Криптографічніметодинаосновіеліптичнихкривих.Частина1.Загальні положення» (ISO/IEC 15946-1:2016, IDT); ДСТУ 9041:2020 «Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса»;

ДСТУISO/IEC15946-5:2019«Інформаційнітехнології.Методизахисту.Криптографічніметодинаосновіеліптичнихкривих.Частина5.Генеруванняеліптичнихкривих»(ISO/IEC15946-5:2017,IDT).

Вище було зазначено, що асиметричні криптосистеминедоцільнозастосовуватидляшифруваннявеликихобсягівданих через повільність процесу обчислювання.

Криптосистеми на еліптичних кривих не є виключенням, протеїхможнавикористовуватидлясистемавтентифікаціїта алгоритмів розподілення ключів.

Застосуванняеліптичнихкривихдляелектронного цифрового підпису,булозакріпленоустандартахСШАANSIX9.62,FIPS186-2 [8], тощо.

В Україні діє стандарт цифрового підпису, щобазується на еліптичнихкривих ДСТУ 4145–2002 [4].

Зазначимо,щобезпекасистемелектронногопідпису на еліптичних кривихспираєтьсяне лише на стійкість алгоритму на еліптичних кривих, але й на стійкістьвикористовуваної геш-функції.

Численні дослідження свідчать, що криптосистеми на еліптичних кривих перевершують інші системи з відкритим ключемзадвома важливимипараметрами, а саме за мироюзахищеності (зрозрахункунакоженбітключа) та зашвидкодієюпрограмноїйапаратноїреалізацій[5,6,7].

Це можнапояснititим,щодляобчисленняобернених функційнаеліптичнихкривих використовуються лишеалгоритмизекспоненційнимзростаннямтрудомісткості,тодіякдлязвичайних асиметричнихсистемзапропонованосубекспоненційніметоди.Згідно з дослідженнями Національного інституту стандартів і технологій СШАNIST

(NationalInstituteofStandardsandTechnology), рівеньстійкості,який забезпечується асиметричною криптосистемоюRSAпривикористанні ключа в 1024 біта,всистемах на еліптичних кривих зреалізовується при довжині ключа в 163 біти.Це забезпечує простішу як програмну, так і апаратну реалізацію, а такожможливість застосування більш коротких ключів [7].

У таблиці 3 наведено співвідношення довжин ключів, які використовуються у відповідних асиметричних криптосистемах.

Таблиця 3 - Відповідність довжини ключів у асиметричних криптосистемах згідно зNIST

Довжина ключа в криптосистемі, біт		Ключове співвідношення
Звичайний асиметричний алгоритм	На еліптичних кривих	
1024	163	1:6
3072	256	1:12
7680	384	1:20
15360	512	1:30

Криптосистеми на еліптичних кривих використовуютьсякриптоперетворення,щобазуютьсянаперетворенняхугрупіточокеліптичних кривихнадполями$GF(p)$,$GF(2^m)$,$GF(p^m)$.

Література

1 Криптографічний захист інформації: навч.посібн. з дисципліни «Криптографічний захист інформації» / О.В.Онацький, Л.Г.Йона, Ю.В.Бєлова; Держ.ун-т інтелект.технологій і зв'язку.- Одеса: Астропринт, 2023.-252с.

2 Системи банківської безпеки / Л.Г. Йона,О.В. Онацький, О.В. Швець// Навчальний посібник,- 2021, -58с.

3 Закон України "Про електронні документи та електроннийдокументообіг". [Електронний ресурс]. – Режим доступу:https://zakon.rada.gov.ua/laws/show/851-15#Text

4 ДСТУ 4145–2002. [Електронний ресурс]. – Режим доступу:https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798

5 ГорбенкоЮ.І.Інфраструктуривідкритихключів.Електроннийцифровий підпис. Теорія та практика: монографія / Ю.І. Горбенко,І.Д.Горбенко.– Харків: Видавництво «Форт»,2010.–608с.

6 Hankerson D. Guide to Elliptic Curve Cryptography / D. Hankerson,Menezes, S. Vanstone. – Springer-Verlag, 2004. – 358 p.

7 AnEllipticCurveCryptography(ECC)PrimerwhyECCisthenextgeneration of public key cryptography The Certicom 'Catch the Curve' WhitePaperSeriesJune 2004.– 24 p.

8 FIPS 186-2. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/csrc/media/publications/fips/186/2/archive/2000-01-27/ documents/fips186-2

Стрелковська І.В., д.т.н., професор; Росолик В.О., магістр 1 курсу навчання зі спеціальності 125 Кібербезпека та захист інформації
Міжнародний гуманітарний університет
i.strelkovskaya@mgu.edu.ua,

ДЕТЕКТУВАННЯ КРИТИЧНОГО DDoS-ТРАФІКУ КІБЕРАТАК

Анотація. *Розглянуто основні підходи щодо детектування DDoS-атак та виконано порівняннязасобів моніторингу, детектування та аналізу DDoS-трафіку з точки зору можливості використання у задачах детектування кібератак у реальному часі. Для детектування DDoS-трафіку запропоновано застосування вейвлет-функцій, показано приклад детектування трафіку атак за допомогою вейвлету Хаара.*

Сучасний підхід до забезпечення захисту від кібератак типу DDoS (Distributed Denial of Service Attack) базується на використанні засобів моніторингу, детектування та аналізу трафіку для систем виявлення вторгнень IDS (Intrusion detection system), міжмережних екранів, аналізаторів трафіку на базі сніферів (Tcpdump, Wireshark, Snort) та протоколів SNMP (NetFlow). Робота систем детектування кібератак ґрунтується на аналізі потоку запитів до мережного ресурсу, адже наявність атаки характеризується суттєвим зростанням кількості запитів. В цілому, використання сучасних методів є детектування за умов застосування різних сценаріїв мережної DDoS-атаки, таких як: флуди –SYN-Flood, ICMP-Flood, UDP-Flood, HTTP-Flood, амплифікації NTP, SNMP, SSDP, DNS, GRE, chargen, атаки на протокол TCP –SYN-Flood, SYN-ACK, FIN-Flood, атаки на протокол IP –фрагметовані IP-пакети [1]. Особливістю ICMP-Flood та UDP-Flood є непередбачуваний і некерований обсяг трафіку, який значно перевищує пропускну спроможність ресурсів і викликає перевантаження об’єктів мережі. Кібератаки DDoS, такі як, TCP –SYN, SYN-ACK, FIN-Floodспрямовані на певний стек мережних протоколів та виконують порушення з’єднань [1]. Кібератаки DDoS HTTP-Flood та Slowloris на прикладному рівні спрямовані на споживання ресурсів і порушення роботи протоколів взаємодії. Важливою задачею є детектування трафіку DDoS-атаки, оскільки трафік, залучений до атаки, часто надходить із кількох джерел і його важко відрізнити від легітимного трафіку. Для моніторингу, детектування та аналізу DDoS-трафіку можуть бути залучені програмно-апаратні засоби [1], порівняння яких наведено в табл. 1.

Таблиця 1 – Порівняння засобів моніторингу, детектування та аналізу DDoS-трафіку

Засіб моніторингу, детектування та аналізу DDoS-трафіку	Програмна реалізація засобу	Види загроз
Аналізатори трафіку	Wireshark	DDoS-атаки на мережні об’єкти, TCP (SYN, SYN-ACK, FIN-Flood)
Моніторинг пропускної здатності мережі	PRTG Network Monitor	DDoS-атаки на перевищення пропускної спроможності
Системи виявлення вторгнень IDS	Snort	Всі види DDoS-атак
Реєстратори мережних протоколів	NetFlow Analyzer	SYN-Flood та TCP-Flood, HTTP-Flood та Slowloris

Детектування трафіку DDoS-атаки може відбуватися за допомогою різних методів серед яких: статистичні методи, інтелектуальний аналіз даних, нейронні мережі та інші. Однак, оптимальним рішенням для детектування критичного трафіку DDoS-атак вважаються рішення, засновані на аналізу аномалій, в результаті якого відбувається порівняння характеристик шкідливого DDoS-трафіку з характеристиками легітимного трафіку, такими як, кількість та види запитів, кількість запитів певного типу або протоколу, швидкість надходження запитів та інше. При цьому, розгляд характеристик трафіку DDoS-атак визначає часті періодичні, короткі і значні «сплески» інтенсивності трафіку, а легітимний трафік має невелику амплітуду пульсацій, які відбуваються на протязі тривалого часу. Основною складністю такого підходу є необхідність мати

актуальні дані щодо легітимного та DDoS-трафіку, що безумовно, частіше не представляється можливим. Тому доцільно було б розглядати трафік на визначеному часовому відрізку з моменту значного збільшення кількості запитів, встановлюючи границю щодо кількості запитів, при порушенні якої буде детектуватися DDoS-атака [2].

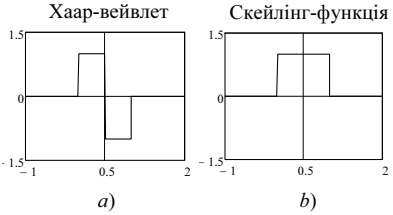
Огляд публікацій [3-6] щодо використання різних методів детектування DDoS-трафіку доводить доцільність використання методів машинного навчання, за умови значних часових витрат на навчання, а використання Байєсівського методу значно ускладнює процес детектування DDoS-трафіку. Використання методу сплайн-апроксимації, запропоновано в роботі [7-8], для детектування критичного DDoS-трафіку може бути використано, але значні та часті «сплески» інтенсивності вимагають іншого підходу, такого як використання апроксимації на базі вейвлет-функцій [8]. Детектування DDoS-трафіку на базі вейвлет-функцій дозволить:

– розглядати характеристики критичного DDoS-трафіку не тільки в частотній області, а й в часовій, що дозволить спростити локалізацію аномалій DDoS-трафіку;

– виявляти локальні особливості DDoS-трафіку (точки розриву, сплески інтенсивності, різкі перепади та самоподібність), які часто втрачають інші методи, наприклад, сплайн-функції;

– виконувати незалежний аналіз DDoS-трафіку на різних масштабах його змін, адже кожна компонента трафіку додатково описується масштабуючою скейлінг-функцією, що дозволяє визначити момент часу, в який змінилася та чи інша характеристика трафіку.

Розглянемо використання вейвлет-функцій Хаара для детектування DDoS-трафіку, для якого базисна вейвлет-функція $\psi(x)$та масштабуюча скейлінг-функція $\varphi(x)$ мають наступний вигляд, показаний на рис. 1,а та 1,б [7].



а) *б*)

Рисунок 1 – Базисна вейвлет-функція $\psi(x)$*а*) Хаар-вейвлет, *б*) Скейлінг-функція $\varphi(x)$

Для Хаар-вейвлету згідно [7-8], аналітичний запис його базисної материнської вейвлет-функції $\psi(x)$та скейлинг-функції $\varphi(x)$ має наступні форми, відповідно:

$$\psi(t)=\begin{cases}1,\ 0\le t<1/2,\\ -1,\ 1/2\le t<1,\\ 0,\ t<0,\ t\ge 1.\end{cases}\quad \varphi(t)=\begin{cases}1,\ 0\le t<1,\\ 0,\ t<0,\ t\ge 1.\end{cases} \qquad (1)$$

Базисна материнська вейвлет-функція $\psi(x)$ та скейлінг-функція $\varphi(x)$ належать ортогональним підпросторам Гібертового простору $L^2(R)$, що відповідає умовам [7]:

$$\sum_k h_k g_{k+2M}=0, \qquad (2)$$

де $h_k = \sqrt{2}\int \varphi(x)\overline{\varphi}(2x-k)dx$, $g_k = (-1)^k h_{(N-1)-k-1}$ – коефіцієнти розкладання, k, N – натуральні числа.

Згідно (2) визначаються залежність між коефіцієнтами h_k та g_k Хаар-вейвлету:

$$g_k = (-1)^k h_{2M-1-k}. \tag{3}$$

Отримані значення коефіцієнтів h_k та g_k визначають Хаар-вейвлет. При виконанні вейвлет-перетворення використовується розрахунок вейвлет-коефіцієнтів Хаар-вейвлету [7-8] використовуючі наступні формули прямого:

$$s_{j-1,k} = \frac{1}{\sqrt{2}}\left[s_{j,2k} + s_{j,2k+1}\right],\ d_{j-1,k} = \frac{1}{\sqrt{2}}\left[s_{j,2k} + s_{j,2k+1}\right] \tag{4}$$

та зворотнього перетворення

$$s_{j,2k} = \frac{1}{\sqrt{2}}\left[s_{j-1,k} + d_{j-1,k}\right], d_{j,2k+1} = \frac{1}{\sqrt{2}}\left[s_{j-1,k} - d_{j-1,k}\right], \tag{5}$$

де вейвлет-коэффициенты $s_{j,k}$ и $d_{j,k}$ визначаються з виразів:

$$s_{j-1,k} = \sum_m h_m s_{j,2k+m},\ d_{j-1,k} = \sum_m g_m s_{j,2k+m}, \tag{6}$$

де h_m, g_m – коефіцієнти апроксимації та розкладання.

Розглянемо легітимний трафік, змодельований за допомогою NetFlow Analyzer [ ], на відрізку [1500;2500] мс (рис. 2).

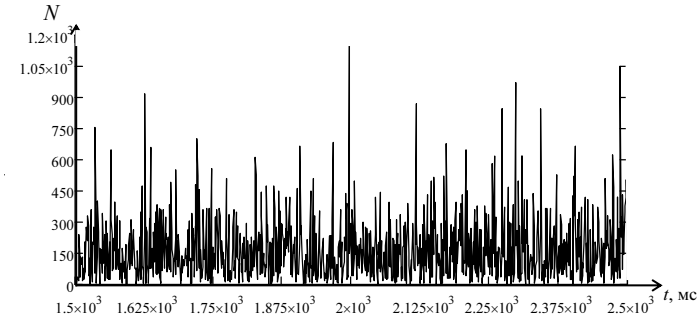


Рисунок 2 – Легітимний трафік на відрізку [1500;2500] мс

Трафік має часті сплески інтенсивності пакетів, іноді досить значні, а між моментами їх надходження існує довготривалий зв'язок, можна відмітити, що такий трафік має властивість самоподібності та володіє масштабною інваріантністю.

Розглянемо детектування трафіку атаки на відрізку [2100;2150] мс вважаючи, що на цьому відрізку можлива тільки одна DDoS-атака, яка буде характеризуватися різким «сплеском» інтенсивності запитів, що може привести до відмови в обслуговуванні.

Використаємо Хаар-вейвлет (1) для визначення аномалії трафіку та детектування значення такої аномалії. Використання вейвлет-функції Хаара для детектування характеристик трафіку показано на рис. 3.

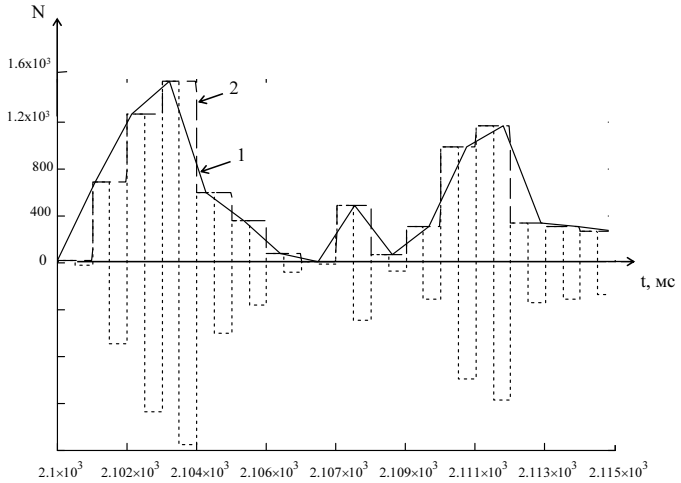


Рисунок 3 – Результати детектування DDoS-трафіку на відрізку [2100;2150] мс
1) легітимний трафік, 2) детектування трафіку з використанням вейвлету Хаара

Висновки

1. Розглянуто основні підходи щодо детектування DDoS-атак та виконано порівняння засобів моніторингу, детектування та аналізу DDoS-трафікуз точки зору можливості використання у задачах детектування кібератак у реальному часі.

2. Запропоновано використання апроксимації на базі вейвлет-функцій для детектування DDoS-трафіку за допомогою вейвлету Хаара.

3. Отримані результати для змодельованого легітимного трафіку та трафіку DDoS-атаки дозволяють детектувати аномалію трафіку.

Література

1. https://gridinsoft.ua/ddos

2. Strelkovskaya I., Kivalov S. «Detection and prediction of DDoS cyber attacks using spline functions», IEEE TCSET 2022: 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering(TCSET), Lviv-Slavske, Ukraine, February 22 – 26, 2022.– P. 710-713.

3. Y. Zang , F. Ni , Z. Feng, S. Cui and Z. Ding, «Wavelet Transform Processing for Cellular Traffic Prediction in Machine Learning Networks», 2015 IEEE China Summit and International Conference on Signal and Information Processing, China, July 2015 [Processing Conference on Signal and Information Processing, 2015].

4. Alghazzawi, D.; Bamasag, O.; Ullah, H.; Asghar, M.Z. Efficient Detection of DDoS Attacks Using a Hybrid Deep Learning Model with Improved Feature Selection. Appl. Sci. *2021,* 11*,* 11634.

5. Petrik, B.., Dubrovin, V.I. (2021). Detection of DoS attacks in network traffic by wavelet transform. Applied questions of mathematical modelling. 4(1), P. 186-196.

6. T. Radivilova, L. Kirichenko, O. Lemeshko and all, "Analysis of anomaly detection and identification methods in 5G traffic," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021.

7. I.V. Strelkovskaya, O. Lysiuk and R. Zolotukhin, «Comparative analysis of signals restoration by diffe-rent kinds of approximation» 3rd International Conference on Applied Innovations in IT, Vol. 3, Is. 1, pp. 29-35, March 2015 [Proceedings of the 3rd International Conference ICAIIT-2015, p. 29-35, 2015].

8. Strelkovskaya I. Multimedia Traffic Prediction Based on Wavelet- and Spline-extrapolation / I.Strelkovskaya, I. Solovskaya, A. Makoganiuk, T. Rodionova // IEEE International Black Sea Conference on Communications and Networking: proceedings of the 8th Black Sea Conference, Odessa, Ukraine, May 26-29, 2020.

9. https://www.manageengine.com/

Стрелковська І.В., д.т.н., професор, Шулішов В.В., магістр 1 курсу навчання зі спеціальності 125 Кібербезпека та захист інформації
Міжнародний гуманітарний університет
i.strelkovskaya@mgu.edu.ua,gradient@i.ua

ВИЯВЛЕННЯ АНОМАЛІЙ FLOOD-ТРАФІКУ КІБЕРАТАК

***Анотація**. Розглянуто основні види DDoS-атак та характеристики Flood-трафіку: SYN-Flood, ICMP-Flood, UDP-Flood. Встановлено, що виявлення аномалій Flood-трафіку DDoS-атак в мережі можливе за рахунок аналізу «сигнатур» трафіку або аналізу аномалій Flood-трафіку. Запропоновано використання сплайн-апроксимації для визначення аномалій Flood-трафікуDDoS-атак.*

Забезпечення безпеки мережної інфраструктури від загроз, зокрема атак, базується на використанні засобів моніторингу та аналізу трафіку. Такий моніторинг націлено насамперед на виявлення «сплесків» мережного трафіку, які є результатом несанкціонованого доступу, вірусів, атак, вторгнень та інших загроз. Серед таких загроз найчастіше зустрічаються атаки типу DDoS (Distributed Denial of Service Attack), таких як SYN-Flood, ICMP-Flood, UDP-Flood, HTTP-Flood [1]. ВизначенняDDoS-атак проводиться за допомогою аналізу аномалій мережного трафіку – пошуку відхилень від визначених характеристик трафіку. В той же час, DDoS-атаки рівнів L2-L4 (UDP-Flood, HTTP-Flood, SYN-Flood, ICMP-Flood) переважно генерують значний обсяг трафіку, а DDoS-атаки прикладного рівня L7 зовсім не вимагають генерації значного обсягу трафіку та складно ідентифікуються звичайними системами [1-2].

Відомо [1-2], що процес виявлення аномалій Flood-трафіку DDoS-атаки в інфокомунікаційній мережі використовує два підходи. Перший підхід ґрунтується на аналізі «сигнатур» трафіку, шаблонів легітимного або шкідливого Flood-трафіку, які визначають DDoS-атаку. Слід зауважити, що виявлення аномалій DDoS-атаки на основі «сигнатур» використовується для відомих типів Flood-трафіку DDoS-атаки. Таке виявлення виконується шляхом порівняння даних, що характеризують поточний трафік з Flood-трафіком, характерними для DDoS-атак. Однак цей метод виявлення шкідливого Flood-трафіку на основі «сигнатур» має значну кількість недоліків. По-перше, виявлення DDoS-атак на основі сигнатур може бути неефективним при виявленні нових або модифікованих типів Flood-трафіку DDoS-атак. По-друге, для кожної «сигнатури» потрібна база даних, яка має безліч «сигнатур». Такий процес завжди ресурсомісткий, він може використовувати всю пропускну здатність і зробить даний тип виявлення вразливим для DDoS-атак [2].

Другим підходом щодо ідентифікації DDoS-атаки є метод виявлення на основі аномалій, побудований на евристиці виявлення поведінки трафіку, яка виходить за межі нормальної роботи. Цей підхід оцінює поточний стан обслуговування трафіку з аномалією, яка викликана Flood-трафіком DDoS-атаки. Безумовною передумовою виявлення Flood-трафіка DDoS-атаки є визначення поточних характеристик трафіку мережі з подальшим пошуком аномалій у його структурі. Тоді будь-яка відмінність у структурі легітимного трафіку, що перевищує певне значення, визначає Flood-трафіком DDoS-атаки [1-2]. Алгоритм визначення аномалій Flood-трафіка DDoS-атаки показано на рис. 1.

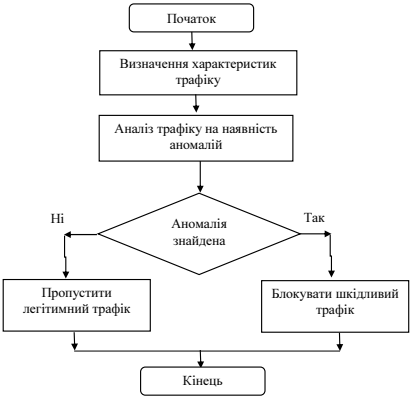


Рисунок 1 –Алгоритм виявлення DDoS-атак

Алгоритм базується на зібраних даних трафіку програмами сніфферами, встановленими на вузлах мережної інфраструктури та порівнюється з характеристиками легітимного трафіку. З огляду на вищезазначене, дослідження аномалій Flood-трафіку та вибір певного методу, який би дозволив забезпечити необхідну точність визначення DDoS-атак як за допомогою «сигнатур», так і за допомогою аномалій, є актуальним. Сплайн-апроксимація [3-4], має хорошу збіжність у порівнянні до поліноміальної апроксимації, сплайни більш стійкі щодо локальних збурень, тобто поведінка сплайна в точці не позначається на поведінці сплайну в цілому, крім того, сплайни володіють корисними екстремальними властивостями.

Розглянемо виявлення аномалій Flood-трафіку DDoS-атак за допомогою сплайн-апроксимації [3-6]. Вихідний Flood-трафік DDoS-атаки, отриманий за допомогою Dataset/ddos-attack-network [7], показано на рис. 2.

Отримані дані легітимного трафіку (рис. 1) використовували агреговані п’ятихвилинні інтервали, середні значення наступних величин: кількість байт в секунду, кількість пакетів в секунду, кількість потоків в секунду, величина середнього розміру TCP-пакета. Наявність різких «сплесків» відповідає певним групам аномалій. Огляд легітимного трафіку, показаного на рис. 1, дозволяє зробити наступні висновки:

– трафік характеризується значною кількістю «сплесків» інтенсивності пакетів,

– трафік має ознаки самоподібності зі значенням параметра Херста H = 0,8.

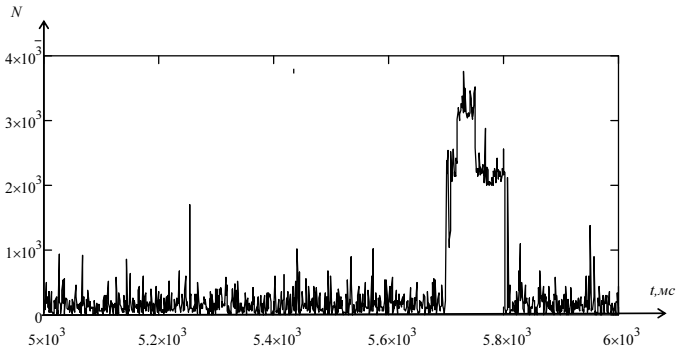


Рисунок 2 –Flood-трафік DDoS-атаки, отриманий за допомогою Dataset/ddos-attack-network

Розглянемо використання сплайн-апроксимації для визначення аномалій Flood-трафіка DDoS-атаки. Використаємо кубічний сплайн $S_3(t)$ для апроксимації трафіку, показаного на рис. 1 на проміжку [5500;6000] мс. Нехай на відрізку [0;T] задані значення характеристик трафику, а саме кількість N - пакетів. Розіб'ємо цей відрізок [0;T] точками Δ: $0 = t_0 < t_1 < ... < t_N = T$ на проміжки $[t_i; t_{i+1}]$, $i = \overline{0, N-1}$, на кожному з яких побудуємо многочлен визначеного ступеню [5].

В якості такого многочлену використуємо кубічний сплайн та отримаємо на проміжку [0;T] кусково-неперервну функцію, яка і буде визначати кубічний сплайн. Нехай на відрізку [0;T] у вузлах сітки Δ: $0 = t_0 < t_1 < ... < t_N = T$ задані значення функції $s_i = s(t_i)$, $i = \overline{0, N}$.

Згідно [5], інтерполяційний кубічний сплайн $S_3(t_i)$ відповідає умовам:

$$S_3(t_i) = S_i,\ S_3(t_{i+1}) = S_{i+1},\ i = \overline{0, N-1}, \qquad (1)$$

– на кожному з відрізків $[t_i; t_{i+1}]$, $i = \overline{0, N-1}$ він є многочленом третього ступеню,

– на всьому відрізку [0;T] має неперервність других похідних $S_3^{"}(t_i) = M_i,\ S_3^{"}(t_{i+1}) = M_{i+1},\ S_3^{"}(t_0) = M_0,\ S_3^{"}(t_1) = M_1$.

Тоді для $S_3(t)$:

$$S_3(t) = f_i(1-t) + f_{i+1}t - \frac{h_i^2}{6}t(1-t)\left[(2-t)M_i + (1+t)M_{i+1}\right] t \in [t_i, t_{i+1}],\ i = \overline{0, N-1}. \qquad (2)$$

Розглянемо трафік на проміжку [0;T], задавши рівномірну сітку розбиття. Для кожної точки розбиття відомі значення кількості пакетів у кожному вузлі інтеполяції. Використовуючи кубічний інтерполяційний сплайн вигляду (2) та вирази (1), (2), отримаємо апроксимацію трафіку, показану на рис. 3.

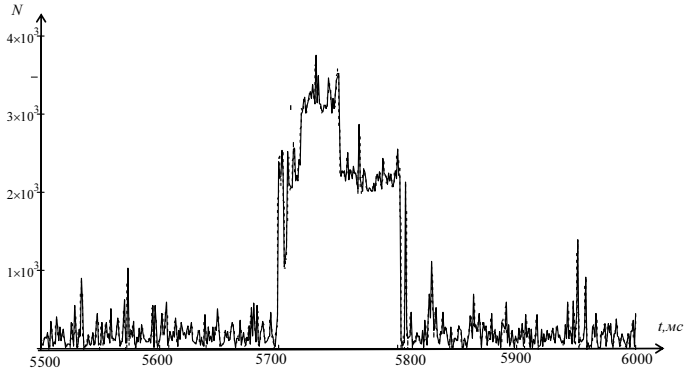


Рисунок 3 – Сплайн-апроксимація Flood-трафіку DDoS-атаки на базі кубічного сплйну на відрізку [5500; 6000] мс

Висновки

1. Розглянуто основні види DDoS-атак та характеристики різних видів Flood-трафіку: SYN-Flood, ICMP-Flood, UDP-Flood. Встановлено, що виявлення аномалій Flood-трафіку DDoS-атак в мережі можливе за рахунок аналізу «сигнатур» трафіку або аналізу аномалій Flood-трафіку.

2. Запропоновано використання сплайн-апроксимації для визначення аномалій Flood-трафікуDDoS-атак на базі інтерполяційного кубічного сплайну.

3. Отримані результати для Flood-трафіку дозволяють визначити аномалію трафіку та надає можливість в реальному часі виконати дії щодо її ліквідації.

Література

1. Strelkovskaya I., Kivalov S. «Detection and prediction of DDoS cyber attacks using spline functions», IEEE TCSET 2022: 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering **(**TCSET**),** Lviv-Slavske, Ukraine, February 22 – 26, 2022.– P. 710-713.

2. T. Radivilova, L. Kirichenko, O. Lemeshko and all, "Analysis of anomaly detection and identification methods in 5G traffic," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021.

3. Strelkovskaya I., Solovskaya I., Strelkovska J. (2021), «Spline-Approximation and Spline-Extrapolation Methods in Telecommunication Problems», Current Trends in Communication and Information Technologies. IPF 2020. Lecture Notes in Networks and Systems, vol 212, Springer, Cham, 2021, P. 3-22.

4. Strelkovskaya I.V. Self-similar traffic in G/M/1 queue defined by the Weibull distribution/ I.V. Strelkovskaya, T.I. Grygoryeva, I.N. Solovskaya // Radioelectronics and Communications Systems. – 2018. – V. 61, № 3 (2018). – P. 173-180.

5. Ahlberg J.H., Nilson E.N., Walsh J.L. The Theory of Splines and Their Applications, Academic Press, New York, 1967.

6. Popovsky V.V., Strelkovskaya I.V. Accuracy of procedures for filtering, extrapolating and interpolating random processes, Telecommunication problems, 1(3), 2011. P. 3-10.

7. https://www.kaggle.com

Володін Дмитро Вікторович ,
Магістр, спеціальність 125 «Кібербезпека та захист інформації»
volodindimka@gmail.com
Науковий керівник
Йона Лариса Григорівна, к.т.н., доцент
Міжнародний гуманітарний університет
yonalarisa66@gmail.com

СИСТЕМАТИЗАЦІЯ ТА АНАЛІЗ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ВІДПОВІДНО ДО ЇХ ФУНКЦІОНАЛЬНОГО ПРИЗНАЧЕННЯ

Анотація *У статті розглядаються сучасні криптографічні алгоритми, систематизовані та проаналізовані відповідно до їх функціонального призначення. Описано ключові алгоритми, включаючи симетричні та асиметричні шифрувальні алгоритми, алгоритми хешування та алгоритми для цифрових підписів. Особлива увага приділена аналізу швидкодії, надійності та специфічних особливостей кожного алгоритму. Представлено порівняльну таблицю, яка містить інформацію про призначення, тип, швидкодію та надійність для кожного з алгоритмів.*

Вступ

Криптографічні алгоритми є основними елементами забезпечення захисту інформації в сучасному цифровому світі. Застосування відповідного криптографічного алгоритму залежить від конкретних потреб користувача та варіюється від захисту особистих даних користувачів до забезпечення безпеки в мережах, фінансових транзакціях та інших критично важливих системах. Для різних потреб використовуються алгоритми, що поділяються на два великих класи: симетричні та несиметричні криптоалгоритми.

Систематизація криптографічних систем

Симетричні криптографічні алгоритми є подовженням історичного розвитку класичних методів шифрування (перестановки, заміни та гамування). Шифрування відбувається шляхом каскадного, послідовного використання базових перетворень зі зміною ключа на кожному кроці. Особливістю симетричних систем є те, що шифрування відбувається блоками відкритого тексту фіксованої довжини, при цьому використовується один і той самий ключ для зашифрування та розшифрування даних. Симетричні алгоритми відрізняються своєю швидкістю та ефективністю, що робить їх придатними для обробки великої кількості даних в реальному часі.

Першим світовим стандартом шифрування був алгоритм **DES (Data Encryption Standard)**. Сьогодні він вважається небезпечним через відносно коротку довжину ключа в 64 біти (зокрема, інформаційних 56 біт). Для можливого використання та підвищення криптостійкості застосовується удосконалена версія цього алгоритму **3DES** (Triple DES або Triple Data Encryption Standard), що використовує три ключі для шифрування блоку даних, довжиною 64 біти. Кожен з цих ключів має довжину 56 біт, що відповідає стандартному розміру ключа для DES. Оскільки 3DES використовує три ключі, загальна ефективна довжина ключа в 3DES становить 168 біт (56 біт × 3). Однак, через деякі технічні обмеження та специфіку алгоритму, реальна криптостійкість 3DES наближається до 112 біт. Це пов'язано з можливістю атаки "зустріч посередині" (meet-in-the-middle attack), яка значно знижує ефективну криптостійкість.

На зміну алгоритмуDES за конкурсом було обрано удосконалений стандарт шифрування **AES (Advanced Encryption Standard)**, що прийнятий у 2001 році. Стандарт AES має довжину блоку 128 біт та можливість обирати довжину ключа 128, 192 та 256 біт. Він вважається одним із найбезпечніших блочних алгоритмів шифрування і широко використовується в сучасних системах захисту інформації [1].

Існує багато інших криптостійких сучасних алгоритмів шифрування, однак головною слабкістю усіх симетричних алгоритмів є управління ключами, всі учасники обміну повинні мати доступ до одного і того ж секретного ключа.

Алгоритми хешування ефективні для забезпечення цілісності даних. Вони швидко обчислюють хеші та мають широкий спектр застосувань. Важливо вибирати сучасні алгоритми, щоб уникнути вразливостей до колізій. Алгоритми хешування створюють фіксованої довжини хеш-код (вихід) з будь-якого вхідного повідомлення. Вони широко використовуються для перевірки цілісності даних та створення цифрових підписів.Популярним є алгоритм **MD5** (Message Digest Algorithm 5), однак тепер він вважається небезпечним через виявлення колізій. Сьогодні широко застосовується алгоритм **SHA-256** (Secure Hash Algorithm 256-біт) для створення хешів у різних системах безпеки, включаючи блокчейн [1,6].

Асиметричні криптографічні алгоритми ще мають назву несиметричні криптосистеми чи криптосистеми з відкритим ключем, а також звуться двоключовими криптографічними системами.

Основним призначенням несиметричних алгоритмів є автентифікація та розподілення ключів. Це зумовлено тим, що асиметричні алгоритми використовують пару ключів: відкритий та закритий ключ. Це забезпечує більш високий рівень безпеки, оскільки закритий ключ зберігається в таємниці та нікому не передається, крім того дуже зручним є можливість вільного передавання відкритого ключа. Однак використання довгих ключів та обробка великих чисел призводить до зниження швидкості роботи системи. Більш повільна обробка даних в асиметричних алгоритмах обмежує застосування їх для процесу шифрування та використовується тільки для захисту невеликих обсягів даних. Асиметричні алгоритми менш ефективні за симетричні через вищу обчислювальну складність при шифруванні, але ідеально підходять для обміну ключами та підтвердження справжності документообігу.

Одним із найвідоміших асиметричних алгоритмів є алгоритм **RSA** . Він може працювати як в режимі шифрування, так і в режимі цифрового підпису та використовує великі прості числа для генерації пари ключів. Застосовується в протоколах SSL/TLS для захисту інтернет-трафіку.

Алгоритми для цифрових підписів забезпечують високий рівень безпеки для автентифікації та валідації даних. Вибір між різними алгоритмами залежить від вимог до швидкості, довжини ключа та рівня безпеки. Ці алгоритми забезпечують автентифікацію даних і підтвердження їх походження. Стандартний алгоритм для цифрових підписів, прийнятий урядом США є **DSA** (Digital Signature Algorithm) [1;6].

Різновидом асиметричних алгоритмів є алгоритми на еліптичних кривих (Elliptic Curve Cryptography, ECC).[4]. Алгоритми на еліптичних кривих є сучасними методами криптографічного захисту інформації, які забезпечують високу безпеку з використанням менших розмірів ключів у порівнянні з традиційними методами, такими як RSA. Наприклад, ECC з 256-бітним ключем забезпечує той самий рівень безпеки, що й RSA з 3072-бітним ключем. Криптографічні перетворення в ECC базуються на математичних властивостях еліптичних кривих над скінченими полями. Основна перевага ECC полягає у високій ефективності та меншій вимозі до обчислювальних ресурсів. Це робить ECC не лише швидшим, але й більш економічним з точки зору ресурсів. Завдяки цьому, алгоритми на еліптичних кривих стають ідеальними для застосувань, де обмежена обчислювальна потужність, таких як мобільні пристрої та вбудовані системи. Також алгоритми на еліптичних кривих застосовуються у різних криптографічних протоколах, таких як SSL/TLS для захисту інтернет-з'єднань, цифровий підпис, а також у системах шифрування та автентифікації.

Завдяки своїм перевагам, ECC стає все більш популярним вибором для забезпечення безпеки в сучасних інформаційних системах, де необхідно збалансувати високу безпеку та ефективність [5].

Сучасні алгоритми на еліптичних кривих охоплюють різноманітні криптографічні протоколи, які використовують властивості еліптичних кривих для забезпечення високого рівня безпеки. Найпоширеніші алгоритми можна поділитиза призначенням. Так, приміром, для шифрування застосовується **ECIES** (Elliptic Curve Integrated Encryption Scheme), гібридна схема шифрування, яка поєднує симетричне та асиметричне шифрування для забезпечення конфіденційності, цілісності та автентичності повідомлень.

Для автентифікації можна застосовувати алгоритм **ECDSA** (Elliptic Curve Digital Signature Algorithm), що забезпечує високий рівень безпеки з меншими розмірами ключів, порівняно з традиційними алгоритмами, такими як DSA або RSA. Варіантом цифрового підпису на еліптичних кривих, який використовує криві Едвардса (Edwards curves)є **EdDSA** (Edwards-Curve Digital Signature Algorithm) Відзначається високою швидкістю та безпекою. Одним із популярних реалізацій є Ed25519.

Крім того, сучасним алгоритмом цифрового підпису на еліптичних кривих є стандарт України **ДСТУ 4145–2002** [2].

Алгоритми розподілу ключів застосовуються для захисту створеного секретного ключа в незахищеному каналі. У багатьох сучасних криптографічних системах для розподілення ключів застосовується протокол **Діффі-Хеллмана** та його розповсюджена версія на еліптичних кривих **ECDH** (Elliptic Curve Diffie-Hellman), алгоритм обміну ключами, який дозволяє двом сторонам обмінюватися секретним ключем через незахищений канал. Використовується для встановлення з'єднань у багатьох інтернет-протоколах, таких як TLS.

Кожен з цих алгоритмів має свої особливості та переваги, які роблять їх відповідними для різних застосувань у сучасних інформаційних системах, від захисту інтернет-з'єднань до забезпечення безпеки мобільних додатків і вбудованих систем.

У таблиці 1 представлено аналіз криптографічних алгоритмів відповідно до їх функціонального призначення. Ця таблиця допоможе краще зрозуміти відмінності між сучасними криптографічними алгоритмами та вибрати найбільш підходящий для конкретних потреб.

Висновки

Криптографічні алгоритми грають вирішальну роль у забезпеченні безпеки інформації. Їх вибір залежить від конкретного застосування та вимог до безпеки.

Симетричні алгоритми використовуються для обробки великих обсягів даних, зокрема, алгоритми хешування – для забезпечення цілісності даних;

Асиметричні алгоритми використовуються для обміну ключами, для автентифікації за допомогою цифрового підпису та можливості шифрування невеликих обсягів даних.

Систематизація та аналіз криптографічних алгоритмів відповідно до їх функціонального призначення допомагає краще зрозуміти їхні сильні та слабкі сторони, що є ключовим для ефективного використання у різних сферах інформаційної безпеки.

Таблиця 1 – Аналіз криптографічних алгоритмів відповідно до їх призначення

Алгоритм	**Призначення**	**Тип**	**Швидкодія**	**Надійність** (довжина ключа, біт)	**Примітки**
DES	Шифрування даних	Симетричний	Висока	Низька (**64**/56 біт)	Застарілий, замінений на більш надійні алгоритми
3DES	Шифруванння даних	Симетричний	Висока	Середня (**168**/112 біт)	Надійний алгоритм
AES	Шифрування даних	Симетричний	Висока	Дуже висока (**128, 192, 256**)	Стандарт для урядів і комерційних організац.
IDEA	Шифрування даних	Симетричний	Висока	Висока (довжина ключа**128**біт)	Європейський стандарт шифрування

ДСТУ 7624:2014« Калина»	Шифрування даних	Симетричний	Висока	Дуже висока (**128, 256, 512**-біт)	Національний стандарт шифрування ДСТУ 7624:2014
MD5	Хешування даних	Симетричний/хешування	Висока	Низька	Не рекомендується через вразливості до колізій
SHA-256	Хешування даних	Симетричний/хешування	Висока	Дуже висока	Використовується в блокчейнах, цілісності даних
Протокол Діффі-Хеллмана	Розподіл ключів	Асиметричний	Середня	Висока	Використовується для створення та розпо ділення ключів по незахищеному каналу
ECDH Версія протоколу Діффі-Хелмана наЕС	Розподіл ключів	Асиметричний	Висока	Висока	Використовується для встановлення з'єднань у багатьох інтернет-протоколах, таких як TLS.
RSA	Шифрування даних невелик. обсягу, цифровий підпис	Асиметричний	Низька (порівнянно з симетричними)	Висока (довжина ключів1024, 2048, 4096 біт)	Широко використовується, висока обчислювальна складність
DSA	Цифровий підпис	Асиметричний	Середня	Висока (довжина ключів 1024 біт)	Стандарт для цифрових підписів
ECDSA Версія протоколу DSA на ЕС	Цифровий підпис	Асиметричний	Висока	Дуже висока (довжина ключа 160 біт)	Висока безпека при меншій довжині ключа.

Література

1 Криптографічний захист інформації: навч.посібн. з дисципліни «Криптографічний захист інформації» / О.В.Онацький, Л.Г.Йона, Ю.В.Бєлова; Держ.ун-т інтелект.технологій і зв'язку.- Одеса: Астропринт, 2023.-252с.

2 ДСТУ 4145–2002. [Електронний ресурс]. – Режим доступу:https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798

3 ГорбенкоЮ.І.Інфраструктуривідкритихключів.Електроннийцифровий підпис. Теорія та практика: монографія / Ю.І. Горбенко,І.Д.Горбенко.– Харків: Видавництво «Форт»,2010.–608с.

4 HankersonD.GuidetoEllipticCurveCryptography/D.Hankerson,

5 Menezes, S. Vanstone. – Springer-Verlag, 2004. – 358 p.

6 AnEllipticCurveCryptography(ECC)PrimerwhyECCisthenextgeneration of public key cryptography The Certicom 'Catch the Curve' WhitePaperSeriesJune 2004.– 24 p.

7 Системи банківської безпеки / Л.Г. Йона,О.В. Онацький, О.В. Швець// Навчальний посібник,- 2021, -58с.

Стрелковська І.В., д.т.н., професор,
Полякова Ю.С, магістр 1 курсу навчання
зі спеціальності 125 Кібербезпека та захист інформації
Міжнародний гуманітарний університет
i.strelkovskaya@mgu.edu.ua,polyakova19@ukr.net

СПЛАЙН-ЕКСТРАПОЛЯЦІЯ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ

Анотація. *Розглянуто можливість використання сплайн-екстраполяції в задачах прогнозуваннякібератак DDoS.Розглянуто сплайн-екстраполяцію трафіку DDoS-атак з використанням кубічних сплайнів.Встановлено, що прогнозування кібератак DDoS з використанням сплайн-екстраполяції дозволяє збільшити точність прогнозування, спростити процес обчислень та може бути використано при прогнозуванні в реальному масштабі часу.*

Однією з найбільш поширених і найефективніших кібератак є DDoS (Distributed Denial of Service) атака, яка реалізується одночасним, масовим надсиланням інформаційних запитів на сервер з метою його перевантаження. Кількість DDoS-атак та їхніх різновидів безперервно збільшується, атаки стають більш інтенсивними та руйнівними, тривалими й періодичними, щоразу включають більшу кількість цілей. Відомі DDoS-атаки часто досить складні і вимагають вивчення особливостей характеристик трафіку конкретної DDoS-атаки, таких як, інтенсивність надходження пакетів трафіку, тривалість обслуговування та час затримки пакетів [1], [2].

Виявлення DDoS-атак є складною задачею через значну кількість джерел DDoS-атак і особливостей їхнього трафіку. Зазвичай, процес виявлення DDoS-атак базується на двох підходах, перший – за допомогою відомих «шаблонів» трафіку DDoS-атак, коли виконується порівняння «шаблону» трафіку кібератаки та легітимного трафіку. Іншим підходом є виявлення аномалій, яке використовує вивчення змін поведінки трафіку, які виходять за межі нормальної роботи. Для оцінки трафіку DDoS-атак можуть використовуватися різні методи, серед яких: статистичні методи, інтелектуальний аналіз даних, штучний інтелект, вейвлет-аналіз та інші [3] – [5].

Іншим підходом може бути прогнозування характеристик DDoS-трафіку та виявлення кібератаки. Вирішення завдання прогнозування характеристик DDoS-трафіку кібератак дозволить за допомогою довгострокового або короткострокового прогнозу визначити характеристики шкідливого трафіку щодо їхнього попередження. До основних задач прогнозування кібератак DDoS слід віднести наступні задачі:

– прогнозування характеристик трафіку DDoS-атак, які характеризуються частими та значними «сплесками» інтенсивностей трафіку;

– прогнозування характеристик трафіку DDoS-атак для можливостей визначати локальні особливості DDoS-трафіку (точки розриву, сплески інтенсивності, різкі перепади та самоподібність);

– прогнозування характеристик трафіку DDoS-атак на різних часових відрізках, визначаючи момент часу, в який змінилася та чи інша характеристика трафіку.

Використання сплайн-екстраполяції при вирішенні завдань прогнозування та оцінки станів даних, сигналів та трафіку показано в роботах [2], [3]. Використання цього методу дозволило покращити результати прогнозування характеристик трафіку різних додатків з використанням сплайн-функцій (лінійних, квадратичних, квадратичних B-сплайн, кубічних, кубічних B-сплайн, сплайн Ерміта). Тому доцільним буде використання сплайн-екстраполяції для прогнозування трафіку DDoS-атак.

Метою даної роботи є вирішення задачі прогнозування характеристик трафіку DDoS-атак з використанням сплайн-екстраполяції.

Розглянемо прогнозування трафіку DDoS-атаки на відрізку [2000;3000] мс за допомогою сплайн-екстраполяції. Нехай трафік має DDoS-атаку, яка характеризується різким «сплеском» інтенсивності надходження пакетів (рис. 1).

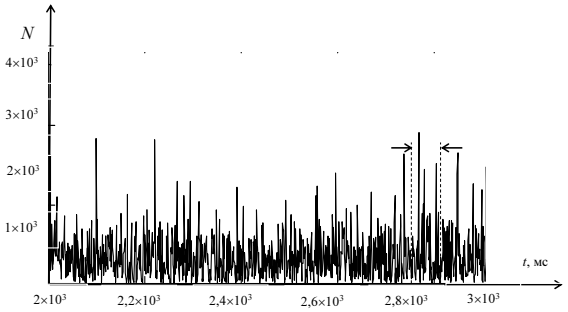


Рисунок 1 – Трафік на відрізку [2000;3000] мс

Нехай на відрізку $[a;b]$ розглядається трафик на якому відбулася DDoS-атака. Розіб'ємо цей відрізок $[a;b]$ точками Δ: $a = x_0 < x_1 < ... < x_N = b$ на проміжки $[x_i,x_{i+1}]$, $i = 0$, …, $N - 1$, на кожному з яких побудуємо многочлен визначеного ступеню. В якості такого многочлена будемо використовувати кубічний сплайн.

Кубічний інтерполяційний сплайн $S_3(x)$ для $x \in [x_i, x_{i+1}]$, $i = 0, 1,\ldots, N - 1$ має вигляд [2]:

$$S_3(x) = f_i(1-t)^2(1+2t) + f_{i+1}t^2(3-2t) + +m_i h_i t(1-t)^2 - m_{i+1}h_i t^2(1-t), \qquad (1)$$

де $t = \dfrac{x - x_i}{h_i}$, $S_3(x_i) = f_i$, $S_3(x_{i+1}) = f_{i+1}$, $m_i = S'(f;x_i)$.

Для визначення кубічного сплайну вигляду (1) на відрізку $[a;b]$ використовуються граничні умови [2],[3]:

$$S'(f;a) = f'(a),\ S'(f;b) = f'(b). \qquad (2)$$

Розглядаючи трафік на відрізку $[a;b]$, задано рівномірну сітку розбиття зі кроком $h_i = h$, $i = 0, 1,\ldots, N - 1$, $h = \dfrac{b-a}{N}$. Для побудови кубічного сплайну, використовуємо значення інтенсивності трафіку у вузлах інтерполяції x_i, $i = 0, 1,\ldots, N$. Використовуючи властивості довгострокової залежності самоподібного трафіку, можливо екстраполювати його значення поза заданим відрізком часу.

Відповідно до [4], [5], трафік кібератак DDoS має властивість самоподібності і, відповідно, характеризується довгостроковою залежністю окремих реалізацій за проміжок часу, схожих як формою, так і візуально. Ступінь самоподібності трафіку визначається значенням параметра Херста $0,5 \le H < 1$. Використовуюи властивості самоподібності трафіку DDoS-атаки, можна отримати значення прогнозованого трафіку на заданому проміжку часу.

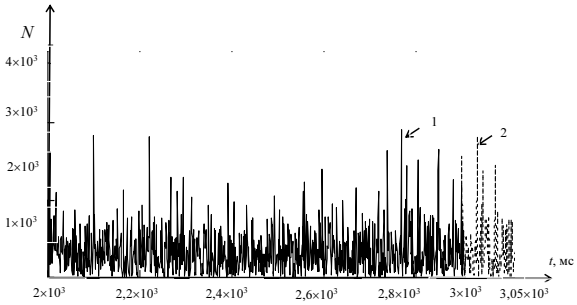


Рисунок 2 – Результати екстраполяції трафіку DDoS-атаки з використанням кубічного сплайну на відрізку [3000;3050] мс, 1) трафік DDoS атаки, 2) екстраполяція трафіка з використанням кубічного сплайна

Визначимо похибку сплайн-екстраполяції трафіка DDoS-атаки за допомогою кубічного сплайна, використовуючи фрагмент екстраполяції трафіку, показано на рис. 3.

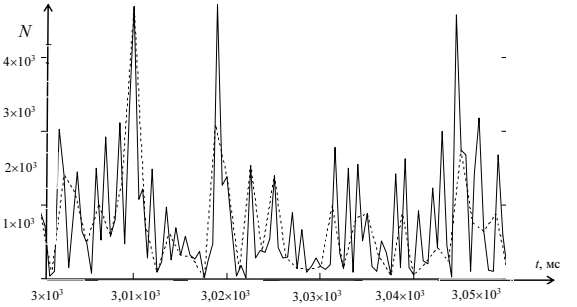


Рисунок 3 – Фрагмент екстраполяції трафіку DDoS-атаки з використанням кубічного сплайну на відрізку [3000;3050] мс, 1) трафік DDoS атаки, 2) екстраполяція трафіка з використанням кубічного сплайна

Використовуючи кубічний сплайн для визначення DDoS-атаки, отримано екстраполяцію трафіку DDoS-атаки, яку показано на рис. 2. Неважко бачити, що використання кубічних сплайнів має похибку, яка найчастіше з'являється на відрізках трафіку DDoS кібератаки, де інтенсивність атаки трафіку має «сплески». Результати зведемо в табл. 1.

Таблиця 1 – Похибка похибку сплайн-екстраполяції трафіка DDoS-атаки за допомогою кубічного сплайна

Проміжок	Значення проміжка, мс	Значення похибки
$[x_0;x_1]$	[3000; 3010]	1,1
$[x_1;x_2]$	[3010; 3020]	5,05
$[x_2;x_3]$	[3020; 3030]	1,01
$[x_3;x_4]$	[3030; 3040]	5,6
$[x_4;x_5]$	[3040; 3050]	3,2

Висновки

1. Розглянуто можливість використання сплайн-екстраполяції в задачах прогнозування кібератак DDoS.

2. Запропоновано використання сплайн-екстраполяції для визначення трафікуDDoS-атак на базі інтерполяційного кубічного сплайну.

3. Встановлено, що прогнозування кібератак DDoS з використанням сплайн-екстраполяції дозволяє збільшити точність прогнозування, спростити процес обчислень та може бути використано у реальному масштабі часу.

Література

1. T. Radivilova, L. Kirichenko, O. Lemeshko and all, "Analysis of anomaly detection and identification methods in 5G traffic," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021.

2. Strelkovskaya I.V. Modeling of self-similar traffic / I.V. Strelkovskaya, I.N. Solovskaya, N.V. Severin // Proceedings of the 4rd International Conference on Applied Innovations in IT (ICAIIT-2016), Vol. 1, Is. 5, Koethen, Germany, March, 10, 2016.– Anhalt University of Applied Sciences. – P. 61-64.

3. Strelkovskaya I.V. Self-similar traffic in G/M/1 queue defined by the Weibull distribution/ I.V. Strelkovskaya, T.I. Grygoryeva, I.N. Solovskaya // Radioelectronics and Communications Systems. – 2018. – V. 61, № 3 (2018). – P. 173-180.

4. Rikli, N.-E. Self-similarity and stationarity of increments in VBR video / N.-E. Rikli // Journal of king saud university – Computer and information sciences. – 2019. – № 24. – P. 7-16.

5. P. Dymora, M. Mazurek, «Network Anomaly Detection Based on the Statistical Self-similarity Factor,» Lecture Notes in Electrical Engineering, 324(1). pp. 271-287. https://doi.org/10.1007/978-3-319-11248-0_21

СЕКЦІЯ 4. ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УДК 621.391

Стрелковська І. В., д.т.н., професор
Міжнародний гуманітарний університет, Одеса, Україна
i.strelkovskaya@mgu.edu.ua
Балик А. Д., магістр з інженерії програмного забезпечення
Міжнародний гуманітарний університет, Одеса, Україна
acreed777@gmail.com

ПРОГРАМНА РЕАЛІЗАЦІЯ ЗНАХОДЖЕННЯ ХАРАКТЕРИСТИК ЯКОСТІ САМОПОДІБНОГО ТРАФІКУ МЕРЕЖІ LTE

Аннотація. *Важливою проблемою при підтримці трафіку і наданні високошвидкісних послуг в мережі LTE-Advanced є підтримка трафіку із заданими значеннями характеристик якості QoS (Quality of Service), які представляють собою стандартні значення часу затримки пакетів, ймовірності втрати пакетів і пропускної здатності. Для відновлення трафіку розроблено програму знаходження характеристик самоподібного трафіку мережі LTE за допомогою програмних продуктів, а саме програмного середовища MATLAB та мови програмування Python. Вирішення цієї задачі має практичне значення щодо передбачення необхідної кількості буферних пристроїв об'єктів мережі, що забезпечують можливість надання високошвидкісних послуг сервісів й додатків в мережі мобільних операторів.*

При практичному застосуванні концепції розвитку мережі LTE-Advanced на практиці часто виникають завдання, пов'язані з вивченням характеристик самоподібного трафіку. Вирішення цих завдань пов'язане з моделюванням самоподібного трафіку і дозволяє визначити залежність між обсягом трафіку, який обслуговується, з підтримкою характеристик якості обслуговування QoS і параметрами мережі, що забезпечують ефективне використання доступних мережевих ресурсів.

Розглянемо рішення задачі знаходження характеристик якості самоподібного трафіку для системи масового обслуговування (СМО) вигляду Wв/M/1/∞ [1], для якої проміжки між пакетами, які поступають на обслуговування, описуються розподілом Вейбула Wв.

З огляду на те, що трафік в мережі IoT пакетний та неоднорідний, так як формується різними сервісами та мережевими додатками, характеризується проявом самоподібних властивостей, має на увазі наявність довгострокової залежності між моментами прийому пакетів, тому визначається кореляційною функцією в різних точках часу. Параметр Херста H, $0.5 \le H < 1$, використовується як кількісна оцінка ступеня самоподібності трафіку [2].

Метою даної роботи є програмна реалізація знаходження характеристик якості самоподібного трафіку мережі LTE.

Відомо, що пакетний трафік мережі мобільного зв'язку описується розподілом Вейбула. Використовуємо розподіл Вейбула, який заданий диференціальною функцією розподілу:

$$f(x) = \begin{cases} \alpha\beta x^{\alpha-1} e^{-\beta x^{\alpha}}, & x \ge 0 \\ 0, & x < 0 \end{cases}, \qquad (1)$$

де α– параметр форми кривої розподілу Вейбулу, $0<\alpha<1$, який визначається, згідно [1], виразом вигляду $\alpha = 2 - 2H$, H – параметр Херста, ,

$$0{,}5 \le H \le 1$$

β – параметр розподілу Вейбула вигляду $\beta = \left[\lambda \Gamma\left(1 + \frac{1}{\alpha}\right) \right]^{\alpha}$, β>0, Γ – гамма-функція Ейлера вигляду $\Gamma(k) = \int_0^{+\infty} t^{k-1} e^{-1} dt$, λ– інтенсивність надходження пакетів на обслуговування в систему масового обслуговування.

Щільність ймовірності розподілу тривалості інтервалів надходження заявок в СМО при цьому має вигляд [3]:

$$f(t) = \alpha\beta t^{\alpha-1} e^{-\beta t^{\alpha}} , \; t \geq 0 , \; 0 < \alpha < 1 \qquad , \tag{2}$$

Необхідно визначити характеристики якості для СМО виду $W_B/M/1/\infty$, де μ – інтенсивність обслуговування заявок в СМО, ρ – коефіцієнт завантаження СМО.Характеристики якості знайдемо наступним чином:

– середній час очікування *W* заявки в СМО за виразом

$$W = \frac{\sigma}{\mu(1-\sigma)}, \tag{3}$$

– середня кількість заявок *Q* у черзі СМО за виразом

$$Q = \frac{\rho\sigma}{\mu(1-\sigma)}, \tag{4}$$

– середня довжина черги заявок *L* виразом

$$L = \frac{\rho\sigma}{1-\sigma} . \tag{5}$$

Вираз (2), згідно [4], запишемо у вигляді трансцендентного рівняння:

$$\sigma = \alpha\beta \int_0^{+\infty} e^{-(\mu-\mu\sigma)t} t^{\alpha-1} e^{-\beta t^{\alpha}} dt . \tag{6}$$

Щоб знайти параметри якості: середній час очікування заявок W в системі, середню кількість заявок Q в черзі та середню довжину L черги заявок, необхідно розв'язати інтегральне рівняння (6) відносно невідомої *σ*.

Для цього складемо блок-схему (рисунок 1) знаходження рішення інтегрального рівняння (6).

Згідно блок-схеми (рисунок 1), складемо програму у програмному середовищі MATLAB [5], за допомогою якої знайдемо *σ*, та підставляючи *σ* у вирази (3), (4), (5), знаходимо параметри якості.

ВИСНОВКИ

1. Розглянуто систему масового обслуговування виду $W_B/M/1/\infty$, яка моделює обслуговування самоподібного трафіка в мережі 4G / LTE на базі розподілу Вейбула.
2. Оскільки не завжди можливо отримати точне аналітичне рішення для визначення характеристик якості системи масового обслуговування вигляду $W_B/M/1/\infty$ з використанням інтегральних рівнянь, для вирішення цього рівняння запропоновано впровадження програмного рішення в середовищі MATLAB.
3. Складено програму, за допомогою якої може бути отримано графічне рішення інтегрального трансцендентного рівняння. Це дозволило визначити характеристики якості обслуговування самоподібного трафіку для СМО виду $W_B/M/1/\infty$, такі як середній час очікування заявки в СМО, середня кількість заявок в СМО і середня довжина черги заявок.

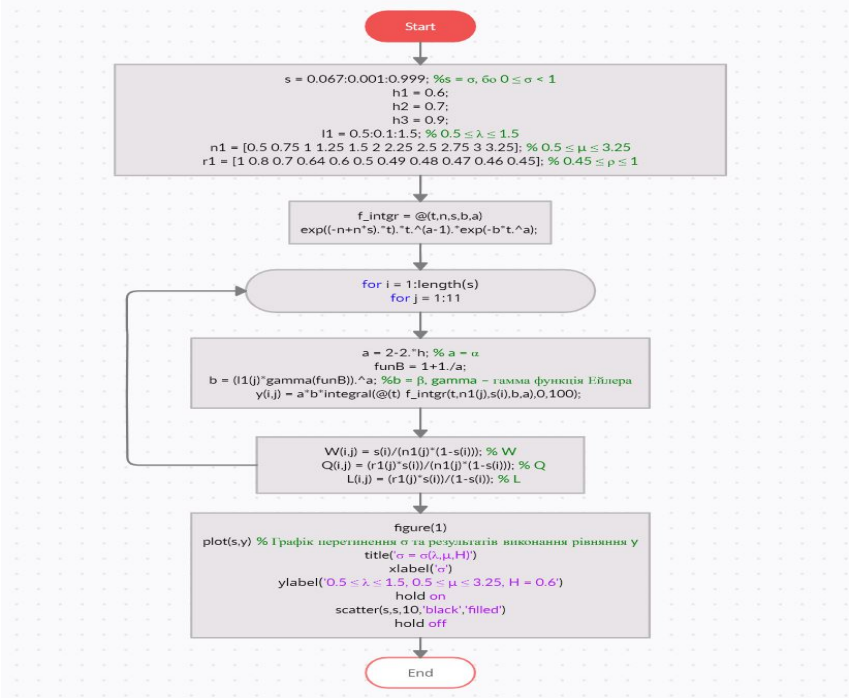


Рисунок 1. Блок-схема програми для знаходження характеристик самоподібного трафіку мережі LTE

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Strelkovskaya I.V. Self-similar traffic in G/M/1 queue defined by the Weibull distribution/ I.V. Strelkovskaya, T.I. Grygoryeva, I.N. Solovskaya // Radioelectronics and Communications Systems. – 2018. – V. 61, № 3 (2018). – P. 173-180. https://doi.org/10.20535/S0021347018030056, Online ISSN 2307-6011

2. Lozhkovskyi A.G. Dependence approximation of the Hurst coefficient on the traffic distribution parameter / A.G. Lozhkovskyi, Ye.V. Levenberg // Information & Telecommunication Sciences. - 2017. - № 2. - P.18-22.

3. Strelkovskaya I.V. Forecasting 5G network multimedia traffic characteristics / I.V. Strelkovskaya, I.N. Solovskaya, A.O. Makoganiuk // Modern Problems of Radio Engineering, Telecommunications and Computer Science: proceedings of the 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Slavske, Ukraine, February 25 – 29, 2020. – Lviv: Lviv Polytechnic National University. – P. 982 - 987. https://doi.org/10.1109/TCSET49122.2020.235585 (Scopus)

4. Strelkovskaya I.V. Research of the quality characteristics of self-similar traffic of a mobile communication network on the basis of software release, Irina V. Strelkovskaya, Irina N. Solovskaya, Anastasiya O. Makoganiuk, Andrii D. Balyk, p.p.51-57. // Information and telecommunication sciences, Volume 11 Number, 2(21) July-December 2020 International Research Journal Registration Certificate KB No 15064-3636P.https://doi.org/10.20535/2411-2976.22020.51-57

5. SIMULINK. User's Guide. Natick: The MathWorks, Inc., 1990. https://uk.mathworks.com/help/index.html
6. Стрелковська І.В. Прогнозування характеристик самоподібного трафіку за допомогою сплайн-екстраполяції / І.В. Стрелковська, І.М. Соловська, Макоганюк А.О., Северин М.В. // Вісник університету «Україна». – 2019. – № 1 (22). – С. 87-94.
7. Strelkovskaya I.V. Different extrapolation methods in Problems of Forecasting / I. Strelkovskaya, I. Solovskaya, A. Makoganiuk // In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. https://doi.org/10.1007/978-3-030-58359-0_12 (Scopus)

УДК 621.391

Розенвассер Д.М., к.т.н.
Шмалько Д.В.
Міжнародний гуманітарний університет
denysrozenvasser@gmail.com

АНАЛІЗ РОЗВИТКУ МЕРЕЖІ СУПУТНИКІВ STARLINK

Анотація. *У роботі проаналізовано останні специфікації та публікації щодо розвитку мережі супутників системи Starlink. Приведено дані щодо кількості супутників на орбіті, пропускної здатності, затримки та вказано перспективи розвитку на найближчий час.*

Starlink - це проект компанії SpaceX, що має на меті забезпечити глобальне високошвидкісне інтернет-покриття за допомогою великої кількості супутників на низькій орбіті Землі. Проект розпочався у 2015 році з метою подолання цифрового розриву між розвиненими та віддаленими регіонами світу, де доступ до інтернету є обмеженим або взагалі відсутній.

Це важливий крок у розвитку супутникового зв'язку та доступу до інтернету для всього світу.

Починаючи з 2019 року, SpaceX регулярно здійснює запуски супутників Starlink, з використанням ракети-носія Falcon 9. Кожен запуск виводить на орбіту від 60 до 120 супутників. Станом на початок 2024 року, на орбіті перебуває понад 4000 супутників Starlink, а на червень 2024 року – вже більше 5000 супутників (рис. 1).

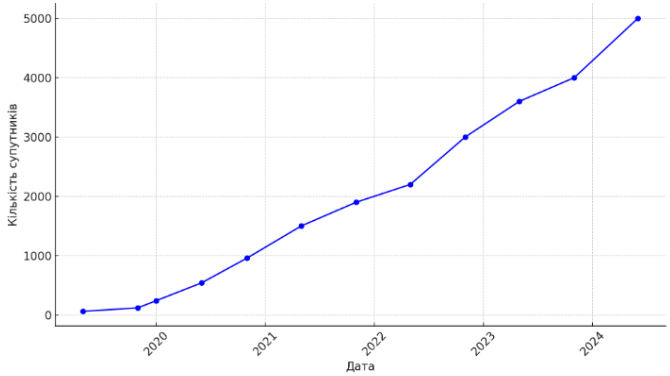


Рисунок 1 – Розвиток мережі супутників Starlink на орбіті.

Графік демонструє подальше стрімке зростання кількості супутників, підкреслюючи інтенсивність запусків SpaceX.

У лютому 2024 року SpaceX розпочала тестування прямого підключення Starlink до смартфонів. Компанія розширює послуги D2D (Device-to-Device), плануючи додати голосовий зв'язок, передачу даних та інтернет речей у 2025 році.

На сьогодні Starlink доступний вже в 100 країнах (рис. 2), до мережі підключено близько 3 млн абонентів (рис. 3).

За останній рік у США медіанна затримка знизилась з 48.5мс до 33мс, найгірша затримка знизилась з понад 150мс до менше ніж 65мс. В інших країнах в середньому медіанна затримка знизилась на 25%, а найгірша затримка знизилась на 35%. Як мета на 2024 рік заявлено досягнення затримки 20 мс.

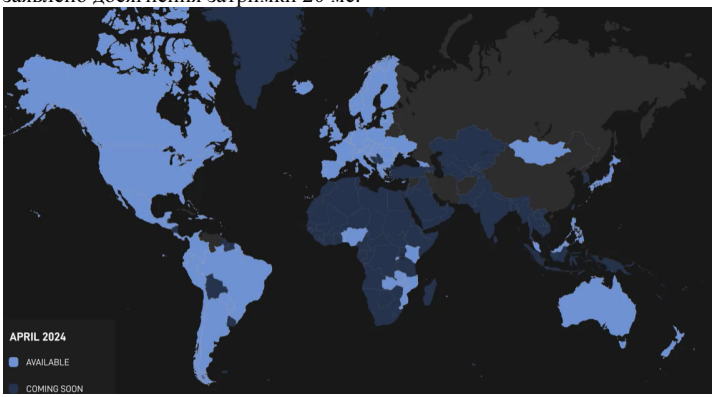


Рисунок 2 – Покриття Starlink станом на квітень 2024 року.

Супутники Starlink оснащені передовими технологіями, такими як:

– лазерні міжсупутникові зв'язки, що дозволяють передавати дані між супутниками без необхідності спуску сигналу на Землю;

– інноваційні антени з фазованими ґратками для забезпечення стабільного і високошвидкісного зв'язку з користувачами;

– автоматичне ухилення від зіткнень, що забезпечує безпечне функціонування мережі в умовах підвищеної кількості об'єктів на орбіті.

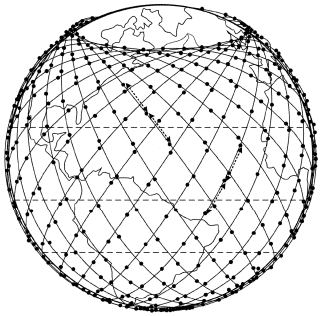


Рисунок 3 – Схема розміщення супутників Starlink на орбіті.

Starlink може забезпечувати резервне інтернет-з'єднання в умовах надзвичайних ситуацій, таких як природні катастрофи або військові конфлікти, коли традиційні інфраструктури можуть бути пошкоджені або зруйновані.

Starlink став життєво важливим джерелом зв'язку в Україні під час російського вторгнення.

Очікується, що Starlink продовжуватиме відігравати важливу роль в Україні протягом багатьох років.

Мережа може бути використана для:

- координації військових дій;
- розвитку цифрової економіки;
- підтримки доступу до освіти та інформації;
- забезпечення доступу до охорони здоров'я;
- надання гуманітарної допомоги;
- підтримки роботи органів влади;
- підтримки досліджень та інновацій.

Література

1. World's most advanced broadband satellite internet. URL: https://www.starlink.com/technology.
2. Cakaj S., The Parameters Comparison of the “Starlink” LEO Satellites Constellation for Different Orbital Shells. Frontiers in Communications and Networks, 2021. 2(7).
3. Dr. S.Pekhterev “The bandwidth of the StarLink constellation and the assessment of its potential subscriber base in USA”, SatMagazine, November 2021, pp. 54-57.
4. Humphreys, Todd E., et al. Signal structure of the Starlink Ku-band downlink. https://doi.org/10.48550/arxiv.2210.11578, 2022.
5. Kim M.G., Jo H.S. Performance analysis of NB-IOT uplink in low earth orbit non-terrestrial networks. Sensors (Basel). 2022 sep 19;22(18):7097. DOI: 10.3390/s22187097
6. Noah Clarke. Starlink Internet Speeds – Updated For 2023. URL: https://www.starlinkhardware.com/starlink-internet-speeds/.
7. Catherine McNally. SpaceX Starlink Satellite Internet Review 2023. URL: https://www.reviews.org/internet-service/spacex-starlink-satellite-internet-review/.
8. Mike Dano. Starlink's network faces significant limitations, analysts find. URL: https://www.lightreading.com/4g3gwifi/starlinks-network-faces-significant-limitations-analysts-find/d/d-id/764159.
9. Anthony Spadafora. Starlink internet coverage, cost, speeds and the latest news — what you need to know. URL: https://www.tomsguide.com/news/starlink-internet-coverage-speed-cost-satellites-ipo-and-latest-news.
10. Tyler Cooper. Starlink Internet Speeds. URL: https://broadbandnow.com/starlink.
11. Michael Kan. SpaceX's Starlink Raises Download Speed Goal From 1Gbps to 10Gbps. URL: https://www.pcmag.com/news/spacexs-starlink-raises-download-speed-goal-from-1gbps-to-10gbps.
12. Denys Rozenvasser and Kateryna Shulakova. Estimation of the Starlink Global Satellite System Capacity // Proceedings of International Conference on Applied Innovation in IT. Volume 11, Issue 1, pp. 55-59. – 2023 (DOI:10.25673/101912).
13. 2024 Starlink Tests: SpaceX's Satellite Internet Keeps Getting Better. URL:https://www.pcmag.com/articles/2024-starlink-speed-tests-spacex-satellite-internet.
14. SpaceX launches 1,000th Starlink satellite of 2024. URL:https://www.aa.com.tr/en/science-technology/spacex-launches-1-000th-starlink-satellite-of-2024/3257077

15. Improving Starlink's latency. URL: https://api.starlink.com/public-files/StarlinkLatency.pdf

УДК 621.391

Стрелковська І.В., д.т.н., професор,
декан факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний гуманітарний університет, Одеса, Україна
i.strelkovskaya@mgu.edu.ua
Золотухін Р.В., начальник департаменту програмування
ТОВ «Телекарт-Прилад», Одеса, Україна
zolotukhinrv@gmail.com

МОДЕЛЬ ОБСЛУГОВУВАННЯ НИЗЬКОШВИДКІСНОЇ РАДІОМЕРЕЖІ ЗВ'ЯЗКУ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

Анотація. *В роботі проводиться аналіз узагальненої моделі показників якості обслуговування радіомереж зв'язку автоматизованих систем управління, побудованих на базі ультракороткохвильових радіостанцій. Імітаційне моделювання дозволяє вирішити проблему вибору необхідних технічних характеристик телекомунікаційного обладнання для забезпечення доступності сервісів ще на етапі проектування. Для проведення імітаційного моделювання в роботі пропонується модель обслуговування радіомережі та визначаються середні показники полоси пропускання, джитеру, втрат в каналі, час відповіді на повідомлення та закони розподілу інтервалів між вимогами на обслуговування, середній розмір пакету даних та необхідна полоса пропускання для різних типів трафіку в автоматизованій системі управління, побудованій на базі низькошвидкісної радіомережі.*

Автоматизовані системи управління (АСУ) набули широкого використання у сучасному світі [1, 3, 5]. АСУ, зазвичай, працюють на базі гетерогенних мереж зв'язку з великою пропускною здатністю, що дозволяє підключати майже необмежену кількість користувачів [3]. АСУ державного рівня низової ланки управління з активним переміщенням користувачів створюються та працюють на основі низькошвидкісних каналів зв'язку з використанням ультракороткохвильових (УКХ) радіостанцій [1]. Такі мережі зв'язку характеризуються низькою пропускною здатністю, великими затримками передачі даних та джитером [3], тому на практиці використовують фільтрацію трафіку, обмежують кількість користувачів та сервісів для роботи АСУ в низькошвидкісних радіомережах зв'язку. Основними типами трафіку в АСУ на базі УКХ радіомереж зв'язку є розмовний трафік, передача файлів, відеотрансляція та трафік спеціалізованого програмного забезпечення АСУ [1-4]. Кожен з цих типів трафіку має свої закони розподілу інтервалів між заявками на обслуговування, різні розміри пакетів даних та тривалості обслуговування, що ускладнює математичні розрахунки щодо визначення навантаження на мережу зв'язку АСУ. Саме тому, для визначення можливого завантаження пропускної спроможності та ймовірності обслуговування мережі зв'язку АСУ доцільно використовувати імітаційне моделювання.

Імітаційне моделювання передбачає використання моделі обслуговування досліджуваної системи зв'язку, але на сьогоднішній день не визначено моделі обслуговування УКХ радіомережі АСУ державного рівня низової ланки управління з активним переміщенням користувачів [1, 5]. Метою роботи є аналіз структури мережі АСУ та її показників якості обслуговування, визначення типів та характеристик трафіку, визначення моделі обслуговування УКХ радіомережі АСУ.

Узагальнену структуру мережі зв'язку АСУ низової ланки управління, побудованої на базі УКХ радіостанції, можна представити у вигляді, показаному на рис.1 [5]. Узагальнену модель її показників ймовірності обслуговування показано на рис.2 [5]. Структуру мережі представлено у вигляді трьох рівнів: доступу, взаємодії та керування. На узагальненій моделі показників функціонування показано наступні позначення (рис. 2):

- $p_{РД}$ – ймовірність обслуговування мережі зв'язку рівня доступу;
- $p_{РВ}$ – ймовірність обслуговування мережі зв'язку рівня взаємодії;
- $p_{КР}$ – ймовірність обслуговування мережі зв'язку керівного рівня.

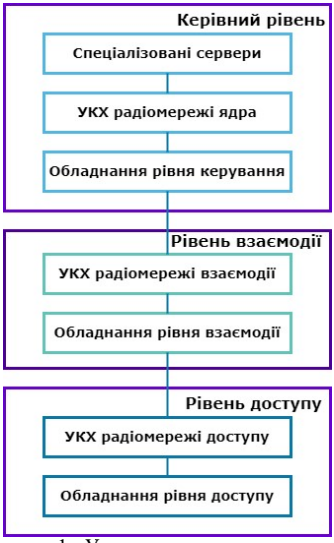


Рисунок 1 - Узагальнена структура мережі зв'язку АСУ низової ланки управління

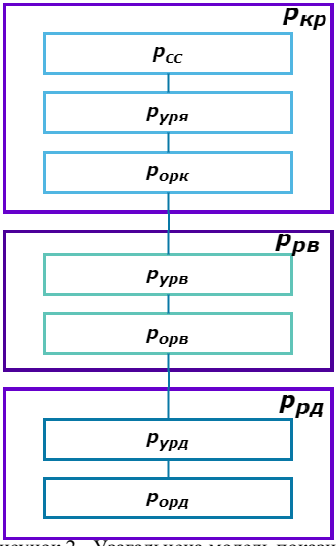


Рисунок 2 - Узагальнена модель показників функціонування мережі зв'язку АСУ

На кожному рівні узагальненої архітектури АСУ використовується різні типи мережевого обладнання, а радіомережі використовуються для різної кількості користувачів та сервісів. Відмова одного з елементів кожного рівня призведе до відмови в обслуговуванні усього рівня. На узагальненій моделі (рис. 2) показано ймовірнісні показники функціонування мережі зв'язку АСУ:

$p_{ОРД}$ – ймовірність обслуговування «обладнанням рівня доступу»;

$p_{УРД}$ – ймовірність обслуговування «УКХ радіомережі доступу»;

$p_{ОРВ}$ – ймовірність обслуговування «обладнанням рівня взаємодії»;

$p_{УРВ}$ – ймовірність обслуговування «УКХ радіомережі взаємодії»;

$p_{ОРК}$ – ймовірність обслуговування «обладнанням рівня керування»;

$p_{УРЯ}$ – ймовірність обслуговування «УКХ радіомережі ядра»;

$p_{СС}$ – ймовірність обслуговування «спеціалізованими серверами».

Кожен рівень моделі має різні показники функціонування. Рівень доступу складається з двох послідовно включених елементів: обладнання рівня доступу та УКХ радіомережі доступу. Тоді ймовірність обслуговування на рівні доступу відповідно буде [5]:

$$p_{РД} = p_{ОРД} \cdot p_{УРД}.$$

Аналогічно можна визначити ймовірність обслуговування на рівнях керування та взаємодії відповідно [5]:

$$p_{РВ} = p_{ОРВ} \cdot p_{УРВ},$$
$$p_{КР} = p_{ОРК} \cdot p_{УРЯ} \cdot p_{СС}.$$

Ймовірність обслуговування користувача рівня доступу спеціалізованими серверами $p_{ОРД-СС}$ визначається:

$$p_{ОРД-СС} = p_{РД} \cdot p_{РВ} \cdot p_{КР}.$$

Для розрахунку ймовірності обслуговування АСУ необхідно визначити ймовірності обслуговування кожного елемента кожного рівня. Ймовірності обслуговування обладнання рівня доступу, взаємодії, керівного рівня та спеціалізованих серверів можливо розрахувати на основі характеристик обладнання, часу його роботи тощо. Для розрахунку ймовірностей обслуговування радіомереж необхідно проводити імітаційне моделювання, так як ймовірність обслуговування залежить від втрат в радіоканалі та використання пропускної здатності радіообладнання. Відповідно до проведених вимірювань в роботах [1-4], середні показники полоси пропускання, джитеру, втрат в каналі на час відповіді на Internet Control Message Protocol (ICMP) повідомлення в УКХ радіомережах показано у табл.1.

Таблиця 1 – Середні показники якості обслуговування УКХ радіомереж АСУ

Режим роботи	Фіксована частота	Псевдовипадкове перелаштування робочої частоти	Широкосмуговий режим
Полоса пропускання	100 кбіт/с	15,8 кбіт/с	350 кбіт/с
Джитер	120 мс	1000 мс	46 мс
Втрати в каналі	2 %	2 %	2 %
Час відповіді на ICMP повідомлення	1200 мс	2000 мс	320 мс

Втрати в радіоканалі в середньому має показник в 2%, що зменшує ймовірність обслуговування, але окрім цього можна побачити, що максимальна полоса пропускання значно обмежена в порівнянні з сучасними технологіями організації зв'язку. Відповідно до робіт [1-4] можна визначити, що основними типами трафіку для АСУ, побудованих на базі низькошвидкісних радіомереж зв'язку, є розмовний трафік, передача файлів, відеотрансляція та трафік спеціалізованого програмного забезпечення (СПЗ) АСУ. Кожен тип трафіку має свій закон розподілу інтервалів між заявками на обслуговування та різні розміри пакетів даних. У табл. 2 показано закони розподілу інтервалів між заявками на обслуговування, середній розмір пакету даних та середню полосу пропускання трафіку УКХ радіомереж АСУ на одного користувача або сервісу відповідно до [1-4].

Таблиця 2 – Середні характеристики трафіку УКХ радіомереж АСУ

Тип трафіку	Закон розподілу інтервалів між заявками на обслуговування	Середній розмір пакету даних	Полоса пропускання
Розмовний	Експоненціальний	-	2,4 кбіт/с
Відеотрансляції	Розподіл Парето	1350 байт	102 кбіт/с
Передача файлів	Логонормальний закон	1400 байт	45 кбіт/с
Трафік СПЗ АСУ	Розподіл Вейбула	1108 байт	1,4 кбіт/с

Розмовний трафік передається за допомогою симплексного зв'язку та лише один користувач може передавати голосове повідомлення. Іншому користувачу потрібно дочекатися закінчення передачі, щоб передати своє голосове повідомлення. Окрім цього, деякі радіостанції можуть підтримувати аудіокодеки з різним бітрейтом (MELP 2400, 1200, 800 тощо).

Відеотрансляції можуть передаватися лише у широкосмуговому режимі роботи радіостанції. При передачі відео у режимах фіксованої частоти або ППРЧ трафік від відео передачі заповнить повністю полосу пропускання, що знизить ймовірність обслуговування інших типів трафіку до 0%. Окрім того, в залежності від роздільної здатності зображення, FPS та відеокодеку полоса пропускання може змінюватись від декількох кілобіт на секунду до мегабіт на секунду [4].

Трафік передачі файлів залежить від типу використовуваного протоколу (FTP, TFTP) та часу відповіді на ICMP повідомлення. Протоколи передачі даних завжди очікують підтвердження про прийом пакетів даних, тому зміна режиму роботи радіомережі призводить на змінення затримки передачі даних, інтенсивності передачі пакетів даних і використовуваної полоси пропускання.

Полоса пропускання для передачі трафіку СПЗ АСУ залежить лише від кількості користувачів, адже СПЗ використовує спеціалізовані протоколи для передачі повідомлень, зображень та інших даних.

На основі узагальненої моделі показників функціонування та типу трафіку, що циркулює в УКХ радіомережі, можна запропонувати модель обслуговування УКХ радіомережі АСУ, як показано на рис. 3.

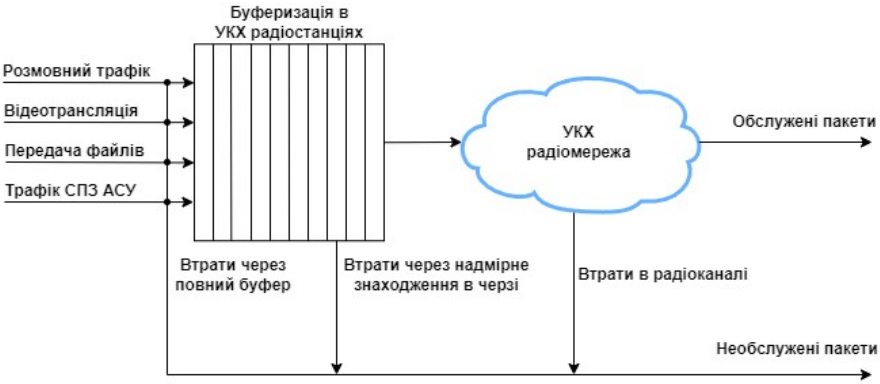


Рисунок 3 – Модель обслуговування УКХ радіомережі АСУ

В залежності від кількості користувачів формується інтенсивність вимог на обслуговування, пакети даних поступають до буферу радіостанції (черги), звідки пакети відправляються в радіомережу. Усі передані через УКХ радіомережу дані представляють собою обслужені пакети, але частина даних втрачається через втрати в радіоканалі, переповнення буферу радіостанції через зайнятість радіомережі та надмірне знаходження даних в черзі. Втрачені пакети представляють собою необслужені пакети. Таким чином, при проведенні моделювання можна розрахувати ймовірність обслуговування радіомережі як відношення числа обслужених пакетів до загальної кількості пакетів, що поступило на обслуговування:

$$p_{\text{РМ}} = \frac{N_s}{N_s + N_e},$$

де $p_{\text{РМ}}$ – ймовірність обслуговування радіомережі,
N_s – кількість обслужених пакетів,
N_e – кількість необслужених пакетів.

Висновки

1. Проведено аналіз узагальненої моделі показників функціонування АСУ, побудованої на базі УКХ радіомереж зв'язку. Визначено, що для розрахунку ймовірності обслуговування радіомережі необхідно проводити імітаційне моделювання.

2. Визначено середні показники полоси пропускання, джитеру, втрат в каналі на час відповіді на ICMP повідомлення УКХ радіомереж. Встановлено, що основними типами трафіку АСУ, побудованих на базі УКХ радіостанцій є розмовний трафік, відеотрансляції, передача файлів, трафік СПЗ АСУ та показано середній розмір їх пакетів даних та необхідну полосу пропускання на одного користувача.

3. Запропоновано модель обслуговування УКХ радіомережі АСУ державного рівня низової ланки управління з активним переміщенням користувачів та визначено формулу ймовірності обслуговування цієї радіомережі.

4. На основі запропонованої моделі обслуговування УКХ радіомережі та отриманих показників обслуговування трафіку можливо розробити програмне забезпечення імітаційного моделювання мереж зв'язку АСУ державного рівня низової ланки управління з активним переміщенням користувачів.

Література

1. Strelkovskaya I.V. Modeling of telecommunication components of automated control systems in low-bandwidth radio networks / I.V. Strelkovskaya, R.V. Zolotukhin, A.O. Makoganiuk // In: P. Vorobiyenko, M. Ilchenko, I. Strelkovska. Current Trends in Communication and Information Technologies. Lecture Notes in Networks and Systems, 2021,. Springer, Cham, DOI: https://doi.org/10.1007/978-3-030-76343-5_9, P 150-170.

2. Strelkovskaya I. Comparative analysis of file transfer protocols in low-bandwidth radionetworks / I. Strelkovskaya, R. Zolotukhin, J. Strelkovska // Proceedings of the 9rd International Conference on Applied Innovations in IT (ICAIIT-2021), Vol. 9, Is. 1, Koethen, Germany, March, 16, 2017. - Anhalt University of Applied Sciences. – P. 27-32.

3. Strelkovskaya I., Zolotukhin R., "Research of low-bandwidth radionetworks QoS parameters" in Information and Telecommunication Sciences, International Research Journal, Volume 11, Number 1(20), January-June 2020, DOI: https://doi.org/10.20535/2411-2976.12020.77-81.6.

4. Strelkovskaya I., Zolotukhin R., Pascalenko V., «Research of audio and video traffic the characteristics in low-bandwidth radio communication networks», Вимірювальна та обчислювальна техніка в технологічних проецас, вип. 4, с. 183–190, Лис 2023, DOI: https://doi.org/10.31891/2219-9365-2023-76-26.

5. Стрелковська, І., Золотухін, Р., Григор'єва, Т. Узагальнена модель оцінки показників функціонування низькошвидкісних мереж зв`язку автоматизованих систем управління. Інфокомунікаційні та комп'ютерні технології, 1(03), с. 153-168, 2022. DOI: https://doi.org/10.36994/2788-5518-2022-01-03-09.

Петков Євген Ігорович.
Магістр, спеціальність 172,
yepetkov@gmail.com
Науковий керівник,
Йона Лариса Григорівна, к.т.н., доцент
Міжнародний гуманітарний університет
yonalarisa66@gmail.com

АНАЛІЗ ПОТОЧНОГО СТАНУ І ПЕРСПЕКТИВ РОЗВИТКУ ГЛОБАЛЬНОЇ МЕРЕЖІ ІНТЕРНЕТ

Анотація. *Дослідження включає аналіз поточного стану мережі Інтернет, зокрема Протоколу граничного шлюзу BGP(Border Gateway Protocol). Проаналізовано два історичних недоліки в архітектурі мережі Інтернет з адресацією IPv4.*

Еволюція регіональних локальних мереж дослідницьких установ (таких як ARPANET зразка 60-70х років) до глобальної мережі Інтернет відбулась дуже швидко, просто миттєво в історичних масштабах. Перші стандарти і документи із серії пронумерованих інформаційних документів Інтернету (Request for Comments, RFC), зокрема фундаментальні протоколи мережі Інтернет, як наприклад, протокол динамічної маршрутизації BGP (Border Gateway Protocol) або технологія DNS (Domain Name System) прийняті у 80-90х роках, сформували ту архітектуру і особливості Всесвітньої мережі, яка використовується дотепер. Впродовж свого існування та розвитку мережа Інтернет, виходячи із своєї архітектури побудови, має як переваги так і недоліки.

До переваг мережі Інтернет можна віднести її дійсно глобальне значення і незалежність від відстані в можливостях встановлення взаємодій типу «peer-to-peer» або «client-server». За виключенням деяких країн з «особливим політичним режимом» та обмеженим доступом до ресурсів Інтернет чи доступом до дозволених ресурсів, більша частина людства має можливість одержувати доступ до будь-яких ресурсів чи користувачів, що мають підключення до мережі Інтернет. Саме ця глобальність і рівнозначність всіх публічних IP-адрес є основною перевагою мережі Інтернет. Приміром, в порівнянні з телефонною мережею загального користування (ТМЗК), складно сьогодні знайти користувача який би дзвонив в інше місто, країну, або континент, оплачуючі дороговартісні тарифи операторів ТМЗК, замість використання великого різноманіття додатків передачі голоса/відео через IP, меседжерів, соціальних мереж або електронної пошти. Також користувач сервісів Інтернету не замислюється над питанням де фізично розташований сервер чи датацентр для хостингу додатка, вебресурса чи соціальної мережі, які він використовує. Для користувача це не має жодного значення з точки зору вартості. Вартість для користувача обумовлює тільки: відстань до найближчого провайдера підключенння до мережі Інтернет (ISP – Internet Service Provider), запропонована «остання миля» - технологія підключення (кабельна електрична, кабельна оптоволоконна, мобільна, супутникова, тощо), та умови конкуренції та кількості ISP провайдерів в місці підключення користувача.

Для сервісів мережі Інтернет питання розташування фізичного або віртуального серверу, сервісу або мікросервісу, підключеного до Всесвітньої мережі не мають великого значення.

Більше уваги приділяється умовам розгортання в тому чи іншому місці, а саме має значення:

- вартість хостингу фізичних серверів в датацентрі;
- вартість надання віртуальних серверів;
- вартість сервісів, мікросервісів в будь-якому типі датацентра (On-premise, Cloud);
- надійність датацентра;
- вартість «останньої милі» підключення до мережі Інтернет;
- кількість та якість каналів підключення запропонованих ISP провайдерів;
- тощо.

До переваг Інтернету можна додати можливості використання в якості транспорта через публічну IP-мережу приватних VPN користувачів або бізнесу, що вартує значно

нижче ніж замовляти у телекоммунікаційних операторів виділені приватні лінії чи канали зв'язку.

Також слід відзначити можливості, які надає використання мережі Інтернет для дистанційного навчання чи віддаленої роботи. Все більше перспектив отримання освіти здобувачем, незалежно від відстані і різниці в часі із закладом освіти. Так само, як організація географічно розподілених команд та підрозділів на територіях різних країн й частин світу, з використанням сучасних технологій в теперішній час не є проблемою для великих компаній або корпорацій.

Крім переваг, мережа Інтернет має свої недоліки.

Так, недоліки архітектури мережі Інтернет можна знайти в:

– самому протолі динамічної маршрутизації BGP [1], як зв'язуючого між Автономними Системами (AS), на яких побудована мережа Internet;

– історичному процесі розподілення адресного простору IPv4 та номерів Автономних Систем (ASN) організацією IANA, яка делегує цій функціонал на Регіональні Інтернет Реєстри (RIR), а саме: AFRINIC (Африканський Регіон), APNIC (Азія/Тихоокеанський Регіон), ARIN (Північна Америка), LACNIC (Латинська Америка), RIPE NCC (Європа, Близький Схід, та Центральна Азія) [4].

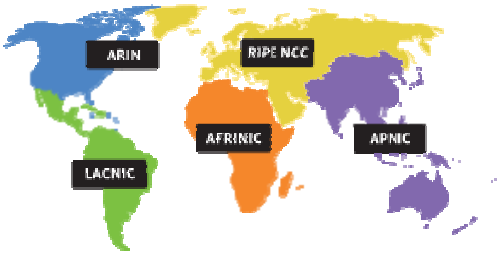


Рисунок 1 – Регіональні Інтернет Реєстри.

Однією з основних вразливостей протоколу BGP в Інтернеті є можливість здійснення атаки, відомої як «BGP hijacking». У ході такої атаки, зловмисна або помилкова Автономна Система (AS) заявляє BGP-провайдеру про IP-мережу, яка фактично належить іншій AS. Це призводить до того, що трафік, який повинен йти до легітимного власника мережі (жертви), перенаправляється до зловмисника, який використовує вразливість для власних цілей.

Відомим прикладом цієї атаки є інцидент "YouTube Hijacking" [5]. Він стався, коли оператор Pakistan Telecom (AS17557), намагаючись заблокувати доступ до YouTube в Пакистані, випадково анонсував IP-префікс цього сервісу своєму провайдеру, а отже, й глобальному Інтернету. Це призвело до того, що трафік користувачів YouTube був тимчасово перенаправлений на некоректну AS оператора Pakistan Telecom, викликавши помилкову маршрутизацію IP-пакетів.

Основна проблема протоколу BGP полягає в тому, що він не містить вбудованих засобів захисту, покладаючись натомість на довіру між операторами мережі. Це означає, що оператори повинні самостійно забезпечувати безпеку своїх систем і уникати передачі невірної інформації. Однак, помилки все одно можуть траплятися, і виникають ризики зловмисного втручання в таблиці маршрутизації, які використовує BGP.

Щоб протистояти вразливості BGP, необхідно вжити таких заходів:

— насамперед, усі інтернет-провайдери повинні ретельно налаштовувати фільтрацію як вхідних, так і вихідних IP-префіксів на своїх з'єднаннях з іншими провайдерами та ця фільтрація повинна базуватися на даних з відповідних реєстрів RIR;

— по-друге, використовувати доступну систему сертифікації ресурсів RPKI, яка застосовує криптографічні підписи Route Origin Authorization (ROA) для підтвердження та перевірки права конкретної Автономної Системи на володіння певними IP-ресурсами.

Інтернет-провайдери можуть використовувати ROA для перевірки права авторизованої Автономної Системи на анонс певного IP-префікса. Однак, хоча значна кількість провайдерів підтримують механізм RPKI, на жаль, це ще не є загальноприйнятою практикою. Тому верифікація за допомогою RPKI поки що не забезпечує стовідсоткову захищеність у всьому глобальному Інтернеті.

Історичний процес виділення IPv4-адрес не був впорядкованим і довгостроково спланованим. Зі зростанням потреби, блоки IP-адрес послідовно видавалися різним регіональним реєстрам, а згодом – кінцевим автономним системам. Сьогодні на одну AS, що має більше одного IP-префікса, можуть припадати IP-мережі з різних класів. Також велика кількість IP-префіксів не агрегується за територіальним принципом (оператор, країна, континент тощо). Кожен маршрутизатор, підключений до Інтернету через BGP і отримуючий повну таблицю маршрутизації IPv4 (Full View), зараз змушений обробляти приблизно 1 мільйон маршрутів (історичне зростання показано на Рис.2) [6]. Це необхідно враховувати при плануванні ресурсів BGP-маршрутизатора, зокрема оперативної пам'яті.

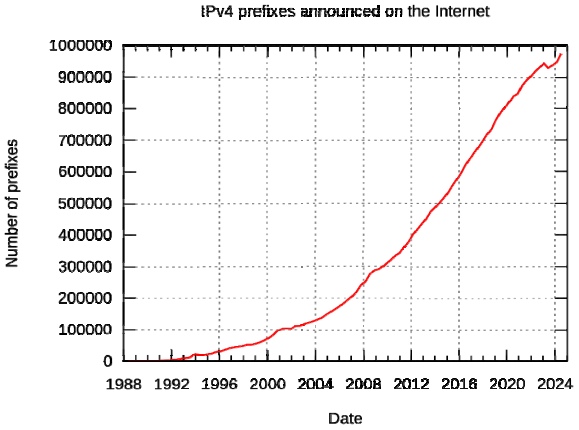


Рисунок 2 – Зростання таблиці BGP в Інтернеті

Таким чином, проаналізовано два історичних недоліки в архітектурі мережі Інтернет з адресацією IPv4. Напрямком подальших досліджень може бути пошук переваг мережі Інтернет з адресацією IPv6 та можливість виправлення в мережі з IPv6 будь-яких недоліків поточної глобальної мережі з IPv4.

Література

1. A Border Gateway Protocol 4 (BGP-4). URL: https://datatracker.ietf.org/doc/html/rfc1654.

2. Multiprotocol Extensions for BGP-4. URL: https://datatracker.ietf.org/doc/html/rfc2283.
3. What is BGP? BGP routing explained. URL: https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-bgp/.
4. Internet Assigned Numbers Authority (IANA). URL: https://www.iana.org/numbers.
5. YouTube Hijacking: A RIPE NCC RIS case study. URL: https://www.ripe.net/publications/news/youtube-hijacking-a-ripe-ncc-ris-case-study/.
6. Wikipedia. Border Gateway Protocol. Routing table growth. URL: https://en.wikipedia.org/wiki/Border_Gateway_Protocol#Routing_table_growth.

Andrii Raichuk, Larysa Globa
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv Ukraine
raaukr@gmail.com, lgloba@its.kpi.ua

ОГЛЯД СЦЕНАРІЇВ ВИКОРИСТАННЯ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ У V2V КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Анотація. *Взаємодія між автомобілями (V2V communication) є однією з ключових технологій майбутнього для безпечного та ефективного дорожнього руху. З розвитком автономних автомобільних систем ця технологія набуває все більшої актуальності, сприяючи підвищенню безпеки дорожнього руху, зменшенню заторів та оптимізації екологічного впливу транспортних засобів. Для пришвидшення інтеграції смарт автомобілів необхідно проводити дослідження ефективності їх комунікаційних протоколів з метою забезпечення надійного зв'язку між транспортними засобами.*

При постійно змінюваній швидкості руху автомобілів до протоколів маршрутизації висуваються високі вимоги щодо стабільності та ефективності передачі інформації. Результати дослідження можуть бути корисними для подальшого розвитку інтелектуальних транспортних систем та оптимізації протоколів комунікації в реальних умовах експлуатації.

Ключові слова: *V2V комунікація, IEEE 802.11p, IEEE 1609.4, інтелектуальні транспортні системи, надійність, зв'язність, динамічний рух.*

Вступ

Розвиток технологій комунікації між транспортними засобами (V2V) є ключовим елементом для підвищення безпеки дорожнього руху, зменшення заторів та покращення ефективності транспортних систем. Протоколи IEEE 802.11p та IEEE 1609.4 розроблені спеціально для підтримки V2V комунікацій, забезпечуючи швидку та надійну передачу даних.

У перспективі інтелектуальні транспортні системи та V2X комунікації матимуть великий вплив на дорожній трафік. Для комунікації автомобілів під час руху використовуються різні технології та протоколи. Це викликано тим, що дані, які передаються, мають різне призначення. Специфікація протоколу IEEE 802.11p підтримує класифікацію якості обслуговування [Quality of Service (QoS)] з використанням розширеного розповсюдженого каналу доступу [Enhanced Distributed Channel Access (EDCA)] [1]. EDCA може класифікувати маяки, засновані на чотирьох категоріях (ACs):фоновий трафік (background traffic BK), важливий трафік (best effort traffic BE), голосовий трафік (voice traffic VO), або відео трафік (video traffic VI).

Під час V2V комунікації використовується інфраструктура бездротових мереж, яка дозволяє транспортним засобам обмінюватися інформацією з метою забезпечення безпеки та комфорту водія.

Основними ключовими елементи цієї інфраструктури є CCH та SCH.

Control Channel (CCH) – це канал керування, який використовується для обміну критично важливою інформацією між транспортними засобами та дорожньою інфраструктурою. Основна мета CCH - передача повідомлень про безпеку та управління, таких як попередження про зіткнення, повідомлення про аварії, стан дорожнього руху та інші критичні сповіщення.

CCH працює на конкретних частотах, визначених стандартами для забезпечення надійної та швидкої передачі даних. Наприклад, у стандарті IEEE 802.11p та архітектурі WAVE (Wireless Access in Vehicular Environments) частота CCH зазвичай працює у діапазоні 5.885-5.895 ГГц. Оскільки інформація, що передається через CCH, є критично важливою для безпеки, цей канал має високий пріоритет у порівнянні з іншими типами даних.

Service Channel (SCH) - це сервісний канал, який використовується для передачі менш критичної, але все ще важливої інформації між транспортними засобами та інфраструктурою. SCH використовується для передачі інформації, що стосується зручності та продуктивності, таких як мультимедійні послуги, оновлення карт, комерційні об'яви, інформація про паркування тощо. SCH використовує інші частоти, відмінні від CCH, для зменшення навантаження на канал керування. У системі WAVE є кілька сервісних каналів, кожен з яких призначений для певних типів даних. Дані, що передаються через SCH, мають нижчий пріоритет у порівнянні з CCH.

У системах V2V комунікації важливо, щоб CCH та SCH ефективно взаємодіяли для забезпечення безпеки та комфорту дорожнього руху. Ця взаємодія досягається за рахунок таймслотів, пріоритезації та координованої передачі даних.

Огляд існуючих рішень

Альтернативні схеми комутації каналів

У дослідженнях [1-4] вважають, що стандартизована схема комутації каналів IEEE 1609.4 викликає проблему втрати пропускної здатності для SCH. Якщо передача пакету має відбутися в кінці інтервалу SCH і розрахунковий час передачі для цього пакету перевищує залишковий час поточного інтервалу, тоді стандарт IEEE 1609.4 рекомендує, щоб вузол, що передає, запобігав надсиланню цього пакета протягом поточного інтервалу, але натомість має надіслати його протягом наступного інтервалу, залишаючи кінець кожного інтервалу синхронізації невикористаним.

Миттєвий доступ та розширений доступ

Дві різні схеми комутації каналів були запропоновані в [2] для мінімізації проблеми втрати пропускної здатності SCH. Ці схеми — миттєвий доступ і розширений доступ, див. рис. 1. Ці схеми покращують продуктивність додатків, які потребують пропускної здатності, у SCH за рахунок CCH.

Коли використовується схема миттєвого доступу, вузлу не потрібно чекати, поки закінчиться інтервал CCH. Він може переключитися на SCH, як тільки CCH завершить свої передачі, і може залишатися там до закінчення інтервалу синхронізації. Схема розширеного доступу дозволяє передачу по SCH без очікування CCH. Це відбувається за рахунок жертви продуктивністю CCH для SCH. Ці схеми не зосереджені на мінімізації впливу перемикання каналів на продуктивність сигналізації IEEE 802.11p (тобто CCH).

Схема фрагментації

Схема фрагментації [4] призначена для зменшення впливу проблеми втрати пропускної здатності на SCH. Це досягається за допомогою фрагментації пакетів, щоб використати залишковий час наприкінці інтервалу SCH. Вихідний пакет, який необхідно передати в кінці службового кадру, фрагментується таким чином, що розрахунковий час передачі одного його фрагмента дорівнює залишковому часу поточного службового кадру. Таким чином у кадрі служби не буде невикористаного часу та пропускної здатності. Таким чином, пом’якшується проблема втрати пропускної здатності за рахунок додаткового заголовка для фрагментованого пакета.

Ця схема працює для великих пакетів (таких як TCP), але є неефективною, якщо застосовувати її до природи обміну повідомленнями маяків, оскільки повідомлення вже відносно малі.

Згідно проаналізованого матеріалу, рекомендується в майбутній роботі зосередитися на розробці схеми, яка могла б мінімізувати вплив перемикання каналів та покращити продуктивність маяків (тобто CCH), навіть якщо це відбуватиметься за рахунок SCH. Також варто розглянути можливість використання багатоканальних радіостанцій. Такий підхід краще відповідатиме вимогам до масштабованості та надійності додатків, спрямованих на підвищення продуктивності та безпеки дорожнього руху, оскільки для цього необхідна хороша кооперативна обізнаність.

Показники продуктивності:

Щоб проаналізувати продуктивність V2V комунікації, можна використовувати кілька показників:

Імовірність отримання: Ця метрика вказує на ймовірність успішного отримання маяка після його передачі. Зі збільшенням кількості вузлів у системі збільшується кількість маяків, що транслюються по каналу CCH за секунду. Це підвищує навантаження на канал і, як наслідок, збільшує ймовірність зіткнення та втрати маяків. Висока ймовірність отримання свідчить про ефективність комунікації в умовах високого навантаження.

$$P_r = \frac{N_r}{N_g}$$

P_r– ймовірність прийому,N_r – загальна кількість отриманих маяків,N_g– загальна кількість згенерованих маяків.

Наскрізна затримка (актуальність): У міру збільшення навантаження на канал затримка конкуренції зростає, що може вплинути на свіжість отримуваної інформації. Для забезпечення своєчасної реакції вузлів важливо, щоб кінцева затримка маяків не була надто високою. Наскрізну затримку обчислюють шляхом додавання мітки часу до маяка, коли він починає боротьбу за доступ до каналу. Вузли використовують однаковий годинник для ідеальної синхронізації, що дозволяє вузлу-одержувачу відняти мітку часу отриманого маяка з часу отримання.

$$D_{avg} = \frac{\sum_{i=1}^{N_r} D_i}{N_r}$$

де D_{avg}– середня наскрізна затримка,D_i– затримка і-го отриманого маяка, N_r– загальна кількість отриманих маяків.

Сценарії моделювання

OMNeT++ [7] і платформа INET підтримують багатоканальні операції за стандартами IEEE 802.11p і IEEE 1609.4. Усі вузли під час моделювання мають знаходитист в межах діапазону один одного, а їх положення не змінюівтись. Це означає, що всі вузли є досяжними та видимими один для одного, і в цій ситуації прихованих терміналів не існує. Вузли рівномірно розподілені на площі, меншій за граничний діапазон досяжності зв'язку, що дозволить спрощено моделювати умови без впливу відносного розташування та відстаней між вузлами.

Таким чином, у експерименті буде ізольовано проблеми MAC шару, щоб дослідити саме дослідження продуктивності маяків на основі різних методів, таких як перемикання каналів, або використання буферизації.

Для дослідження можливе два основні сценарії моделювання для аналізу V2V комунікації. У безперервному сценарії вузол знаходиться 100% часу на CCH для передачі маяків, як визначено в стандарті IEEE 802.11p. У сценарії, де канали чергуються, вузол кожні 50 мс перемикається між CCH і SCH, відповідно до стандарту IEEE 1609.4.

Параметри моделювання

Для проведення симуляцій, пропонуються наступні параметри:

Швидкість генерації маяка вважається 10 повідомлень на секунду, що достатньо для забезпечення спільної обізнаності. Середня частота генерації маяка становить 10 Гц. У безперервному сценарії генерація маяків рівномірно розподілена. У сценарії, де канали чергуються, генерація маяка обмежена періодами ССН. Швидкість передачі даних для всіх вузлів була встановлена 3 Мбіт/с, що є найнижчою швидкістю, визначеною в IEEE 802.11p. Це забезпечує найбільш надійну модуляцію для критичної інформації.

Актуальність отриманого маяка (R) залежить від кількох факторів, наприклад таких як, затримка в черзі(Dq), затримка під час колізій (D_c) та затримка передачі(D_t).

$$R= f(D_q, D_c, D_t)$$

де f– це функція, яка враховує вплив кожної із затримок на загальну актуальність. Якщо розглянути суму всіх трьох затримок як загальну затримку, то формула може мати вигляд:

$$R= D_q + D_c + D_t$$

Альтернативно, якщо кожна затримка має різну вагу в залежності від її впливу на актуальність, можна використовувати зважену суму:

$$R= w_q \cdot Dq + w_c \cdot D_c + w_t \cdot D_t$$

де w_q, w_c та w_t – вагові коефіцієнти, які визначають вплив кожного типу затримки на загальну актуальність отриманого маяка.

У цих експериментах всі згенеровані маяки мають однакову довжину, що робить затримку передачі постійною. Оскільки всі вузли VANET знаходяться відносно близько один до одного, затримка поширення незначна.

Якщо говорити більш детально про OPD та NPD, то механізм буферизації OPD (Oldest Packet Drop) призначений для забезпечення того, щоб найновіші пакети завжди мали шанс бути переданими, видаляючи найстаріші пакети, коли черга заповнена. Це дозволяє зберігати актуальність переданої інформації, але може призводити до втрати старих, можливо, важливих пакетів. Механізм буферизації NPD (Newest Packet Drop) діє протилежним чином до OPD. При заповненій черзі новий пакет відразу видаляється, залишаючи в черзі старі пакети. Це дозволяє зберігати старі пакети.

Висновки

В статті розглянуто сценарії спільного використання протоколів IEEE 802.11p та IEEE 1609.4 для покращкеея ефективність та надійність V2V комунікацій у динамічних умовах дорожнього руху.

Використання різних механізмів буферизації та змінюваних протоколів може значно впливати на продуктивність V2V комунікацій

Безперервний сценарій забезпечує стабільне з'єднання, проте сценарій із перемиканням каналів згідно з протоколом IEEE 1609.4 може виявитися більш надійним у ситуаціях з високою щільністю трафіку

Проведений аналіз літературних джерел дозволяє визначити важливість вибору відповідного протоколу для різних сценаріїв дорожнього руху та може слугувати основою для подальших розробок в області інтелектуальних транспортних систем.

Подальші дослідження можуть бути спрямовані на розробку адаптивних алгоритмів перемикання між протоколами в реальному часі, а також на тестування цих рішень в реальних умовах.

Джерела

[1] Naila Bouchemal, Rola Naja, Samir Tohmé - Traffic Modeling and Performance Evaluation in Vehicle to Infrastructure 802.11p Network

[2] Dynamic Channel Coordination Schemes for IEEE 802.11p/1609 Vehicular Networks: A Survey
[3] Chung-Ming Huang, Chia-Ching Yang, Huai-De Huang - An Effective Channel Utilization Scheme for IEEE 1609.4 Protocol
[4] Claudia Campolo, Antonella Molinaro, Alexey Vinel - Understanding the performance of short-lived control broadcast packets in 802.11p/WAVE Vehicular networks
[5] Lin Zhang, Yu Liu, Zi Wang, Jinjie Guo - Evaluating and improving the performance of IEEE 802.11p/1609.4 networks with single channel devices
[6] Shie-Yuan Wang, Hsi-Lu Chao, Kuang-Che Liu, Ting-Wei He - Evaluating and improving the TCP/UDP performances of IEEE 802.11(p)/1609 networks
[7] OMNeT++ https://omnetpp.org/

УДК 621.391

Педяш В.В., к.т.н., доцент
Юркул М.Ю., студент
Міжнародний Гуманітарний Університет
vpedyash@gmail.com

АНАЛІЗ МЕТОДІВ МОДУЛЯЦІЇ ДЛЯ ВИСОКОШВИДКІСНИХ СИСТЕМ WDM

Анотація. *У роботі розглядаються методи підвищення спектральної ефективності волоконно-оптичних систем передачі з мультиплексуванням по довжині хвилі та канальною швидкістю передавання 400 Гбіт/с. Розглядаються переваги та обмеження використання квадратурної амплітудної модуляції (QAM) високого порядку для підвищення спектральної ефективності. Обговорюються проблеми, пов'язані з чутливістю до шуму, нелінійними ефектами та зменшенням дальності передачі при використанні складних форматів модуляції. Представлено аналіз сучасних рішень для досягнення швидкості 400 Гбіт/с на канал, зокрема, використання суперканалів з двома піднесучими по 200 Гбіт/с PDM-QAM-16.*

Мережеві оператори зв'язку продовжують відчувати зростаючий попит на пропускну здатність в міських, регіональних і магістральних мережах. Річний приріст трафіку наближається до двох разів, що зумовлено збільшенням використання потокового відео, хмарних обчислень, центрів обробки даних, соціальних мереж і мобільного зв'язку. На сьогоднішній день широко використовуються оптичні системи з далеким радіусом дії, які здатні передавати дані зі швидкістю 100 Гбіт/с [1]. Ці системи базуються на модуляції з поляризаційним поділом каналів і квадратурною фазовою модуляцією (PDM-QPSK), що використовує когерентне виявлення і цифрову обробку сигналів (ЦОС). Вони досягають спектральної ефективності на рівні 2 біт/с/Гц, що значно перевершує звичайні оптичні мережі з частотою 50 ГГц. Це збільшило пропускну здатність системи до близько 10 Тбіт/с для передачі в оптичному волокні С-діапазону. Міжнародні організації зі стандартизації IEEE/ITU-T успішно завершили процеси стандартизації клієнтської частини 100GE, транспортного рівня Optical Transport Unit 4 (OTU4) та ключових аспектів його функціонування. Це було зроблено з метою забезпечення наскрізного з'єднання та сумісності мережі.

Наразі проводяться активні наукові дослідження та розробки з метою вдосконалення оптичного транспорту для підтримки зростаючого обсягу трафіку, покращення спектральної ефективності і зниження вартості передачі даних через оптичне волокно зі швидкістю понад 100 Гбіт/с [2]. Тому досягнення швидкості передачі даних до 400 Гбіт/с на один оптичний канал вважається природнім та перспективним кроком, який відображає як еволюцію швидкості передачі даних і транспортних інтерфейсів, так і

складність їх реалізації. Розглядаються різні підходи до масштабування пропускної здатності каналу до 400 Гбіт/с, такі як підвищення швидкості передачі даних, використання високорівневих форматів квадратурної амплітудної модуляції (KAM/QAM) та створення суперканалів з передовими технологіями спектрального формування і мультиплексування [3].

Основною метою цього дослідження є дослідження методів, що спрямовані на підвищення спектральної ефективності оптичних систем передачі інформації за допомогою мультиплексування по довжині хвилі та досягнення канальної швидкості передавання на рівні 400 Гбіт/с.

На відміну від загальноприйнятого рішення для системи 100 Гбіт/с, технологія 400 Гбіт/с перебуває на етапі активного розвитку, в якому розглядаються різні варіанти з урахуванням чутливості приймача до оптичного співвідношення сигнал/шум (OSNR). Оскільки прогрес у сфері ВОСП поступово просувається до швидкості 400 Гбіт/с, важливо, щоб міжнародні організації співпрацювали, як це було зроблено раніше для оптичних інтерфейсів 100 Гбіт/с [4].

Через фізичні обмеження та обмеження мережевих додатків, що враховуються з точки зору досяжності, чотирикратне покращення спектральної ефективності для 400 Гбіт/с порівняно з 100 Гбіт/с PDM-QPSK (2 біт/с/Гц) є недосяжним. Для досягнення значного покращення спектральної ефективності понад 2 біт/с/Гц потрібно використовувати QAM-M (де M - порядок сузір'я). Найквістовська фільтрація (або спектральна обробка), яка реалізована на стороні передавача, також може сприяти покращенню спектральної ефективності. Однак це призводить до скорочення дальності передачі через високі вимоги до *OSNR* для цих сузір'їв QAM, що робить їх більш чутливими до фазового шуму лазера (наприклад, QAM-16 в 4 рази чутливіший, ніж QPSK) і до нелінійних ефектів волокна, таких як нелінійний фазовий шум. Також важливо враховувати, що вищий порядок QAM менше терплячий до каскадних ефектів переконфігурованих оптичних мультиплексорів з введення-виведення (ROADM) і більш чутливий до смугової оптичної фільтрації. Наприклад, QAM-16 менше стійкий до вузькостмугових оптичних фільтрів, ніж QPSK.

Внаслідок цих різних обмежень, виробники обладнання зараз спрямовують свої зусилля на розробку суперканалів, які складаються з двох піднесучих, що передають по 200 Гбіт/с кожен за технологією PDM-QAM-16 у смузі частот 75 ГГц. Це відповідає спектральній ефективності 5,33 біт/с/Гц. Порівняно з використанням технології 100 Гб PDM-QPSK, два канали PDM-QAM-16 по 200 Гбіт/с вимагають на 7 дБ вищого оптичного сигнал-шумового співвідношення *OSNR*, що приблизно в 5 разів зменшує максимальну відстань передачі для цих каналів.

Вище було вказано, що одночасне збільшення спектральної ефективності і максимальної відстані передачі у системах WDM є неможливим завданням. Тому виникає необхідність у пошуку компромісу між порядком модуляції QAM, швидкістю передачі символів і спектральною ефективністю. Однак, символьна швидкість 32 Гбод/с виявляється оптимальним варіантом для збільшення спектральної ефективності без надмірного навантаження на електроніку, таку як цифро-аналоговий перетворювач (ЦАП), аналого-цифровий перетворювач (АЦП), радіочастотні модулятори і ефективність передачі.

Підводячи підсумки, можна стверджувати, що поставлена мета по дослідженню методів підвищення спектральної ефективності оптичних систем передачі інформації за допомогою мультиплексування по довжині хвилі та досягнення канальної швидкості передавання на рівні 400 Гбіт/с досягнута. Кожен з розглянутих варіантів підвищення спектральної ефективності має свої переваги та обмеження, і вибір конкретного рішення залежить від конкретних вимог до системи, включаючи дальність передачі, допустиме зниження якості сигналу та економічні фактори.

Література

1. Педяш В.В. Моделювання каналу оптичної системи передавання ОТН з квадратурною амплітудною модуляцією // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2022. – No 5. – С.61-65.
2. Keang-Po H. Phase-Modulated Optical Communication Systems / Keang-Po H. – Springer, 2005. – 430 p.
3. Seimetz M. High-Order Modulation for Optical Fiber Transmission / Seimetz M. – Berlin: Springer, 2009. – 252 p.
4. Agrawal G.P. Fiber-Optic Communication Systems / Agrawal G.P. – New York: Wiley-Interscience, 2002. – 580 p.

УДК _____

Стрелковська І.В., д.т.н., професор
Міжнародний гуманітарний університет, Одеса, Україна
i.strelkovskaya@mgu.edu.ua
Бабенцов І.О., магістр з інформаційних мереж зв'язку
ПрАТ Київстар, Одеса, Україна
illyababentsov@gmail.com

ДОСЛІДЖЕННЯ МОДЕЛЕЙ РОБОТИ МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ ПІД ЧАС ВІДСУТНОСТІ СТАБІЛЬНОГО ЕЛЕКТРОЖИВЛЕННЯ

Анотація. *Якість роботи мережі мобільного зв'язку залежить від стабільного електроживлення. Під час останніх 2 років мережі українських фіксованих та мобільних операторів стикнулися з проблемою відключення електроживлення, що впливає на якість сервісів, покриття мережі та дотримання граничних (нормованих) рівнів показників якості телекомунікаційних послуг встановлені НКЕК (національна комісія електронних комунікацій). Під час блек-аутів мережа оператора працює в обмеженому режимі та підтримується завдяки додатковим засобам електроживлення - генератори, акумуляторні батареї (АКБ) тощо, які мають різні параметри, характеристики та нерівномірно постачають електроживлення на всіх рівнях мережі. В рамках підвищення доступності мережі розглянуті декілька моделей роботи системи мобільних операторів. Створений перелік пріоритетних критеріїв для побудови ефективної моделі з використанням штучного інтелекту (ШІ), який підвищує рівень доступності мережі на 2-3%, збільшує середню швидкість передачі даних до 5-6% та зберігає покриття на середнього рівні під час непрогнозованих відключень електроживлення.*

Вступ

Мобільна мережа верхньорівнево складається з декількох основних елементів: базові станції, вузлові станції, транспортні вузли, центри комутації. Кожен з цих елементів має свою внутрішню структуру побудови, технологію, а, відповідно, рівень споживання електроенергії. Нерівномірні відключення електроживлення на мережі призводять до частково непрацюючих елементів (базові станції, транспортні вузли тощо), що в свою чергу має наслідки у вигляді нерівномірного покриття різних стандартів (GSM, UMTS, LTE) [1] або його відсутності, погіршення якості сервісів або часткова недоступність, збільшення навантаження на окремі вузли мережі. Для запобігання масових відключень мережі оператори мобільного зв'язку встановлюють додаткове обладнання, здатне підтримувати доступність окремих вузлів – мобільні та стаціонарні генератори, АКБ, сонячні панелі та інше, кожен з яких має різні технічні параметри [1,2]. Враховуючі складність побудови мережі, нерівномірність відключень електроживлення, різні типи додаткового обладнання потребують побудови моделі роботи мережі під час нештатних

ситуацій/ блек-аутів. Розглянемо основні моделі роботи мережі та дослідимо найефективніший підхід по основним критеріям - доступність мережі (відсоток часу, за який мережа була доступна з дотриманням мінімальних параметрів якості сервісів), відсоток покриття та середня швидкість передачі даних (в мережі LTE) [2,6].

Модель 1, яка побудована на трафіку

Пріоритетність вузлів мережі, розподіл електроживлення, налаштування мережі будується на існуючих даних по трафіку, який проходить через кожний окремий вузол. Тип трафіку, його кількість напряму впливають на пріоритетність роботи вузла мережі, забезпечення його додатковим обладнанням тощо. Основна перевага – дана модель фокусується на тих ділянках мережі, які генерують найбільшу частину трафіку, а, відповідно, мають найбільше навантаження та обслуговують найбільшу кількість девайсів та сервісів. Дана модель має свої недоліки, а саме: нерівномірність розподілу трафіку буде приводити до нерівномірної роботи мережі та зменшення покриття до 5% в порівнянні з іншими моделями. Також дана модель не враховує мобільність абонентів та нерівномірність розподілу навантаження у часі (часи найбільшого та найменшого навантаження) [5].

Модель 2, яка побудована за ієрархією мережі

Мобільна мережа має ієрархічну структуру. Більш критичні, важливіші вузли та станції мають більший пріоритет, ніж віддалені (принцип побудови мережі «зірка» - чим віддаленіше станції, тим менший пріоритет) [3]. Основна перевага даної моделі – простота реалізації та експлуатації, так як дана модель формує та фіксує пріоритети для кожного вузла мережі.

Дана модель має свої недоліки – це відсутність сервісу на певних не пріоритетних ділянках мережі.

Модель 3, яка передбачає пріоритетність покриття мережі

Кожен стандарт (GSM, UMTS, LTE) мобільної мережі має певний діапазон частот, який впливає на покриття. Дана модель роботи мережі під час блек-аутів пріоритезує ресурс мережі через підтримання максимально можливого покриття [4]. Дана модель має за свою перевагу доступність сервісів. Одним з основних недоліків є зменшення якості сервісів із-за нерівномірності розподілу клієнтських девайсів та трафіку, що в свою чергу призводить до перенавантаження на окремих ділянках та вузлах (що частково може призвести до відсутності сервісів у часи найбільшого навантаження). Дана модель знижує середню швидкість передачі даних до 5%.

Модель 4, яка передбачає зниження ключових показників ефективності мережі (Key Performance Indicator – далі KPi)

На якість сервісів впливають встановлені таргети оператором – потужність базової станції (БС), середня швидкість передачі даних по кожній технології, час з'єднання тощо. Зменшення основних KPis балансує споживання електроживлення та продовжує роботу мережі на альтернативних джерелах живлення. З іншого боку, недоліками є зменшення якості сервісів, швидкості передачі даних, що негативно впливає на клієнтський досвід.

Також існують інші параметри, на основі яких можливо моделювати роботу мережі під час відключень електроживлення, такі як:

- тип живлення;
- ємність альтернативних джерел живлення [7];
- додаткові сервіси, які працюють на мережі (наприклад, фіксований інтернет);
- відключення несучих;
- зміна режиму роботу БС в залежності від кількості клієнтських сервісів та типу девайсів;
- перерозподіл трафіку між стандартами і т.д.

Модель 5 - комплексний підхід

Як зазначено вище, кількість параметрів, які впливають та оптимізують роботу мережі мобільного оператора, досить значна. Комплексний підхід передбачає створення універсальної моделі, яка на вході отримує параметри для моделювання – причому модель

будується таким чином, що на вхід може буде передано необмежену кількість параметрів. На виході – модель будує оптимальну роботу мережі під час відключень електроживлення, яка підвищує доступність мережі до 2%, збільшує середню швидкість передачі даних до 6% та зберігає покриття на середньому рівні в порівнянні з іншими розглянутими моделями. В даному підході за допомогою ШІ модель буде використовувати історичні дані мережі, має можливість адаптуватися до нових параметрів та самонавчатися.
Блок схема моделі Комплексного підходу представлена на Рис.1.

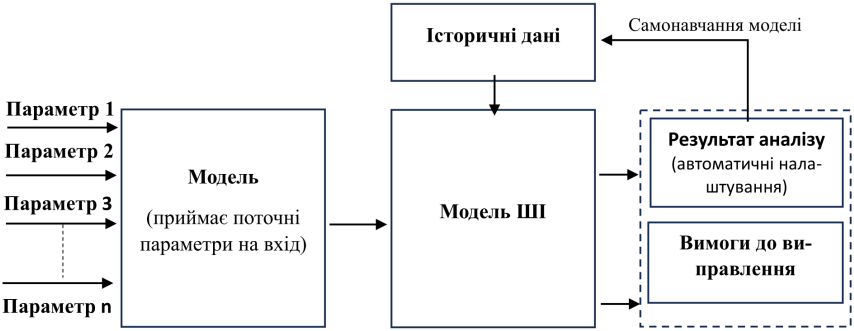


Рис. 1

Комплексний підхід включає в себе основні переваги кожного включеного параметру моделі та здатний знизити споживання мережі, збільшити час її роботи та покращити сервіс під час відключень/блек-аутів основної мережі електроживлення.

Висновки

1) Розглянуті різні підходи по плануванню роботи мережі мобільного зв'язку під час блек-аутів, такі як – модель, яка побудована за трафіком, за ієрархією мережі, за пріоритетністю покриття тощо. Дані моделі мають відповідні недоліки – зменшення покриття, доступності та перевантаження мережі.

2) Розглянута модель комплексного підходу, яка враховує основні параметри, які впливають на якість роботи мережі під час блек-аутів. Запропонована модель здатна підвищити доступність мережі до 2% та збільшує середню швидкість передачі даних до 6% в порівнянні з іншими моделями.

3) Сучасні тренди, пов'язані з ШІ, спрямовані на розширення можливостей моделі комплексного підходу за допомогою аналізу історичних даних та самонавчання, що в свою чергу направлене на покращення якості мережі під час відключень електроживлення.

Література

1. Matyokubov U.K., Davronbekov D.A. The Impact of Mobile Communication Power Supply Systems on Communication Reliability and Viability and Their Solutions. 2020. P. 7-18

2. Alan Wiig. Demanding Connectivity, Demanding Charging: The Co-production of Mobile Communication Between Electrical and Digital Infrastructures. 2018. P. 107-112

3. Аббас Джамаліпур. The Wireless Mobile Internet: Architectures, Protocols and Services. Wiley. John Wiley & Sons, LTD. 2003.

4. Seppo Borenius, Petri Ahokangas. Smart grid evolution and mobile communications —Scenarios on the Finnish power grid. 2021. P. 18-20.

5. Рівні якості послуг рухомого (мобільного) зв'язку (затверджені наказом Мінтрансзв'язку від 19.03.2010 № 147 та зареєстрованим в Міністерстві юстиції України 6 квітня 2010 за № 277/17572).
6. Показники якості послуг із передачі даних, доступу до Інтернету та їх рівні (затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 28.12.2012 № 803 та зареєстрованим в Міністерстві юстиції України 21.01.2013 за № 135/22667).
7. Казанський С. В. Надійність електроенергетичних систем : навч. посіб. / С. В. Казанський, Ю. П. Матеєнко, Б. М. Сердюк. – К. : НТУУ «КПІ», 2011. – 216 с. – ISBN 978-966-622-453-1. С. 77-80.

Стрелковська І.В., д.т.н., професор,
Кодимський К.А., магістр 1 курсу навчання
зі спеціальності 121 Інженерія програмного забезпечення
Міжнародний гуманітарний університет
i.strelkovskaya@mgu.edu.ua, kirill.kodymskyi@gmail.com

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ СПЛАЙН- ТА ВЕЙВЛЕТ-ЕКСТРАПОЛЯЦІЇ В ЗАДАЧАХ ПРОГНОЗУВАННЯ ТРАФІКА

Анотація. *Розглянуто завдання прогнозування характеристик самоподібного трафіку, що має значну кількість пульсацій та властивість довгострокової залежності, що ускладнює прогнозування на практиці. Запропоновано використання методів сплайн- та вейвлет-екстраполяції. Проведено порівняння результатів прогнозування характеристик самоподібного трафіку на базі кубічної сплайн-функції та Хаар-вейвлету з використанням сплайн- та вейвлет-екстраполяції. Встановлено, що перевагу має вейвлет-екстраполяція, яка дозволяє підвищити точність прогнозування.*

Завдання прогнозування трафіку виникають на етапах проектування комп'ютерних мереж і завжди супроводжуються умовами, які дозволяють характеризувати трафік мережі. До таких властивостей трафіку відноситься самоподібність, що характеризується значними та частими сплесками інтенсивності та виглядають статистично подібними для різних масштабів часу [1], [2]. Така властивість трафіку дозволяє на основі накопичених статистичних даних або на підставі результатів моделювання трафіку прогнозувати його стан у майбутньому. Вирішення завдання прогнозування самоподібного трафіку дозволяє передбачити можливі пікові навантаження в мережі та виконати ефективне керування трафіком, забезпечивши цим необхідні характеристики. При цьому використання короткострокового прогнозування в реальному часі є нагальним питанням для дослідження. Враховуючи вищевикладені факти, можливо, наголосити на актуальності розв'язання задачі – прогнозування самоподібного трафіку.

Питанням прогнозування самоподібного трафіку присвячено значну кількість наукових праць, в яких запропоновані різні методи прогнозування. Одним із загальноприйнятих є моделі лінійної регресії ARIMA і FARIMA [3], які використовуються тільки для короткострокових прогнозів. Однак, для їхнього використання необхідним є точна оцінка параметра Херста, визначення якої для реального масштабу часу є складним завданням. Методи нейронних мереж, зокрема машинного навчання [4], ефективні в прогнозуванні та дозволяють вирішити багато практичних завдань, однак, значними є витрати на навчання мережі та отримання значної кількості даних. Точність прогнозу в такій мережі залежить від кількості варіантів її навчання, а реалізація має високі вимоги до обчислювальних можливостей. Раніше авторами [1], [2] отримано результати короткострокового прогнозування самоподібного трафіку за допомогою методу сплайн-екстраполяції [1], при цьому використання кубічних сплайн-функцій показало перевагу

їхнього використання, особливо для прогнозів в реальному масштабі часу. Використання вейвлет-екстраполяції, за думкою авторів [2], має більше переваг, особливо для трафіку з частими пульсаціями. Розглянемо вирішення завдання прогнозування характеристик самоподібного трафіку за допомогою сплайн- та вейвлет-екстраполяції.

Метою даної роботи є порівняльний аналіз методів сплайн- та вейвлет-екстраполяції в задачах прогнозування трафіку з метою підвищення точності прогнозування.

Для вирішення поставленого завдання прогнозування самоподібного трафіку використовуємо метод екстраполяції, запропонований авторами у роботах [1], [2] було використано метод екстраполяції. Тоді завдання дослідження полягає в наступному [2]:

1) спрогнозувати самоподібний трафік за межами розглянутого проміжку часу, на якому розглядається передача даних;

2) підібрати метод, за допомогою якого можна виконати більш точний прогноз самоподібного трафіку, використовуючи метод сплайн-екстраполяції бо вейвлет-екстраполяції;

3) визначити похибку екстраполяції самоподібного трафіку.

Розглянемо самоподібний трафік на відрізку [4100;4500] мс, показаний на рис. 1, де N– кількість пакетів, t – час надходження пакетів.Трафік, змодельований за допомогою NetFlow Analyzer [5] на відрізку [4100;4500] мс, є самоподібним з інтенсивністю надходження пакетів $\lambda = 250$ пак/с, μ– тривалістю обслуговування пакетів в системі, $\mu = 150$ пак/с та параметром Херста H=0,75. З рис. 1 видно, що трафік має інваріантність, характеризується наявністю «сплесків» інтенсивності та довгостроковою залежністю між моментами їх надходження.

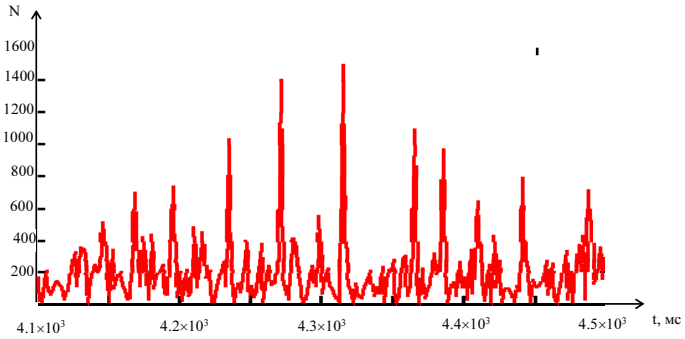


Рисунок 1 – Самоподібний трафік на відрізку [4100; 4500] мс

Для прогнозування характеристик трафіку використаємо сплайн-екстраполяцію на базі кубічного сплайну [1]. Розглянемо самоподібний трафік на відрізку $[a;b]$. Нехай на цьому відрізку $[a;b]$ задано розбиття Δ: $a = x_0 < x_1 < \ldots < x_N = b$. У вузлах сітки Δ задані значення інтенсивності самоподібного трафіка $f_i = f(x_i)$, що описуються функцією $f(x)$, яка визначена на відрізку $[a;b]$.

Кубічний інтерполяційний сплайн $S_3(x)$, що побудовано на проміжку $[x_i, x_{i+1}]$, $i = 0, 1,\ldots, N-1$, має вигляд [1]:

$$S_3(x) = f_i(1-t)^2(1+2t) + f_{i+1}t^2(3-2t) + m_i h_i t(1-t)^2 - m_{i+1}h_i t^2(1-t), \qquad (1)$$

де $t = (x - x_i)/h_i$, $S_3(x_i) = f_i$, $S_3(x_{i+1}) = f_{i+1}$, $m_i = S'(f; x_i)$.

Для визначення кубічного сплайна виду (1) на відрізку [*a;b*] використовуються граничні умови [1]:

$$S'(f;a) = f'(a),\ S'(f;b) = f'(b). \qquad (2)$$

Розглядається рівномірне розбиття відрізку [*a;b*], тобто $h_i = h = \frac{b-a}{N}$, i = 0, 1,…, N–1.

Результати прогнозування трафіку за допомогою сплайн-екстраполяції показано на рис. 2. Трафік розглянуто зовні відрізку [*a;b*], а саме, правіше точки *b*. Для визначеності це буде точка x_c, $x_c > x_N = b$, $x_c - b = h$, де h– крок розбиття відрізку [*a;b*] [1]. Використовуючи вихідні дані, отримуємо екстраполяцію трафікуна відрізку [4330;4350] мс за допомогою кубічного сплайна (рис. 2).

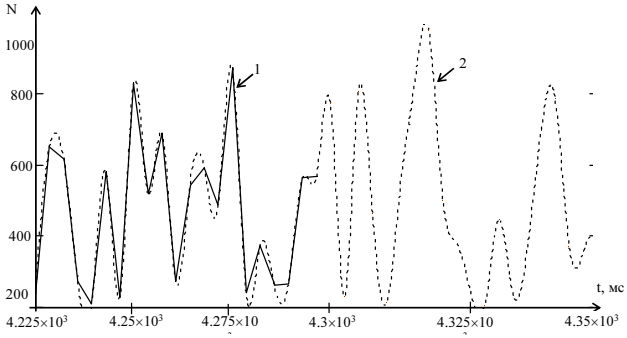


Рисунок 2 – Сплайн-екстраполяція трафіку на відрізку [4300; 4350] мс,
1) самоподібний трафік, 2) екстраполяція самоподібного трафіку за допомогою кубічного сплайну

Використовуючи кубічний сплайн для прогнозування трафіку на відрізку [4300; 4350] мс, отримано екстраполяцію трафіку, яку показано на рис. 2. Результати похибки сплайн-екстраполяції самоподібного трафіку наведено у табл. 1.

Вайвлет-перетворення, згідно [2], дозволяють виконати екстраполяцію трафіку як у часовій області за допомогою базисної вейвлет-функції $\psi(x)$, так і у частотній за допомогою масштабуючої скейлинг-функції $\varphi(x)$:

$$\psi(x) = \sqrt{2}\sum_k g_k \varphi(2x-k),\ \ \varphi(x) = \sqrt{2}\sum_k h_k \varphi(2x-k), \qquad (3)$$

де $h_k = \sqrt{2}\int \varphi(x)\overline{\varphi}(2x-k)dx$, $g_k = (-1)^k h_{(N-1)-k-1}$– коефіцієнти розкладення, k, N – натуральні числа.

Для екстраполяції розглянемо простішу вейвлет-функцію –вейвлет Хаара, коротке прямокутне коливання на інтервалі [0,1], яке має довгий "хвіст" у частотній області і може бути використано для трафіку. Для Хаар-вейвлету згідно [2], аналітичний запис його базисної вейвлет-функції $\psi(x)$та скейлинг-функції $\varphi(x)$ мають наступний вигляд:

$$\psi(t)=\begin{cases}1,\ 0\le t<1/2,\\ -1,\ 1/2\le t<1,\\ 0,\ t<0,\ t\ge 1.\end{cases}\quad \varphi(t)=\begin{cases}1,\ 0\le t<1,\\ 0,\ t<0,\ t\ge 1.\end{cases} \qquad (4)$$

Базисна материнська вейвлет-функція $\psi(x)$ та скейлінг-функція $\varphi(x)$ належать ортогональним підпросторам Гільбертового простору $L^2(R)$, що відповідає умовам [2]:

$$\sum_k h_k g_{k+2M} = 0, \qquad (5)$$

де $h_k = \sqrt{2}\int \varphi(x)\overline{\varphi}(2x-k)dx$, $g_k = (-1)^k h_{(N-1)-k-1}$ – коефіцієнти розкладання, k, N – натуральні числа.

Згідно (2) визначаються залежність між коефіцієнтами h_k та g_k Хаар-вейвлету:

$$g_k = (-1)^k h_{2M-1-k}. \qquad (6)$$

де вейвлет-коефіцієнти $s_{j,k}$ и $d_{j,k}$ визначаються з виразів:

$$s_{j-1,k} = \sum_m h_m s_{j,2k+m},\ d_{j-1,k} = \sum_m g_m s_{j,2k+m}, \qquad (7)$$

де h_m, g_m – коефіцієнти апроксимації та розкладання.

Розраховані значення коефіцієнтів значень Хаар-вейвлета h_k, g_k та значення коефіцієнтів вейвлет-перетворень $s_{j,k}$, $d_{j,k}$ дозволяють отримати екстраполяцію трафіку на базі Хаар-вейвлета.

Розглянемо самоподобний трафік, який описується функцією $f(x)$, яка визначена на відрізку, що розглядається. Екстраполяцію самоподібного трафіку $f(x)$ з використанням вейвлет-функції Хаара (рис. 1), заданого його базисною функцією $\psi(x)$та масштабуючою скейлинг-функцією $\varphi(x)$ формулами (4) – (7).

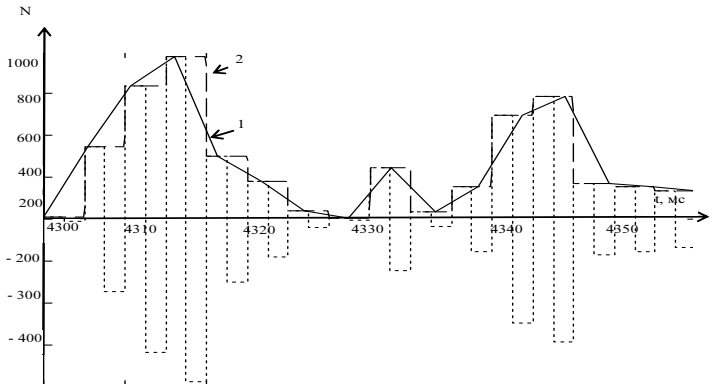


Рисунок 3 – Вейвлет-екстраполяція трафіку на відрізку [4300; 4350] мс,
1) самоподібний трафік, 2) екстраполяція самоподібного трафіку за допомогою Хаар-вейвлету

Умовою екстраполяції за допомогою вейвлет-функції є визначення кількості відліків, $N = 2^{jn}$, де $j_n \geq 1$ визначає максимально можливу кількість рівнів масштабування [2]. В данному випадку $j_n = j_{max} = 4$, $N = 2^4 = 16$Екстраполяція трафіку за допомогою Хаар-вейвлетадля трафіку на відрізку [4300; 4350] мс, материнський вейвлет $\psi(x)$ та маштабуюча функція $\varphi(x)$ визначаються формулами(4) – (7).

Значення похибки екстраполяції самоподібного трафіку за допомогою вейвлет-екстраполяції наведені у табл. 1.

Таблиця 1 – Порівняння значень похибки з використанням сплайн- та вейвлет-екстраполяції

Відрізок	Чисельні значення	Значення похибки з використанням сплайн-екстраполяції	Значення похибки з використанням вейвлет-екстраполяції
$[x_0;x_1]$	[4300;4310]	6,1	2,1
$[x_1;x_2]$	[4310;4320]	3,4	1,4
$[x_2;x_3]$	[4320;4330]	4,6	2,6
…	…	…	…
$[x_4;x_5]$	[4340;4350]	10,3	5,3

Висновки

1. Розглянуто задачу прогнозування характеристик самоподібного трафіку за допомогою сплайн-екстраполяції на базі кубічних сплайнів та вейвлет-екстраполяції на базі Хаар-вейвлету.

2. Проведено порівняльний аналіз результатів сплайн- та вейвлет-екстраполяції на конкретному прикладі за результатами якого перевагу має вейвлет-екстраполяція.

3. Використання вейвлет-екстраполяції для вирішення задач прогнозування трафіку має низку переваг:

– достатня простота у реалізації, мала ресурсомісткість та невелика похибка, що дозволяє використання для прогнозування трафіку у реальному масштабі часу;

– застосування Хаар-вейвлета для екстраполяції самоподібного трафіку, що характеризується сплесками інтенсивності і різкими зростаннями функції, призводить до глобального згладжування, при цьому локальні «сплески» на момент різких змін інтенсивності трафіку мають незначну похибку екстраполяції, меншу ніж для сплайн-екстраполяції. Однак, застосування вейвлет-екстраполяції не заважає відновленню піків інтенсивностей завдяки властивостям масштабованості.

Література

1. Strelkovskaya I. Comparative Analysis of the Methods of Wavelet- and Spline-extrapolation in Problems of Predicting Self-similar Traffic / I. Strelkovskaya, I. Solovskaya, A. Makoganiuk, O. Tsyra/ The Fourth International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2019): proceedings of the Conference, Odessa, Ukraine, 9-13 September, 2019: Odessa National Academy of Telecommunication named after O.S. Popov. – P. 1-6.

2. Strelkovskaya I. Multimedia Traffic Prediction Based on Wavelet- and Spline-extrapolation / I.Strelkovskaya, I. Solovskaya, A. Makoganiuk, T. Rodionova // IEEE International Black Sea Conference on Communications and Networking: proceedings of the 8th Black Sea Conference, Odessa, Ukraine, May 26-29, 2020.

3. Iqbal M.F. Efficient Prediction ob Network Traffic for Real-Time Applications / M.F. Iqbal, M. Zahid, D. Habib, L.K. John // Journal of Computer Networks and Communications. – 2019. – Vol. 1.

4. Y. Zang , F. Ni , Z. Feng, S. Cui and Z. Ding, «Wavelet Transform Processing for Cellular Traffic Prediction in Machine Learning Networks», 2015 IEEE China Summit and International Conference on Signal and Information Processing, China, July 2015 [Processing Conference on Signal and Information Processing, 2015].
5. https://www.manageengine.com/

УДК 621.391

Шендерей В.О., Волохов О.О.
Міжнародний гуманітарний університет
Науковий керівник
Розенвассер Д.М.
кандидат технічних наук,
доцент кафедри комп'ютерних наук
Міжнародний гуманітарний університет

ОЦІНКА ЕФЕКТИВНОСТІ КОДОВИХ КОНСТРУКЦІЙ

***Анотація**. Оцінка ефективності використання кодових конструкцій є складною задачею, яка залежить від багатьох факторів.Класичні завадостійкі коди не завжди відповідають сучасним критеріям щодо якості та швидкості виправлення помилок. В даній роботі розглянуті сучасні кодові конструкції, їхня класифікація та ефективність.*

Комп'ютерні мережі постійно стикаються з проблемою шумів, які можуть призвести до втрати та спотворення даних. Це може мати негативний вплив на роботу різних програм, особливо тих, що потребують надійної та безперебійної передачі інформації.

До поширених причин проблем з передачею даних належать втрата пакетів та затримка пакетів, які можуть виникати через перевантаження мережевих пристроїв, колізії або обмежену пропускну здатність каналу та спотворення пакетів, що може бути викликано помилками при передачі даних або впливом зовнішніх факторів.

Традиційні протоколи передачі даних, такі як TCP, використовують механізми автоматичного повторного запиту (ARQ) для забезпечення надійності. ARQ передбачає повторну передачу втрачених або пошкоджених пакетів, що гарантує доставку даних одержувачу. Однак ARQ не завжди є оптимальним рішенням, особливо для чутливих до затримки додатків, таких як потокове аудіо та відео. Повторні передачі пакетів можуть призвести до значних затримок, що неприйнятно для таких програм.

До класичних завадостійких кодів відносяться блокові та згорткові коди, які на сьогодні не завжди здатні забезпечити необхідних рівень ймовірності помилки, затримки, та швидкості кодування.

В цій роботі пропонується дослідити альтернативні методи кодування даних, які використовують зворотний канал для виявлення та виправлення помилок. Це дозволяє покращити стійкість передачі даних до шумів без істотного збільшення затримок.

В рамках цієї роботи буде проведено дослідження та аналіз різних методів кодування з зворотним каналом. Буде розроблено та протестовано прототип системи, яка використовує один з обраних методів кодування. За результатами дослідження буде зроблено висновок про те, який метод кодування є найбільш ефективним для передачі даних в комп'ютерних мережах з урахуванням таких факторів, як затримка, пропускна здатність та якість передачі.

Оцінка ефективності використання кодових конструкцій є складною задачею, яка залежить від багатьох факторів.

Різні типи каналів, такі як дротові, бездротові та оптичні, мають різні характеристики шуму та завад, що впливає на вибір оптимальної кодової конструкції.

Кодові конструкції можуть бути розроблені для виправлення різних типів помилок, таких як помилки з одним бітом, помилки з пакетами та вибухи помилок. Різні кодові конструкції пропонують різні компроміси між швидкістю передачі даних та стійкістю до помилок. Деякі кодові конструкції є більш складними для реалізації, ніж інші, що може вплинути на їх практичну придатність.

Існує декілька методів для оцінки ефективності використання кодових конструкцій:

- аналітичні методи, що дозволяють обчислити теоретичну ефективність кодової конструкції;

- моделювання, що може використовуватися для оцінки ефективності кодової конструкції в більш реалістичних умовах, враховуючи такі фактори, як нелінійні ефекти каналу та синхронізаційні помилки.

- експериментальні методи, що дозволяють оцінити продуктивність кодової конструкції в реальній системі.

До ключових показників, які використовуються для оцінки ефективності використання кодових конструкцій, відносяться:

- швидкість кодування, що визначає, яка частка вхідних даних використовується для кодування надлишкових бітів. Більш висока швидкість кодування зазвичай призводить до більшої стійкості до помилок, але також зменшує пропускну здатність каналу.

- бітова помилка (BER) визначає ймовірність того, що біт буде помилково прийнятий після декодування. Низький BER є важливим для таких застосунків, як передача даних, де важлива точність.

- пропускна здатність, що визначає максимальну швидкість, з якою дані можуть бути передані по каналу. Кодові конструкції з більш високою швидкістю кодування зазвичай мають меншу пропускну здатність.

- затримка, що визначає час, необхідний для кодування та декодування даних. Низька затримка є важливою для таких застосунків, як голосовий зв'язок, де важлива чутливість до часу.

- складність реалізації кодової конструкції, яка може вплинути на її практичну придатність. Більш складні кодові конструкції зазвичай потребують більше апаратних та програмних ресурсів.

Для сучасних телекомунікаційних систем більш актуальною є нова класифікація, яка враховує нові розробки в цій галузі.

1. Каскадні коди, послідовне зєднання декількох класичних кодів з перемежуванням.

2. Турбоподібні паралельні структури об'єднують декілька простих кодів в більш складну систему.

3. М'яке декодування. Еволюція методів декодування призвела до переходу від жорсткого декодування (визначення помилок) до м'якого декодування (оцінка ймовірності помилок).

4. Ітераційне декодування, що використовує інформацію про ймовірність помилок, отриману з попередніх ітерацій, для покращення точності декодування. Ітеративний процес декодування дозволяє досягти значно кращої стійкості до помилок, ніж у простих кодів.

5. Нові базові конструкції, які можна використовувати як самостійно, так і в складі каскадних структур. Ці конструкції часто пропонують кращі характеристики, такі як гнучкість та ефективність, порівняно з традиційними кодами.

Складні кодові конструкції, такі як турбо, каскадні, фонтанні та полярні коди, пропонують кращу стійкість до помилок у порівнянні з простими кодами, але зазвичай мають більш складну структуру та реалізацію.

Фонтанні коди - це тип кодової конструкції, яка розбиває дані на декілька незалежних потоків, які можна передавати по мережі. Фонтанні коди стійкі до втрати

пакетів, оскільки одержувач може відтворити оригінальні дані, отримавши лише частину потоків.

Полярні коди - це тип кодової конструкції, яка використовує канал з різним рівнем шуму в різних частотних діапазонах. Полярні коди можуть бути дуже ефективними в каналах з шумом, що змінюється, але їх реалізація може бути складною.

Важливо зазначити, що дослідження кодових конструкцій є постійно активною областю досліджень. Розробляються нові кодові конструкції, які пропонують кращі компроміси між різними показниками.

Література:

1. Tahir B., Schwarz S., Rupp M. BER comparison between Convolutional, Turbo, LDPC, and Polar codes," : 2017 24th International Conference on Telecommunications (ICT), Limassol 3-5 May 2017, Limassol 2017, pp. 1-7.

2. Наритник, Т. М. Особливості формування сигнально-кодових конструкцій на основі технології Wi-Fi для побудови телекомунікаційних систем терагерцового діапазону [Текст] / Т. М. Наритник, С. О. Осипчук, Л. О. Уривський // Проблеми телекомунікацій. – 2015. – № 2 (17). – С. 37-53.

3. Kaykac Egilmez Z. B., Xiang L., Maunder R. G., Hanzo L. The Development Operation and Performance of the 5G Polar Codes : IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 96-122, 2020 //doi.org/10.1109/COMST.2019.2960746.

4. Пятін І.С., Бойко Ю.М. Методика полярного кодування в 5G мобільних засобах телекомунікацій багатопозиційною модуляцією : Вимірювальна та обчислювальна техніка в технологічних процесах. 2020. №1 С.67-76.

5. Пятін, І., & Бойко, Ю. (2022). Порівняння продуктивності завадостійких кодів на основі програмного HDL моделювання для захищених інформаційних технологій. Інфокомунікаційні та комп'ютерні технології, 1(03), 43-68. https://doi.org/10.36994/2788-5518-2022-01-03-03.

6. Бойко, Ю., & П'ятін, І. (2023). Особливості формування кодової надлишковості у каналах передачі інформації. Інфокомунікаційні та комп'ютерні технології, 2(04), 12-25. https://doi.org/10.36994/2788-5518-2022-02-04-01.

7. Зубенко, В. О., Березюк, І. А., & Телюта, Р. В. (2023). Обгрунтування шляхів удосконалення методів завадостійкого кодування. Таврійський науковий вісник. Серія: Технічні науки, (2), 68-77. https://doi.org/10.32782/tnv-tech.2023.2.8

8. Bioglio V., Condo C. Land I. Design of Polar Codes in 5G New Radio : IEEE Communications Surveys & Tutorials, pp. 1, Jan. 2020.

УДК 621.314

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Розга Ратібор Альгімантасович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 172 Електронні комунікації та радіотехніка
Міжнародний гуманітарний університет

ВИЗНАЧЕННЯ ПИТОМИХ ПОКАЗНИКІВ ІНДУКТИВНИХ ЕЛЕМЕНТІВ ДЛЯ ПЕРЕТВОРЮВАЧІВ НАПРУГИ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Анотація. *Отримано формули для розрахунку питомих показників індуктивних елементів для перетворювачів напруги телекомунікаційного обладнання: дроселів та трансформаторів. Показано що за всіх однакових інших умов для дроселів потрібні магнітопроводи, що повинні мати щонайменше у вісім разів більші геометричні розміри, порівняно із магнітопроводами трансформаторів. Отримані результати дозволяють більш глибоко розібратися в електричних та енергетичних процесах, що протікають в імпульсних перетворювачах електричної енергії та покращити техніко-економічні показники телекомунікаційного обладнання, складовою частиною яких вони є.*

Перетворювачі електричної енергії є важливим компонентом сучасних телекомунікаційних засобів. До переліку функцій, які виконують імпульсні перетворювачі в телекомунікаційних пристроях та системах, відносяться зміна рівня постійної та змінної напруги, перетворення однополярної напруги в багатополярну, перетворення роду струму (постійний в змінний і навпаки), корекція коефіцієнту потужності, створення електрично ізольованих джерел напруги та багато інших.

На сьогоднішній день, перетворювачі, що використовуються в телекомунікаційному обладнанні, перетворюють електричну енергію імпульсним способом, який забезпечує найкращі техніко-економічні показники порівняно з іншими методами перетворення, наприклад, електромеханічним. Особливістю імпульсного перетворення є необхідність використання індуктивних елементів: дроселів, спроможних накопичувати енергію в магнітному полі магнітопровода, та трансформаторів, призначених для передавання та перетворення параметрів енергії без її накопичення в магнітному полі. Розміри усіх, без винятку, індуктивних елементів безпосередньо залежать від їх потужності – кількості енергії, що проходить через магнітне поле їхнього магнітопроводу за одиницю часу. Це призводить до того, що реактивні елементи, що використовуються в силовій частині імпульсних перетворювачів, дуже часто стають самими габаритними, важкимита дорогими елементами в телекомунікаційні техніці. При цьому додаткове збільшення вартості реактивних елементів обумовлено використанням дорогих матеріалів з унікальними властивостями, наприклад, феритів або пермалоїв. Таким чином, зменшення розмірів, ваги та вартості індуктивних елементів є актуальною задачею, яка виникає перед розробниками електронного обладнання кожного разу, коли необхідно перетворити параметри електричної енергії.

Схемотехніка імпульсних перетворювачів постійно розвивається та вдосконалюється. З кожним роком у цій галузі з'являються нові схемотехнічні рішення, які дозволяють покращити ті, чи інші показники перетворювача [1]. Проте питання порівняння питомих показників різних типів індуктивних елементів поки що залишається відкритим. Це і обумовило мету цієї роботи, яка полягає у визначенні питомих показників індуктивних елементів для перетворювачів напруги телекомунікаційного обладнання.

Найпростіший індуктивний елемент, призначений для накопичення або передачі енергії, складається із магнітопроводу та щонайменше однієї обмотки з числом обвитків N, яка зв'язує електричну схему із магнітним полем, зосередженим в магнітопроводі (рис. 1) [2].Головними параметрами будь-якого магнітопроводу, окрім параметрів магнітного матеріалу, що використовувався для його виготовлення, є середня довжина магнітної лінії $L_{СР}$, площа перерізу магнітопроводу S_C та площа вікна, призначеного для розташування обмоток S_O. Добуток довжини середньої лінії на площу перерізу магнітопроводу дадуть об'єм активної частини магнітного матеріалу V:

$$V = S_C L_{СР}. \tag{1}$$

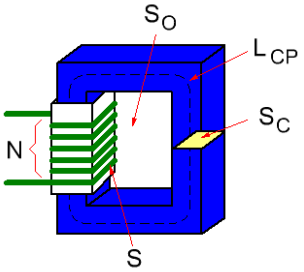


Рисунок 1 – Будова найпростішого індуктивного елемента

Через конструктивні обмеження, наприклад, для магнітопроводів броньового типу, реальний об'єм магнітного матеріалу може бути більшим за значення отримане по формулі (1). Проте у цьому дослідженні надалі будемо вважати, що формула (1) справедлива для усіх магнітопроводів (наприклад, вона справедлива для тороїдальних магнітопроводів).

В процесі роботи по обвиткам обмотки протікає електричний струм I, який, відповідно до закону Джоуля-Ленца, призводить до її нагрівання. При розрахунках індуктивних елементів використовують спрощений метод визначення необхідного перерізу проводу, який полягає у завданні певної густини струму J, яка залежно від призначення індуктивного елемента та умов його експлуатації може знаходитися в межах $J = 2…8$ А/мм^2. Таким чином, площа S, яку займає обмотка у вікні магнітопроводу, визначається формулою:

$$S = N\frac{I}{J}. \tag{2}$$

Кількість обвитків обмоткиNбезпосередньо зв'язана із змінами магнітного потоку$\Delta\Phi$, які відбуваються в магнітному полі магнітопроводу. Якщо на виводах обмотки протягом часу Δtприсутня напруга U. Відповідно до закону Фарадея:

$$\Delta\Phi = \frac{U\Delta t}{N}. \tag{3}$$

Магнітний потік визначається як добуток величини магнітної індукції B та площу перерізу магнітопроводу S_C. Таким чином, зміна магнітного потоку в магнітопроводі трансформатора пропорційна зміні магнітної індукції:

$$\Delta\Phi = S_C\Delta B. \tag{4}$$

Якщо визначити з формули (3) кількість обвитків N і підставити її у формулу (2), то з урахуванням (4) отримаємо:

$$S = \frac{IU\Delta t}{JS_C\Delta B}. \tag{5}$$

З формули (5) видно, що площаS, яку займає обмотка у вікні магнітопроводу, безпосередньо пов'язана з кількістю енергії, що проходить через індуктивний елемент,

густинами електричному струму (J) та магнітного поля (B). Таким чином, для того, щоб створити індуктивний елемент із необхідними енергетичними показниками, потрібен магнітопровід, розміри якого відповідають нерівності:

$$S_O S_C \geq \frac{IU\Delta t}{J\Delta B}. \tag{6}$$

В трансформаторах, які призначені для передачі енергії, енергія, що накопичується в магнітопроводі трансформатора, є реактивною – вона періодично переміщується між джерелом первинного живлення і магнітопроводом, і часто не виходить за межі цього кола. Це дозволяє максимально збільшити величину ΔB – до величини$\Delta B \leq 2B_{\text{MAX}}$, де B_{MAX}–максимально допустима індукція для магнітного матеріалу. Таким чином, за час Δtтрансформатор спочатку повертає з магнітопроводу у джерело живлення енергію, пропорційну B_{MAX}, а потім накопичує від джерела живлення таку ж саму кількість енергії.

Для дроселя такі енергетичні процеси небажані, оскільки дросель за час Δt повинен накопичити певну кількість енергії для того, щоб віддати її протягом іншого проміжку часу. Оскільки будь яка зміна знаку магнітної індукції B супроводжується переходом магнітоного потоку через нульове значення, що еквівалентно розряду дроселя, то максимальна зміна магнітної індукції в магнітопроводі дроселя не може перевищувати B_{MAX}. В реальних схемах, через додаткові технічні обмеження, наприклад, через наявність ефекту залишкової намагніченості, практичне значення магнітної індукції не перевищує $0{,}5B_{\text{MAX}}$.

Трансформатори імпульсних перетворювачів, зазвичай працюють із напругами прямокутної форми. Крім того, форма струму в обмотках зумовлюється навантаженням, тому вона може бути любою, у тому числі і не змінюватися протягом робочого інтервалу Δt. Тому можна вважати, що для трансформатора добуток напруги U та струму I приблизно дорівнює потужності $P = UI$, що проходить через трансформатор. Періодроботи трансформатора дорівнює подвоєному часу перемагнічування магнітопроводу ($T = 2\Delta t$). Таким чином, частота на якій працює трансформатор буде дорівнювати:

$$f = \frac{1}{T} = \frac{1}{2\Delta t}. \tag{7}$$

І наостанок слід врахувати, що в трансформаторі струми, що намагнічують та розмагнічують його магнітопровід, протікають одночасно. Тому для трансформатора площа вікна, необхідного для розташування його обмоток повинна бути вдвічі більша, порівняно із площею вікна магнітопровода дроселя. Таким чином, мінімально необхідні розміри для магнітопровода трансформатора можна визначити за формулою:

$$\frac{S_O S_C}{P} \geq \frac{0{,}5}{\text{к}_\text{С}\text{к}_\text{О} J B_{MAX} f}, \tag{8}$$

де $\text{к}_\text{С}$ – коефіцієнт заповнення вікна магнітопроводу магнітним матеріалом; $\text{к}_\text{О}$ – коефіцієнт заповнення вікна проводом.

У трансформаторі енергія передається в навантаження при любій зміні магнітного потоку: і позитивній, і негативній. На відміну від трансформатора, дросель при збільшенні магнітного потоку енергію накопичує, а при зменшенні – віддає в електричну схему. Кількість енергії E, яка накопичується або віддається дроселем протягом часу Δt визначається формулою:

$$E = UI\Delta t\,, \tag{9}$$

де I – середнє значення струму в обмотці протягом інтервалу Δt.Якщодросель працює в межовому режимі – режимі в якому енергетична ємність магнітопровода використовується максимально ефективно – тоді середнє значення струму дорівнює половині розмаху струму I_{MAX} ($I = 0{,}5I_{MAX}$).

Потужність, яка передається в навантаження, при використанні дроселя буде вдвічі менша, порівняно із потужністю трансформатора, оскільки на одному інтервалі часу дросель енергію накопичує, а на наступному інтервалі – її віддає. Якщо тривалість інтервалів накопичення та повернення енергії однакова, тоді потужність перетворювача, що використовує дросель для перетворення параметрів електричної енергії, визначається формулою:

$$P = \frac{E}{2\Delta t} = \frac{UI}{2}. \tag{10}$$

Оскільки період роботи дроселя складається із двох інтервалів тривалістю Δt, то частота роботи дроселя визначається формулою (7). Таким чином, мінімально необхідні розміри для магнітопроводу дроселя можна визначити за наступною формулою:

$$\frac{S_O S_C}{P} \geq \frac{4}{\kappa_C \kappa_O J B_{MAX} f}. \tag{11}$$

Аналіз формул (8) та (11) показує, що за усіх інших однакових умовах розміри магнітопроводу дроселя повинні бути щонайменше в вісім разів більшими за розміри магнітопроводу трансформатора. Таким чином, якщо є така можливість, то замість дроселів слід використовувати трансформатори. Проте повністю відмовитися від дроселів в імпульсних перетворювачах дуже важко, оскільки трансформатори мають фіксований коефіцієнт передачі і непридатні для точного або плавного регулювання напруги. Одним з методів зменшення розмірів індуктивних елементів є використання технології подвійного перетворення, коли за допомогою трансформаторів виконується груба зміна рівня напруги, а за допомогою дроселів – остаточне точне регулювання.

Висновки

Отримано формули для розрахунку питомих показників індуктивних елементів для перетворювачів напруги телекомунікаційного обладнання. Показано що за всіх однакових інших умов для дроселів потрібні магнітопроводи, що повинні мати щонайменше у вісім разів більші геометричні розміри, порівняно із магнітопроводами трансформаторів.

Література

1. Zehendner M., Ulmann M. Power Topologies Handbook. Texas Instruments, 2016. 216c.

2. Kadatskyy A.F., Rusu A.P. Determination of the necessary inductor core dimensions for switching electrical energy converters.*Наукові праці ОНАЗ ім. О.С. Попова*. 2018. №1. С.125-134.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

УДК 004.8:371.3

Непомящий І.О.
здобувач другого (магістерського) рівня вищої освіти
факультету кібербезпеки, програмної інженерії
та комп'ютерних наук
спеціальність: 014.09 «Середня освіта (Інформатика)»
igornesan@gmail.com
Міжнародний гуманітарний університет
м. Одеса, Україна

Науковий керівник
Григор'єва Т.І.
кандидат технічних наук, доцент,
завідувачка кафедри інформаційних технологій
факультету кібербезпеки, програмної інженерії
та комп'ютерних наук
tig15090808@gmail.com
Міжнародний гуманітарний університет

ПЕРЕВАГИ І НЕДОЛІКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТІ

Анотація. *Впровадження штучного інтелекту в навчальні процеси може суттєво змінити підхід до викладання та навчання, зробити освіту більш доступною та ефективною. В роботі розглянуто деякі інноваційні ідеї та перспективи використання штучного інтелекту в освіті. Проведено аналіз переваг і недоліків застосування штучного інтелекту в освіті.*

Одним із пріоритетних напрямків розвитку освіти в Україні є впровадження сучасних інформаційно-комп'ютерних технологій [1-3], що сприятимуть підвищенню доступності освіти та вдосконаленню навчального процесу. Штучний інтелект має значний потенціал для трансформації освіти, пропонуючи нові можливості для навчання, викладання та управління освітніми процесами. Проте, його впровадження також супроводжується певними викликами та ризиками [4,5]. Нижче розглянемо основні ідеї, переваги і недоліки застосування в освіті.

1. Персоналізоване навчання

Однією з головних переваг штучного інтелекту є можливість адаптації навчального процесу під індивідуальні потреби учнів. Адаптивні навчальні платформи, що використовують алгоритми машинного навчання, можуть аналізувати успішність кожного учня і пропонувати матеріали, які найкраще відповідають його рівню знань та темпу навчання. Це дозволяє забезпечити персоналізований підхід, який сприяє глибшому розумінню матеріалу та підвищенню мотивації до навчання.

2. Автоматизація оцінювання

Штучний інтелект може суттєво спростити процес оцінювання знань учнів. Автоматизовані системи оцінювання здатні швидко і об'єктивно перевіряти роботи, зокрема тести з множинним вибором, програмні коди та навіть есе. Це звільняє викладачів від рутинної роботи, дозволяючи їм зосередитися на більш творчих та інтерактивних аспектах навчання. Штучний інтелект також може допомогти вчителям у написанні звітів, упорядкуванні матеріалів та генерації контенту, який можна використовувати як зразок.

3. Інтелектуальні репетитори та віртуальні асистенти

Віртуальні асистенти, керовані штучного інтелекту, можуть відповідати на запитання учнів у режимі реального часу, надавати пояснення до складних тем та

допомагати з виконанням домашніх завдань. Інтелектуальні репетитори [6] можуть проводити індивідуальні заняття, адаптуючи свій підхід відповідно до потреб учня, і забезпечувати підтримку навіть поза класом.

4. Аналіз даних та прогнозування

Штучний інтелект здатний аналізувати великі обсяги даних про навчальний процес та успішність учнів, виявляючи закономірності та тренди, які можуть бути неочевидними для людини. На основі цього аналізу можна прогнозувати успішність учнів, виявляти тих, хто потребує додаткової допомоги, та оптимізувати навчальні плани. Це дозволяє вчасно вживати заходів для підвищення якості навчання та покращення результатів.

5. Віртуальна та доповнена реальність

Інтеграція штучного інтелекту з технологіями віртуальної (VR) та доповненої реальності (AR) відкриває нові можливості для створення інтерактивного та захоплюючого навчального контенту. Учні можуть проводити віртуальні лабораторні роботи, досліджувати історичні події або мандрувати всередині клітини людського організму. Це сприяє глибшому розумінню складних тем та підвищує залученість учнів.

6. Розширення доступу до освіти

Завдяки штучному інтелекту онлайн-курси стають більш доступними та ефективними, що дозволяє забезпечити якісну освіту людям з віддалених регіонів або з обмеженими можливостями. Мовні перекладачі на основі штучного інтелекту дозволяють викладати матеріали на різних мовах, розширюючи доступ до знань для міжнародної аудиторії.

7. Емоційний інтелект та підтримка ментального здоров'я

Системи штучного інтелекту можуть бути оснащені алгоритмами розпізнавання емоцій, що дозволяє вчителям краще розуміти емоційний стан учнів та вчасно реагувати на їхні потреби. Це може допомогти в створенні більш підтримуючого та позитивного навчального середовища, що сприяє покращенню ментального здоров'я учнів.

Недоліки та виклики впровадження штучного інтелекту в освіті

Незважаючи на всі переваги, впровадження штучного інтелекту в освіту також супроводжується певними викликами та ризиками:

1. **Конфіденційність та безпека даних**. Збір та зберігання великої кількості даних про учнів може створювати ризики для конфіденційності та безпеки.

2. **Технічні проблеми та вартість**. Впровадження штучного інтелекту вимагає значних фінансових інвестицій та технічної підтримки, що може бути недоступним для деяких навчальних закладів.

3. **Залежність від технологій**. Надмірна залежність від технологій може призвести до проблем у випадку технічних збоїв або відсутності доступу до інтернету.

4. **Етичні питання.** Використання штучного інтелекту може викликати етичні питання щодо заміни вчителів машинами та впливу на працевлаштування в галузі освіти.

5. **Обмеження алгоритмів.** Алгоритми штучного інтелекту можуть мати обмеження в розумінні контексту та культурних особливостей, що може впливати на якість навчального контенту.

6. **Прогрес та регрес.** Штучний інтелект може бути корисним інструментом для учнів, допомагаючи ефективно засвоювати новий матеріал. Проте існує ризик, що учні можуть використовувати його для пошуку швидких відповідей, не залучаючи власну розумову діяльність. Яскравим прикладом є chatGPT.

Висновки

Впровадження штучного інтелекту в освіту відкриває величезні можливості для покращення навчальних процесів та підвищення якості освіти. Персоналізоване навчання, автоматизація оцінювання, інтелектуальні репетитори та віртуальні асистенти, аналіз даних та прогнозування, а також інтеграція з VR та AR – це лише деякі з напрямків, де штучний інтелект може внести суттєві зміни. Проте важливо враховувати можливі

виклики та ризики, пов'язані з використанням штучного інтелекту, та вживати заходів для їхнього подолання.

Література

1. Інноваційні технології в сучасному освітньому просторі: колективна монографія / За заг. редакцією Г.Л. Єфремової. – Суми: Вид-во СумДПУ імені А. С. Макаренка, 2020. – 444 с.
2. https://vseosvita.ua/webinar/vykorystannia-materialiv-shtuchnoho-intelektu-v-osviti-iak-ne-porushyty-akademichnu-dobrochesnist-1070.html
3. Дзвінчук Д. І., Радченко О. В., & Качмар О. В. Сучасні моделі та форми використання інформаційно-комп'ютерних технологій в освіті. International Academy Journal Web of Scholar , 6(36), 2019. – С.47-54. https://doi.org/10.31435/rsglobal_wos/30062019/6556
4. Європейська інтеграція та трансформація публічного врядування в Україні: матер. наук.-практ. конф. (19 квітня 2024 р., м. Львів) / упорядн.: Буник М. З., Бліщук К. М., Федорчак О. В, Худоба О. В. – Львів: НУ «Львівська політехніка», 2024. – 282 с.
5. Тютюнник О.І. Забезпечення розвитку громадянської освіти на місцевому рівні як чинника формування української національної ідентичності // Перспективи регіонального та місцевого розвитку: матер. 2-ї конференції молодих учених (23 листопада 2023 р., м. Львів) / упорядн.: Матвіїшин Є.Г., Бліщук К.М. – Львів: НУ «Львівська політехніка», 2023. – С. 117-120.
6. Букатов Д. Використання ШІ для персоналізації навчального процесу // Штучний інтелект у науці та освіті (AISE 2024). Artificial intelligence in science and education : збірник матеріалів міжнародної наукової конференції (Київ, 1-2 березня 2024 р.) [Електронний ресурс] / [упоряд: А. Яцишин, В. Матусевич, В. Коваленко]. – Київ : УкрІНТЕІ, 2024. – С. 37-39.

УДК 37.014.5:004.94

Григор'єва Т.І., кандидат технічних наук, доцент,
Міжнародний гуманітарний університет, місто Одеса
tig15090808@gmail.com
Ратько Л.А.
Міжнародний гуманітарний університет, місто Одеса
alimdul13011308@gmail.com

АНАЛІЗ ТА ПРОГНОЗУВАННЯ РОЗВИТКУ ДОШКІЛЬНОЇ ТА ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ У ЗАКЛАДАХ КОМУНАЛЬНОЇ ВЛАСНОСТІ ТЕРИТОРІАЛЬНОЇ ГРОМАДИ М. ОДЕСА

Анотація.*Аналіз та прогнозування розвитку дошкільної та загальної середньої освіти є дуже важливим для забезпечення розвитку сучасної освітньої системи. Показана можливість формування обґрунтованих прогнозів розвитку дошкільної та загальної середньої освіти за допомогою статистичного аналізу, економіко-математичних моделей, демографічного аналізу, експертних оцінок та системного аналізу, спрямованих на прийняття зважених управлінських рішень.*

В умовах сьогодення освіта, як царина, відзначається одним із ключових елементів, який впливає не тільки на інтелектуальний розвиток особистості, а й на її соціалізацію, визначення місця в суспільстві та, як наслідок, на її емоційний розвиток. У регіональному аспекті, освіта є також найпріоритетнішим з напрямів розвитку людини, оскільки забезпечує її безпосередній інтелектуальний розвиток та виховання. На думку провідного наукового співробітника відділу інновацій та стратегій розвитку освіти, кандидата

педагогічних наук, доцента Пузікова Д.О., освітньо-педагогічне прогнозування є одним з найпотужніших засобів обґрунтовування та визначення управлінських рішень, які є основою для розробки проєктів, програм та планів освітніх реформ на основі коротко-, середньо- й довгострокових освітніх прогнозів [1].

З метою забезпечення стабільного розвитку системи освіти для задоволення потреб територіальної громади міста Одеси, росту економіки, особистісного розвитку учнів та вихованців закладів освіти згідно з їх індивідуальними здібностями і потребами та забезпечення вирішення, на території міста Одеси, зокрема, проблеми розвитку системи дошкільної, загальної середньої освіти та моніторингу її якості, рішенням Одеської міської ради від 03.05.2023 №1144-VIII затверджено Міську цільову програму розвитку освіти в м. Одесі на 2023 – 2025 роки, на реалізацію якої з бюджету Одеської міської територіальної громади виділено 1 030 432 040 грн. В контексті Програми, прогнозування розвитку освіти передбачено пунктом 6, де серед очікуваних результатів та ефективності Програми є трансформація освітньої мережі та забезпечення закладів освіти педагогічними кадрами [2].

Про пріоритетність освітньої галузі в соціально-економічному розвитку міста Одеси свідчить і Розподіл видатків бюджету Одеської міської територіальної громади на 2024 рік, відповідно до якого на освіту в м. Одеса виділено 5 118 015 954 грн., що складає 37% від загальної кількості видатків бюджету Одеської міської територіальної громади у сумі 13 780 995 939 грн. Водночас, освітня субвенція з державного бюджету місцевим бюджетам (бюджету Одеської міської територіальної громади на 2024 рік)складає 1 840 964 200 грн. [3].

Для прогнозування розвитку загальної середньої та дошкільної освіти в роботі пропонується використання даних минулих років для виявлення тенденцій та закономірностей за допомогою статистичного аналізу. Для прогнозування фінансових та ресурсних потреб – застосування економіко-математичних моделей. Для аналізу поточного стану та прогнозування майбутніх змін дуже важливими є методи демографічного та системного аналізу.

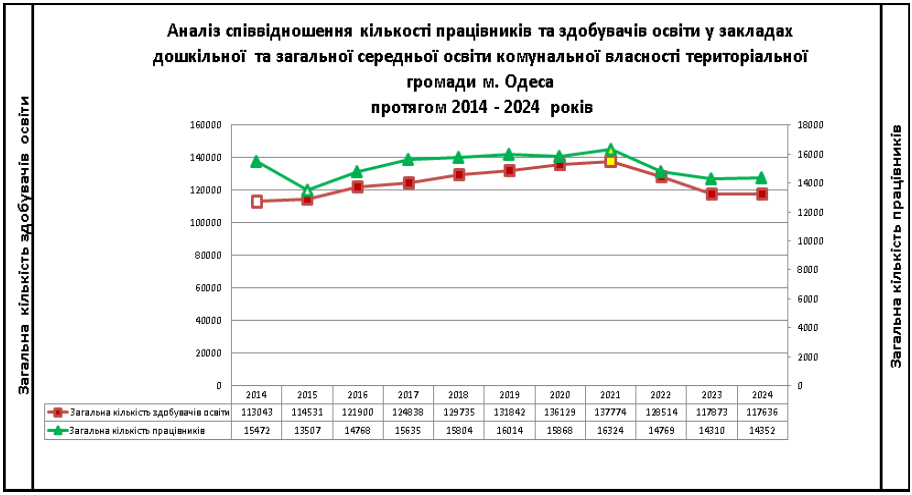
В результаті аналізу й прогнозування розвитку дошкільної та загальної середньої освіти, в роботі визначені ключові напрями, які потребують уваги:

1. Інвестиції в інфраструктуру - будівництво нових закладів освіти та модернізація існуючих.
2. Аналіз існуючих вакансій у закладах освіти - необхідність підготовки педагогічними вишами спеціалістів для роботи у закладах освіти м. Одеса.
3. Підвищення кваліфікації педагогічних працівників - забезпечення сучасними методиками та технологіями навчання.
4. Впровадження новітніх технологій - використання інформаційно-комунікаційних технологій для покращення якості освіти.
5. Забезпечення рівного доступу до освіти - створення умов для навчання дітей з особливими освітніми потребами.

Серед широкого інструментарію аналітичних методів, які застосовуються практиками, прогнозування переважно здійснюється за допомогою екстраполяційних методів [4].

Відповідно до статистичних даних, зображених на графіку, найбільшими значеннями крайніх вузлів екстраполяції є загальна кількість здобувачів освіти та працівників у закладах дошкільної та загальної середньої освіти комунальної власності територіальної громади м. Одеса в 2021 році (вузли виділено жовтим кольором), найменшими значеннями крайніх вузлів екстраполяції є загальна кількість здобувачів освіти у закладах дошкільної та загальної середньої освіти комунальної власності територіальної громади м. Одеса в 2014 році, а працівників закладів дошкільної та загальної середньої освіти комунальної власності територіальної громади м. Одеса в 2015 році (вузли виділено білим кольором).

Згідно зі статистичними даними, спостерігаємо стале пропорційне співвідношення кількості працівників до кількості здобувачів освіти закладів дошкільної та загальної середньої освіти комунальної власності територіальної громади м. Одеса протягом 10 років.



Доцільним є зауваження щодо наслідків суспільно-політичних подій в Україні: виникнення точок біфуркації на полі атракторів та їх вплив на утворення вузлів екстраполяції. Так, наприклад, Революціягідності на зламі 2013-2014 років та збройне, навесні 2014 року, вторгнення в Крим вплинули на показники кількості здобувачів освіти, працівників закладів дошкільної та загальної середньої освіти комунальної власності територіальної громади м. Одеса [5].

Незважаючи на те, що у закладах дошкільної та загальної середньої освіти комунальної власності територіальної громади м. Одеса, станом на 30.05.2024, загальна кількість здобувачів освіти, із числа внутрішньо переміщених осіб, складала 7160 осіб, на тлі збройної агресії російської федерації проти України 24.02.2022, спостерігаємо зменшення кількості здобувачів освіти та працівників закладів дошкільної та загальної середньої освіти комунальної власності територіальної громади м. Одеса. Відносно даних 2021 року (найбільші значення вузлів екстраполяції), у 2024 році спостерігаємо зменшення кількості здобувачів освіти на 15%, а працівників закладів дошкільної та загальної середньої освіти комунальної власності територіальної громади м. Одеса на 12%.

Таким чином, зміна суспільно-політичних чинників на рівні держави, знаходить своє відображення на ситуаційному положенні в м. Одеса. Збільшення або зменшення кількості учасників освітнього процесу може бути важелем для прийняття рішення щодо модернізації закладів освіти або їхнього будівництва, що в свою чергу вплине на Розподіл видатків бюджету Одеської міської територіальної громади на освіту.

Висновки

1. Аналіз та прогнозування розвитку дошкільної та загальної середньої освіти є важливим завданням для забезпечення сталого розвитку освітньої системи.

2. Впровадження сучасних методик та технологій, підвищення кваліфікації педагогів та інвестиції в інфраструктуру сприятимуть підвищенню якості освіти та формуванню компетентних громадян, здатних відповідати на виклики сучасного світу.

3. Методи прогнозування розвитку загальної середньої освіти дозволяють комплексно оцінити стан та перспективи освітньої системи, виявити проблеми та розробити ефективні стратегії для їх вирішення. Використання різноманітних методів, таких як статистичний аналіз, економіко-математичні моделі, демографічний аналіз, експертні оцінки та системний аналіз, сприяє формуванню обґрунтованих прогнозів та прийняттю зважених управлінських рішень у освітній галузі.

Література

1. Пузіков Д.О. Теоретична модель прогнозування розвитку загальної середньої освіти// Український педагогічний журнал. – 2016. – № 4. – С. 128–137.

2. Про затвердження Міської цільової програми розвитку освіти в м. Одесі на 2023 – 2025 роки: рішення Одеської міської ради від 03.05.2023 № 1144-VIII – С. 4, 15-16. URL: https://omr.gov.ua/ua/acts/council/197681.

3. Про внесення змін до рішення Одеської міської ради від 29.11.2023 № 1618-VIII «Про бюджет Одеської міської територіальної громади на 2024 рік»: рішення Одеської міської ради від 22.05.2024 №2186-VIII URL: https://omr.gov.ua/ru/acts/council/204266.

4. Василь А. Пігош. Аналіз та прогнозування діяльності вищих навчальних закладів за допомогою методів інтерполяції та екстраполяції.//Актуальні проблеми економіки №2(152), 2014. С 529-538.

5. Котляр Ю. Революція гідності: вибір європейського майбутнього /Ю. Котляр, О. Мосін// Acta de Historia & Politica: Saeculum XXI. – 2024. – Vol. VII. – P. 47–56. – Bibliogr. at the end of the art. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/2024

УДК 372.851.9

Горбачов В. Е., к.т.н., доцент
Морозов М. В., студент V курсу
Міжнародний гуманітарний університет
Горбачов П. В., учень I курсу
Фаховий коледж НТІІС
physmgu@gmail.com

ВИКОРИСТАННЯ МЕТОДИКИ АДАПТИВНОГО НАВЧАННЯ РОБОТИ З ОПЕРАЦІЙНИМИ СИСТЕМАМИ

Анотація. *У роботі розглядаються особливості використання методики адаптивного навчання роботи з операційними системами. Сформовано таку структуру курсу вивчення процесу встановлення ОС на базі ядра Linux при якій студент у процесі навчання може вибрати індивідуально сплановану послідовність блоків знань та навчальних завдань, що відповідає його можливостям та здібностям. Як показує практика, учні з ентузіазмом сприймають таку організацію навчального процесу через ясність поставленої мети та можливість самому приймати рішення про вибір складності шляху досягнення цієї мети.*

Наразі неможливо уявити діяльність будь-якої людини від школяра до вченого без використання комп'ютера. Основним програмним продуктом у комп'ютері є операційна система (ОС), без якої комп'ютер називають «цеглою». В даний час монопольне становище корпорації Microsoft на ринку операційних систем призвело до постійного вибивання грошей із користувачів. Вартість ліцензії базового комплекту Windows складає 7900 грн. та вимагає покупки додатків, які необхідні для конкретних потреб користувача.

Лише підписка Microsoft Office коштує додатково 1900 грн. на рік. Крім того, разом з ОС Windows автоматично завантажуються вбудовані різні брадмауери, оркестратори, фаєрволли, служби збору телеметрії, а також спонсорські програми незалежно від Вашого бажання. Періодично Microsoft оголошує про припинення підтримки попередньої версії ОС Windows, змушуючи користувачів часто змінювати комп'ютер у зв'язку з підвищеними вимогами нової версії ОС. У зв'язку з цим використання альтернативних операційних систем, які позбавлені цих недоліків є актуальним вирішенням проблеми.

Тим більше, що така можливість існує: вже більше 30 років широко використовуються і постійно вдосконалюються операційні системи на базі ядра Linux з відкритим вихідним кодом. Ці ОС, на відміну від Windows, є абсолютно безкоштовними та загальнодоступними, оскільки розробляються та тестуються спільнотою ентузіастів для потреб користувачів. Вже створені цілі репозиторії з пакетами різноманітних службових програм та додатків під різні завдання та сценарії використання. Але головна перевага ОС на базі ядра Linux полягає в можливості вибору конфігурації системи, оскільки тільки сам користувач вирішує які програми встановлювати і використовувати, і жодна програма не може бути встановлена або запущена без команди користувача. Крім того, в репозиторії розміщуються лише перевірені пакети програм, тому така ОС не вимагає антивірусів та фаєрволів, що значно економить час обробки даних та ресурси. Цим же пояснюються низькі системні вимоги до процесора, оперативної пам'яті та накопичувача комп'ютера під час встановлення ОС на базі ядра Linux. Незважаючи на всі ці переваги, широке використання альтернативних ОС обмежується непоінформованістю користувачів у цій сфері та побоюваннями про складність процесу встановлення.

Метою даної роботи є використання методики адаптивного навчання роботі з операційними системами на базі ядра Linux для кращого розуміння та засвоєння матеріалу, що вивчається різними категоріями користувачів.

Результати сучасних дослідників у галузі підвищення доступності знань при постійно збільшенні їх обсягу свідчать про те, що найбільш ефективним засобом вирішення цієї проблеми є використання технологічної педагогічної системи адаптивного навчання [1]. Ця система передбачає використання низки методик, які дозволяють створити для учнів адаптивне освітнє середовище, в якому кожен учень отримує знання, що відповідають його можливостям та здібностям [2]. Система адаптивного навчання, як і всі педагогічні методи, перебуває у стані постійного вивчення та вдосконалення, тому немає суворого протоколу виконання вимог, а пропонуються лише деякі методики, які слід використовувати в залежності від конкретного випадку [2].

По-перше, це структуризація навчального матеріалу, виділення послідовних самостійних частин курсу, кожна з котрих має бути логічно закінчена та представляти самостійний елемент.

По-друге, це диференціація навчального матеріалу за рівнями складності його сприйняття, виділення найпростіших елементів курсу, прикладних та творчих.

По-третє, повторення пройденого матеріалу.

По-четверте, наявність такої системи контролю за успішністю при якій не тільки викладач, а й сам учень міг би оцінити свій рівень засвоєння матеріалу.

Як зазначено в роботі [3] основна мета – це побудова такої послідовності курсу навчання, при якій суб'єкт навчання буде забезпечений індивідуально спланованою послідовністю блоків знань та навчальних завдань для забезпечення його компетенцій (технологія навчального планування).

У цієї роботі вивчається можливість застосування перерахованих вище методик адаптивного навчання для курсу вивчення процесу установки ОС з урахуванням ядра Linux.

По-перше, процес установки ОС з урахуванням ядра Linux можна як наступної послідовності самостійних елементів процесу: створення завантажувального носія, розмітка дискового простору, установка ядра і службових програм, установка графічної

оболонки інтерфейсу, установка додатків. Структурно-логічна схема послідовності навчальних елементів процесу встановлення ОС з урахуванням ядра Linux показано на рис. 1.

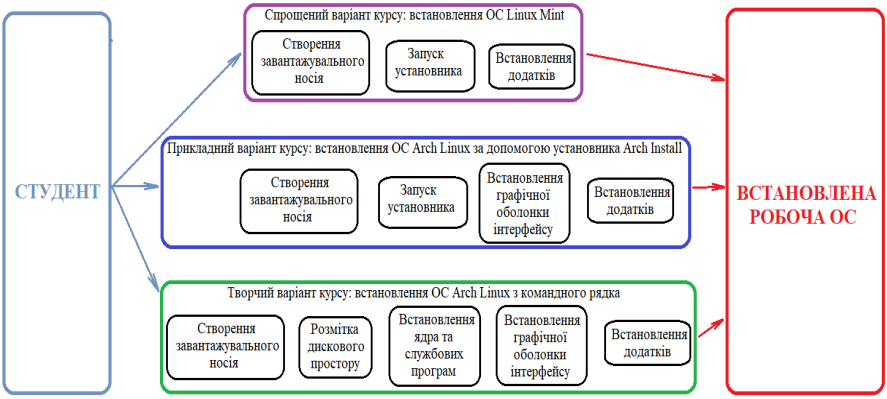


Рисунок 1 – Структурно-логічна схема послідовності навчальних елементів процесу встановлення ОС з урахуванням ядра Linux

З рисунка видно, що кожен із елементів є логічно закінченим і представляє самостійний елемент у процесі установки.

По-друге, існує можливість диференціації навчального матеріалу за рівнями складності сприйняття: в якості спрощеного варіанту установки ОС пропонується встановити ОС Linux Mint, інтерфейс якої практично є копією інтерфейсу Windows, а процес установки є спрощеним варіантом установки ОС Windows, і зводиться до відповідей на запитання установника. Однак, при своїй простоті такий варіант дозволяє досягти мети – установки робочої ОС на комп'ютер. В якості прикладного варіанту установки ОС пропонується встановити ОС Arch Linux за допомогою установника Arch Install, який запускається з командного рядка і вимагає певних знань для встановлення числових значень параметрів установки. При такому варіанті встановлюються стандартні службові програми відповідно до конфігурації комп'ютера. І, нарешті, в якості творчого варіанту установки ОС пропонується встановити Arch Linux повністю з командного рядка. При такому варіанті установки ОС користувач повністю управляє процесом і сам вибирає ті службові програми, які найкраще підходять до конфігурації комп'ютера.

По-третє, повторення та закріплення пройденого на занятті матеріалу пропонується організувати за допомогою лекційного тестового опитування, при виконанні якого дозволяється користуватися конспектом. Це стимулює учня переглянути та зафіксувати у пам'яті основні моменти заняття.

По-четверте, результати проведеного лекційного тестового опитування мають бути доступні студентам на цьому ж занятті. Це дозволить кожному учневі самому оцінити свій рівень засвоєння матеріалу та ухвалити рішення про вибір рівня складності навчання на наступних заняттях.

Таким чином, сформовано таку структуру курсу вивчення процесу встановлення ОС на базі ядра Linux при якій студент у процесі навчання може вибрати індивідуально сплановану послідовність блоків знань та навчальних завдань, що відповідає його можливостям та здібностям.

Як показує практика, учні з ентузіазмом сприймають таку організацію навчального процесу через ясність поставленої мети та можливість самому приймати рішення про вибір складності шляху досягнення цієї мети.

Література

1. Носенко Ю.Г. Адаптивні системи навчання: сутність, характеристика, стан використання у вітчизняних закладах педагогічної освіти / Ю.Г. Носенко // Фізико-математична освіта. – 2018. – В. 3(17). – С. 73-78.

2. Пішванова В.О. Принципи адаптивного навчання / В.О. Пішванова // Вісник Запорізького національного університету. Педагогічні науки. – 2015. – № 1(24). – С. 178-183.

3. Мінцер О.П. Обрії розвитку адаптивного навчання / О.П. Мінцер // Медична інформатика та інженерія. – 2017. – № 1. – С.5-11.

УДК

Горбаньова В. О.,
старший викладач кафедри менеджменту
Міжнародного гуманітарного університету,
vik.gorbanyova@gmail.com

ТЕНДЕНЦІЇ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В ОСВІТИ

Анотація. *Цифрова трансформація впевнено охопила всі сфери, зокрема й сферу надання освітніх послуг. Впровадження цифрових технологій в умовах Індустрії 4.0 розкриває нові можливості та перспективи як надання послуг освіти, так і управління цим процесом. Навчальні заклади проєктують створення сучасного електронного інформаційно-освітнього середовища, впровадження технологій онлайн-навчання, розвиток практики використання наскрізних технологій, просування цифрових сервісів, розвиток моделі «цифрового університету». В умовах глобалізації змінюється роль педагога, рівень його цифрової грамотності, наголошується на важливості та перспективності діяльності з впровадження цифрових технологій в інститут освіти.*

Ключові слова: *цифрова трансформація бізнесу, цифрові технології, інформаційні технології, підвищення конкурентоспроможності, цифровізація, діджиталізація, управління у сфері освіти, цифровий сервіс,онлайн платформи, тенденції цифрової трансформації, ринок онлайн-освіти, Індустрія 4.0, електронне інформаційно-освітнє середовище, онлайн-навчання, наскрізні технології, цифровий університет.*

Актуальність проблеми. Домінуючою тенденцієюреформування інституту освіти за умов глобалізації виступила цифровізація як напрямок стратегічної концепції цифрової освіти майбутнього «Touch освіта» [4] . Сутність зазначеної стратегічної концепції полягає у процесі інтеграції цифрових технологій до навчального процесу навчальних закладів усіх рівнів: від шкіл до університетів. Призначення цифрових технологій полягає у допомозі учням у підвищенні їхньої компетентності, розвитку логічного мислення та навичок спілкування в новому комунікативному середовищі.

В останні роки пандемія та запровадження військового стану в Україні значно прискорила перехід на дистанційні освітні моделі як можливі шляхи отримання знань, а digital-середовище зайняло гідне місце в організації навчання для всіх категорій споживачів освітніх послуг незалежно від віку, місця перебування та професійних та особистих інтересів [3].

Впровадження цифрових сервісів у навчальний процес регламентується проєктом Стратегії цифрової трансформації освіти та науки, яка спрямована на: створення цифрового освітнього середовища, цифрові компетентності та сучасний зміст освіти.

Докорінні цифрові зміни передбачені концепцією дозволять створити єдину освітню екосистему [5].

Освіта належить до тієї сфери, де не можна ігнорувати розвиток та враховувати прогресивні технології. На ринку постійно з'являються нові технології навчання, що насичують навчальний процес, роблячи його ефективнішим. Тому цілком очевидно, що конкурентоспроможнішими на сучасному ринку освітніх послуг є саме ті навчальні заклади, які можуть ергономічно інтегрувати інструменти як традиційної, так і онлайн-освіти. Під цифровізацією розуміється: дифузія наскрізних цифрових технологій у бізнес-процеси, процеси життя суспільства; процес, спрямований як створення цифрових копій світових ресурсів, та формування мережевих платформ взаємодії, з метою отримання прогнозованого і гарантованого результату будь-якого управляючого впливу [1]. Особливістю сучасного етапу цифровізації освіти є занурення всіх його суб'єктів у цифрове освітнє середовище [2,3].

Основними тенденціями цифровізації освіти є:

1. Електронне навчання: онлайн-навчання, мікронавчання (microlearning), активне використання елементів відеолекцій, можливість моделювання навчальних занять з елементами ігрових технік (гейміфікація), кросплатформеність (дозволяє Веб-сайту читати на будь-якому пристрої (стаціонарному комп'ютері, ноутбуку, планшеті) т.д.), застосування хмарних сервісів Google Drive, Google.Диск та ін.) для розміщення великого пласта інформації по навчальних онлайн-курсах, застосування з навчальними цілями онлайн-платформ із спільним доступом (Zoom, Teams та ін.) ; використання у навчальному процесі мультимедіа, онлайн-платформ, веб-ресурсів, хмарних сервісів, електронних бібліотек та ін. Передбачається, що зростання сегменту онлайн навчання буде збільшуватися щороку.
2. Розвиток практики використання штучного інтелекту (ШІ), як ресурсу, який буде доповнювати традиційне навчання (чат-ботів та ін.), віртуальної реальності (VR), технології зберігання даних блокчейн (централізоване зберігання електронних портфоліо, атестатів, дипломів, особових справ учнів), великих даних (Big Data) (дозволяють відстежити частоту роботи учня з фондом бібліотеки, інформацію про курси, що вивчаються, відвідуваність та ін), роботехніки (альтернатива заміни педагогів).
3. Створення електронних освітніх середовищ у навчальних закладах, що дозволяють ефективно та оперативно організовувати навчальний процес, взаємодію всередині структурних підрозділів навчального закладу, здійснювати комунікування між суб'єктами освіти та батьками.
4. Просування низки цифрових сервісів. Наприклад,сервіс «Цифрове портфоліо учня» за згодою батьків фіксуватиме освітню траєкторію та всі досягнення учня. За даними сервісу, можна буде сформувати пакет документів для вступу до закладу вищої освіти або коледжу. Сервіс «Цифровий помічник батьків» стане каналом взаємодії школи та батьків, забезпечуючи обмін миттєвими повідомленнями з учителями. Сервіс «Електронний портфель» включатиме всі матеріали для навчання у цифровому форматі.
5. Модель «цифрового університету», що представляє технічну інфраструктуру навчального закладу (бездротовий доступ, комп'ютерне обладнання, мобільні пристрої для доступу до цифрових ресурсів, системи контролю та управління, доступ до установи з цифрових карток, можливість розрахунку та грошових операцій з карток тощо).

У цьому контексті серйозним викликом для навчальних закладів є зміна ролі педагога як транслятора ідей державної освітньої політики, який повинен відповідати викликам цифрової економіки, а саме – демонструвати цифрову культуру та цифрову грамотність з метою максимального використання можливостей цифрового середовища у навчально-виховній діяльності, коректно вибудовувати траєкторію освітнього сегменту на основі відкритих цифрових джерел, застосовувати технології змішаного навчання [8,9].

Стратегічний розвиток в галузі цифрової трансформації науки та вищої освіти регламентується Міністерством освіти і науки України та Міністерством та Комітетом цифрової трансформації України [6,7]. Загальними завданнями цифровізації освіти є:

1) формування цифрової грамотності педагогічних працівників щодо використання цифрових технологій в освітній діяльності;
2) застосування цифрових технологій у освітньому процесі;
3) надання для колективного користування цифрових ресурсів та доступу до них у хмарних ресурсах;
4) підвищення рівня мотивації до застосування цифрових технологій;
5) накопичення, систематизація та розповсюдження інформації щодо використання цифрових та хмарних технологій у навчальному закладі.

Висновки. На підставіпроведеного дослідження можна сформулювати такі висновки:

Цифровий сервіс став потужним інструментом розвитку інституту освіти [10,11].

Основними тенденціями цифровізації освіти виступають: онлайн-навчання, мобільне навчання, штучний інтелект, пристрої AR та VR, великі дані та ін.

Цифрові освітні технології дозволяють в оперативному режимі поширювати та обмінюватися новими та інтерактивними методами як між співробітниками всередині навчального закладу, так і між навчальними закладами, між педагогами та навчальними закладами, педагогами та батьками, що в сучасних умовах є одним із найважливіших факторів конкурентоспроможності навчального закладу.

Цифрові ресурси розглядаються у світі як перспективний орієнтир модернізації інституту освіти. Цифровий сервіс має такі переваги перед традиційною освітою: високу наочність, інтерактивні інструменти, можливість реалістичного відтворення ситуацій із життя, спрощеного моделювання складних метапредметних концепцій; можливість комунікацій учасників освітнього процесу з будь-якої точки світу за наявності доступу до Інтернету; розширення інформаційних кордонів здобувачів освіти.

Отже, цифрові ресурси дають якісний стрибок у розвитку освітньої діяльності.

Список літератури

1. European Commission. Digital Education Action Plan (2021-2027). URL:
2. https://www.csreurope.org/calendar/eu-masterclass-value-chain-transparency-traceability-in-the-deforestation-and-forced-labour-regulations?gad_source=1&gclid=Cj0KCQjws560BhCuARIsAHMqE0G1G7ZGO9trZaiHjWWLIVual8aAqZ_EALw_wcB
3. Біків. В. Цифровізація освіти – імператив інтеграції України у світовий інформаційний простір. Освіта та суспільство. 2022. №10. С. 6. URL: https://naps.gov.ua/ua/press/about_us/2936/
4. Духаніна Н. М., Лесик Г. В. Цифровізація освітнього процесу: проблеми та перспективи. International scientific and practical conference «Modern directions of scientific research development» (May 18-20, 2022), Chicago, USA. Chicago: BoScience Publisher, 2022. P. 406-409. URL: https://ela.kpi.ua/items/790a4aed-f4bf-42dd-8691-8e580e0e8e5d
5. Ілляшенко З. М. , Шипуліна Ю. С. , Ілляшенко Н. З. Цифрова трансформація освітньої діяльності закладів вищої освіти України в умовах війни . Вища освіта за новими стандартами: визови в контексті діджіталізації та інтеграції у міжнародний освітній простір : зб. матеріалів Міжнар. наук.-метод. конф., 10.05.2022. Харків, 2022. С. 7–10. URL: https://dspace2.khadi.kharkov.ua/handle/123456789/5560
6. Кабінет Міністрів України - Артур Селецький: Проект Стратегії цифрової трансформації освіти та науки напрямів створення єдиної екосистеми. ShieldSquare Captcha. URL: https://www.kmu.gov.ua/news/arturseleckij-proyekt-strategiyi-cifrovoyi-transformaciyi-osviti-i-nauki-napravlenij-nastvorennya-yedinoyi-ekosistemi

7. Міністерство освіти і науки України - Цифрова трансформація освіти та науки. Головна | Міністерство освіти і науки України. URL: https://mon.gov.ua/ua/tag/cifrova-transformaciya-osviti-ta-nauki

8. Міністерство та Комітет цифрової трансформації України: вебсайт. URL : https :// thedigital . gov . ua / committees .

9. Опис рамки цифрової компетентності для громадян України. Міністерство цифрової трансформації України. 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20 %D0%A6%D0%9A.pd

10. Про затвердження Концептуальних засідок розвитку педагогічної освіти в Україні та її інтеграції в європейський освітній простір : Наказ МОН від 31.12.2004р . № 988. URL: http://osvita.ua/legislation/Vishya_osvita/3145/

11. Універсальний освітній простір ACCENT : офіційний вебпортал. URL: http://ac-cent.com .

12. Університет менеджменту освіти - Університет менеджменту освіти. URL: http://umo.edu.ua/images/content/document/koncthciya_cifroviz.pdf

УДК 608.4

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Салабай Михайло Олександрович
здобувач 2 курсу першого (бакалаврського) рівня
спеціальності 121 – Інженерія програмного забезпечення
Міжнародний гуманітарний університет

УКРАЇНСЬКИЙ НАУКОВО-ТЕХНІЧНИЙ ПОРТАЛ «UKRAINIAN DEVELOPMENT HUB»

Анотація. *Метою роботи є опис стартапу українського науково-технічного порталу «Ukrainian Development Hub», представленого на конкурсі «Відновлення через соціальне підприємництво», організованого громадською організацією «Джуніор Ачівмент Україна» в межах міжнародного проєкту EU4Youth «Building Back Better Through Social Entrepreneurship». Проєкт реалізований у вигляді інтернет-порталу, призначеного для обміну інформацією між фахівцями українських та закордонних компаній, викладачами, здобувачами та учнями, що працюють в галузях інформаційних технологій, електроніки, робототехніки, штучного інтелекту та інших суміжних галузях.*

В Україні, як і в інших технічно-розвинених країнах світу, постійно існує потреба в обміні актуальними знаннями між здобувачами, викладачами та фахівцями у різних сферах наукової та практичної діяльності, у тому числі і в сфері інформаційних технологій. Однак україномовних публічних освітніх платформ наразі обмаль. Ця ситуація призводить до того, що молодь не має доступу до сучасних, якісних і локалізованих навчальних матеріалів, що стримує їхній професійний розвиток і знижує конкурентоспроможність на міжнародному рівні. Крім того, відсутність сучасних точок обміну інформацією ускладнює співпрацю між навчальними закладами та бізнесом, що обмежує можливості для стажувань, практичної підготовки та працевлаштування.

Для вирішення цієї проблеми було запропоновано створення українського науково-технічного порталу «Ukrainian Development Hub» (UDH) (рис. 1), проєкт якого було представлено на конкурсі стартапів «Відновлення через соціальне підприємництво», організовано ГО «Джуніор Ачівмент Україна» в межах міжнародного проєкту EU4Youth «Building Back Better Through Social Entrepreneurship» [1 – 4]. Основу команди, що займалась проєктом UDH, склали здобувачі Міжнародного гуманітарного університету:

- Салабай Михайло, спеціальність 121 – Інженерія програмного забезпечення;
- Макаров Павло, спеціальність 123 – Комп'ютерна інженерія;
- Абрамцова Катерина, спеціальність 123 – Комп'ютерна інженерія;
- Ніколаев Микола, спеціальність 122 - Комп'ютерні науки;
- Візнюк Георгий, спеціальність 121 – Інженерія програмного забезпечення;
- Светлов Владислав, спеціальність 123 – Комп'ютерна інженерія.

Місією порталу UDH полягала у сприянні підвищенню рівня грамотності технічних фахівців у сучасній Україні шляхом діджиталізації та забезпечення зручного доступу до високоякісних матеріалів державною мовою. Портал UDH планувався як платформа, що об'єднає здобувачів, викладачів та фахівців, забезпечуючи їм можливість обмінюватися знаннями, досвідом та ідеями. Мета проєкту – надати доступ до сучасних навчальних ресурсів, які допоможуть у розвитку професійних навичок та сприятимуть інноваціям у різних технічних галузях.

Головною цільовою аудиторією проєкту UDH стали три групи користувачів, які отримали умовні назви: «Здобувачі», «Викладачі» та «Компанії». Найважливішою ознакою цих груп є зацікавленість у новітніх технологіях, прагнення до саморозвитку та самореалізації.

Здобувачі. У цю категорію потрапляють учні, здобувачі передвищої та вищої освіти та молоді фахівці, які прагнуть підвищити свої знання та навички у сферах інформаційних технологій, електроніки, робототехніки, штучного інтелекту та інших суміжних галузях. Для них портал пропонує можливість зручно та швидко отримувати найактуальніші знання з першоджерел, що дозволить їм бути в курсі останніх тенденцій і технологічних новинок.

Викладачі. У цю категорію потрапляють освітяни, науковці та тренери, які бажають ділитися своїми напрацюваннями та використовувати напрацювання інших для підвищення якості навчального процесу. Портал надасть їм можливість публікувати свої дослідження, навчальні матеріали та обмінюватися досвідом з колегами, що сприятиме створенню активної освітньої спільноти.

Компанії. У цю категорію потрапляють українські та закордонні компанії, які працюють у сфері високих технологій і зацікавлені у залученні талановитих фахівців та підвищенні рівня знань своїх співробітників. Для них портал пропонує можливість залучати здобувачів до вивчення саме їх продуктів, навчати їх, як працювати з цими продуктами, та сприяти потенційному працевлаштуванню в компанії. Таким чином, компанії можуть створювати власні навчальні програми та тренінги, залучаючи майбутніх співробітників ще на етапі навчання.

У участі у конкурсі команда проєкту створила прототипи основних сторінок: головної сторінки (рис. 1), сторінки для розміщення переліку статей, сторінки для розміщення текстів статей та деяких допоміжних технічних сторінок (сторінку автентифікації тощо). Крім того наразі вже визначено основний функціонал бізнес-логіки, що дозволило чітко уявити як буде виглядати і працювати платформа на кожному етапі її розробки та впровадження.

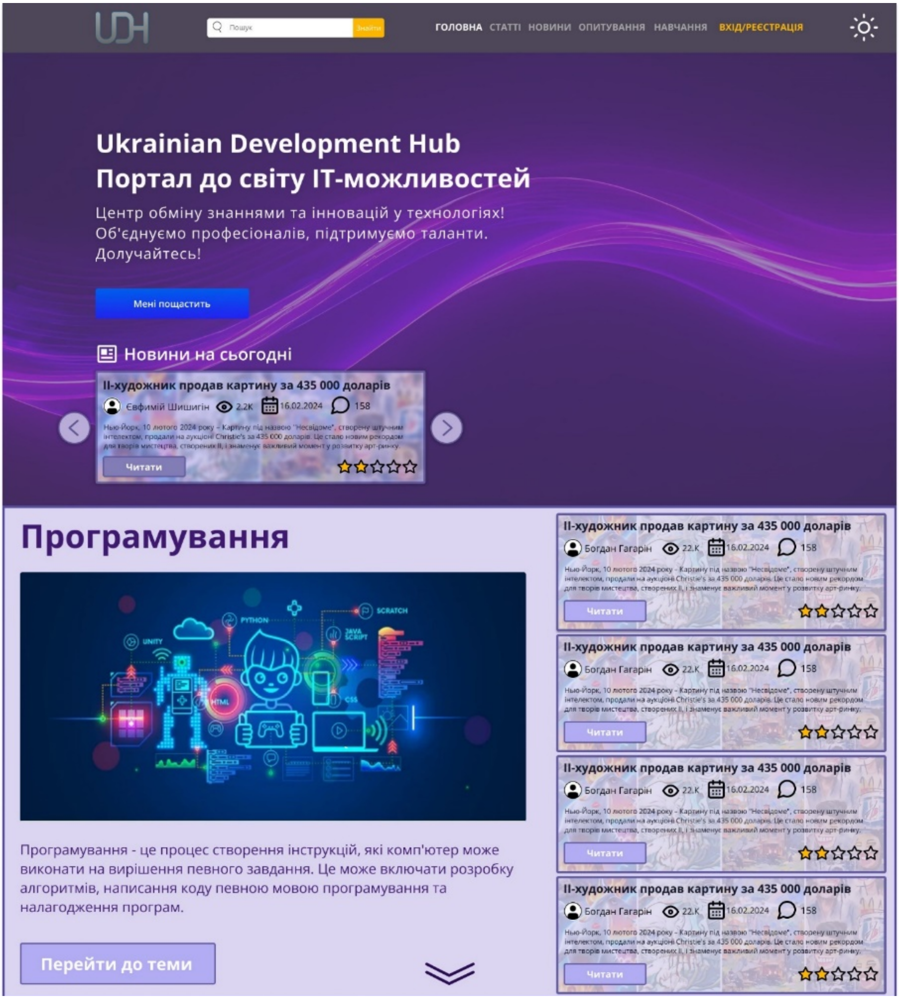


Рисунок 1 – Проєкт головної сторінки порталу UDH

Головним форматом поширення інформації на порталі було обрано статті. Цей формат забезпечує користувачам можливість швидко та цікаво отримувати необхідну інформацію навіть під час короткої перерви на каву. Передбачається, що статті будуть невеликі за обсягом, що дозволяє читачам ефективно використовувати свій час. Кожна стаття зосереджена на конкретній темі, дозволяючи глибоко зануритися в актуальні питання без потреби вичитувати декілька томів книжок. Тематика статей ретельно підбирається, враховуючи найсучасніші тенденції та виклики в галузях інформаційних технологій, електроніки, робототехніки, штучного інтелекту та інших суміжних сферах. Таким чином, користувачі порталу завжди будуть залишатися в курсі новітніх розробок та інновацій.

Висновки

Наведено опис стартапу українського науково-технічного порталу «Ukrainian Development Hub», який може стати важливою умовою для становлення України як незалежної технічно-розвиненої держави. Показано, що поява проєктів подібних «Ukrainian Development Hub» є обґрунтованою, актуальною, і в повній мірі відповідає потребам українського сьогодення. Наразі портал «Ukrainian Development Hub» знаходиться у стані проєкту, але його команда відкрита для будь-якої форми співпраці, і не втрачає надію на практичну реалізаціє свого замислу.

Література

1. Тренінг «Особливості впровадження та викладання курсу з підприємництва». URL: https://mgu.edu.ua/tpost/bar11nkvo1-trenng-osoblivost-vprovadzhennya-ta-vikl

2. Тренінг «Табір підприємництва», в рамках проєкту «Відновлення через соціальне підприємництво». URL: https://mgu.edu.ua/tpost/1jfsv9f4e1-trenng-tabr-pdprimnitstva-v-ramkah-prokt

3. Тренінг «Табір підприємництва». URL: https://mgu.edu.ua/tpost/eudka4s0s1-trenng-tabr-pdprimnitstva

4. Півфінал проєкту «Відновлення через соціальне підприємництво». URL: https://mgu.edu.ua/tpost/sbpo2b3dn1-6-chervnya-2024-roku-komanda-udh-do-skla

УДК 372.862, 519.876.5

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Бучацький Володимир Володимирович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 014 Середня освіта
Міжнародний гуманітарний університет
buchvova1983@gmail.com

МЕТОД НАВЧАННЯ ПРОГРАМУВАННЮ МІКРОКОНТРОЛЕРІВ ПРИ ДИСТАНЦІЙНІЙ ФОРМІ НАВЧАННЯ

Анотація. *Розглянуто метод навчання програмуванню мікроконтролерів здобувачів, що навчаються за дистанційною формою навчання. Наведено стислий опис спеціалізованої віртуальної лабораторії, яка була створена авторами статті для вирішення цієї задачі. Результати практичного впровадження створеної віртуальної лабораторії показують, що наявність спеціалізованих віртуальних макетів дозволяє обійтися без фізичного моделювання та використання реальних контрольно-вимірювальних приладів. При цьому код, написаний для мікроконтролера, що працює у віртуальному тестовому середовищі, може нічим не відрізнятися від коду, призначеному для роботи у реальній схемі.*

Мікроконтролери є головними компонентами самих різноманітних електронних пристроїв та систем, починаючи від дитячих іграшок та побутової техніки і закінчуючи застосунками, які зараз мають помітку «Hi-Tech»: системами типу «Розумний будинок», пристроями Інтернету речей, роботами, дронами та іншими автоматизованими системами [1, 2]. Тому не дивно, що фахівці, які розуміються на програмуванні мікроконтролерів, користуються стабільним попитом як українському, так і на закордонних ринках праці.

Однак на відміну від інших напрямків програмування, наприклад, програмування інтерфейсів або баз даних, для яких достатньо лише наявності комп'ютера, програмування мікроконтролерів має певну специфіку. Річ у тому, що мікроконтролер фактично є повноцінним мікрокомп'ютером, фізично реалізованим у вигляді мікросхеми. Програмне забезпечення мікроконтролерів завжди працює у реальному часі із реальними пристроями та сигналами. Тому для того, щоб перевірити правильність написання програми для мікроконтролера потрібно мати схему, в якій він повинен далі працювати. Крім того, для перевірки та налагодження програмного забезпечення для мікроконтролерів інколи потрібно мати цілий комплекс вимірювальних приладів, таких як мультиметри, осцилографи, аналізатори логічних сигналів тощо.

При очній формі навчання для практичного вивчення дисциплін, пов'язаних із програмуванням мікроконтролерів, створюють спеціалізовані аудиторії (лабораторії), облаштовані необхідним обладнанням. При такому підході здобувачі на початку практичного заняття вже мають заздалегідь зібрану схему (макет) та набір усіх необхідних контрольно-вимірювальних приладів, і їм фактично залишається лише написати програмне забезпечення для мікроконтролера та випробувати його в реальній схемі. Однак при дистанційній формі навчання, коли здобувач не має фізичного доступу до спеціалізованих лабораторій, повноцінна перевірка правильності роботи програмного забезпечення для мікроконтролера у більшості випадків виявляється або дуже утрудненою, або зовсім неможливою, що істотно знижує якість підготовки здобувачів.

У статті розглянуто методи організації навчання програмуванню мікроконтролерів при дистанційній формі навчання, які використовуються на факультеті кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету. Для забезпечення можливості правильності написання програмного забезпечення для мікроконтролерів в рамках проєкту «Віртуальна лабораторія» [3, 4] було створено комплекс віртуальних лабораторних макетів, які дозволяють створювати та налаштовувати програмне забезпечення для мікроконтролерів на віртуальних схемах.

Зовнішній вигляд одного з лабораторних макетів, призначеного для опанування динамічної індикації та принципами керування матричними світлодіодними індикаторами, показано на рис. 1. Головним елементом макету є мікроконтролер DD1 (PIC16F84A), який керує матричним світлодіодним індикатором DD2 із розрядністю 5x8 (5 стовпчиків, 8 рядків).

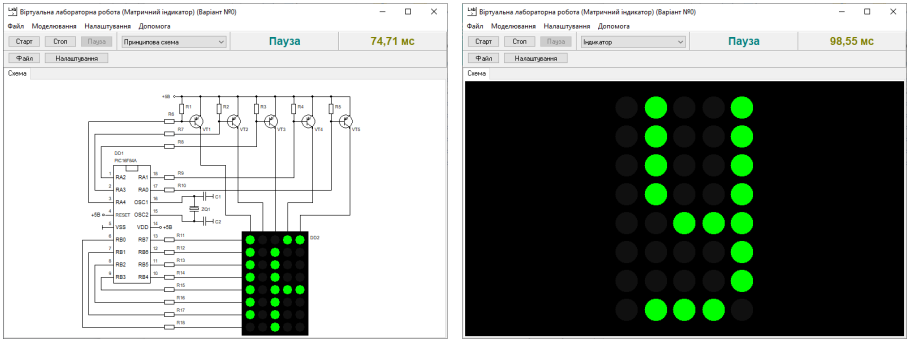


Рисунок 1 – Зовнішній вигляд лабораторного макета для керування матричним індикатором

Практичне завдання полягає у написані програми для мікроконтролера яка б на цьому індикаторі у форматі «рядок, що біжить» відобразила прізвище здобувача. В процесі виконання цього практичного завдання здобувач створює програмне забезпечення

для мікроконтролера, наприклад, в спеціалізованому інтегрованому середовищі MPLAB X [5], і наочно перевіряє його працездатність у віртуальному лабораторному макеті.

Схема підключення мікроконтролера до індикатора залежить від номеру варіанту, таким чином, кожен здобувач працює із власною схемою і програмне забезпечення створене для одного варіанту вже не буде працювати на макеті з іншими налаштуваннями. Це повністю виключає можливість повторення програмного забезпечення у різних здобувачів.

Наразі до переліку лабораторних макетів, що використовуються для навчання програмування мікроконтролерів, входять наступні:

– світлодіодна лінійка (первинне знайомство мікроконтролерами);

– однорозрядний семисегментний світлодіодний індикатор (опанування базових методів програмування мікроконтролерів);

– багаторозрядний семисегментний світлодіодний індикатор (робота з потужним навантаженям, динамічна індикація);

– матричний світлодіодний індикатор (робота з потужним навантаженням, динамічна індикація);

– світлофор (атестаційне заняття).

Як видно з наведеного переліку, наявний набір віртуальних лабораторних макетів дозволяє сформувати у здобувачів первинне уявлення про те, що таке мікроконтролери, а також яким чином за їх допомогою можна керувати типовими електронними пристроями (одиничними, сегментними та матричними світлодіодними індикаторами, тощо). Перелік лабораторних макетів постійно розширюється. В найближчому майбутньому до нього планується додати лабораторні макети для керування колекторними та безколекторними двигунами, кроковими двигунами, сервоприводами та іншими вузлами та пристроями.

Головними перевагами створених лабораторних макетів є:

– відсутність потреби у створенні фізичних макетів та реальних вимірювальних приладів для перевірки працездатності розробленого програмного забезпечення;

– можливість використання створених лабораторних макетів як при дистанційній, так і при очній формах навчання;

– можливість навчання іноземних студентів, оскільки створені лабораторні макети підтримують кілька мов інтерфейсу.

Додатковою перевагою створених віртуальних лабораторних макетів, на відміну від симуляторів загального призначення, таких як Proteus [6], є фокусування на конкретній практичній задачі. Під час створення програмного забезпечення здобувач опановує не тільки тонкощі програмування мікроконтролерів (особливості роботи з ядром, оперативною пам’яттю, периферійними пристроями тощо), а ще й особливості керування реальними застосунками (різними видами світлодіодних індикаторів, приводами, двигунами) та обробки реальних сигналів.

Створені віртуальні лабораторні макети разом із методичними вказівками до виконання практичних робіт розташовують в системі дистанційної освіти, наприклад, Google Classroom або Moodle і можуть у будь який момент бути завантаженими здобувачами для виконання. Результатом виконання практичного завдання є файл прошивки мікроконтролера, який викладач може завантажити у віртуальний лабораторний макет на своєму комп’ютері і, встановивши потрібний варіант, перевірити правильність роботи програмного коду, який створив здобувач. Це дозволяє використовувати асинхронний метод навчання – коли викладач, та здобувач працюють у різні періоди часу – що є іще однією додатковою перевагою запропонованого підходу.

Висновки. Розглянуто метод навчання програмуванню мікроконтролерів здобувачів, що навчаються за дистанційною формою навчання, результати практичного впровадження якого показують, що за допомогою створеної спеціалізованої віртуальної лабораторії можна якісно вирішити цю задачу. Впровадження спеціалізованих віртуальних макетів дозволяє обійтися без фізичного моделювання та використання

реальних контрольно-вимірювальних приладів. При цьому у багатьох випадках код, написаний для мікроконтролера, що працює у віртуальному тестовому середовищі, може нічим не відрізнятися від коду, призначеному для роботи у реальній схемі.

Література

1. Ben Lutkevich What is a Microcontroller and How Does it Work? URL: https://www.techtarget.com/iotagenda/definition/microcontroller

2. Рижова, А.Р. Оникієнко Ю.О. Аналіз особливостей використання ресурсів мікроконтролера для розпізнавання мовлення. *Мікросистеми, Електроніка та Акустика*. Київ, КПІ ім. І.Сікорського. 2022. Т. 27, вип. 2. С. 265406–1 – 265406–7.

3. Русу О.П. Універсальна віртуальна лабораторія для традиційної та дистанційної форм навчання. *Матеріали VIII всеукраїнської науково-практичної конференції студентів, аспірантів та молодих учених «Гуманітарний і інноваційний ракурс професійної майстерності: пошуки молодих вчених». Одеса, Україна, 18 листопада 2022 р.* С. 385 – 388.

4. Русу О.П., Маркітан А.С., Султанзаде Н.Р. Віртуальна лабораторія для програмування мікроконтролерів. *Матеріали IX всеукраїнської мультидисциплінарної конференції «Чорноморські наукові студії». Одеса, Україна, 12 травня 2023 р.* С. 214 – 216.

5. Integrated Development Environment (IDE) MPLAB X. URL: https://www.microchip.com/en-us/tools-resources/develop/mplab-x-ide

6. Proteus: PCB Design and Circuit Simulator Software. URL: https://www.labcenter.com/

УДК 004.9:373.5

Прокопінеко С.В.
здобувач другого (магістерського) рівня вищої освіти
факультету кібербезпеки, програмної інженерії
та комп'ютерних наук
спеціальність: 014.09 «Середня освіта (Інформатика)»
agroprofi.sergei@gmail.com
Міжнародний гуманітарний університет
м.Одеса,Україна
Науковий керівник
Григор'єва Т.І.
кандидат технічних наук, доцент,
завідувачка кафедри інформаційних технологій
факультету кібербезпеки, програмної інженерії
та комп'ютерних наук
tig15090808@gmail.com
Міжнародний гуманітарний університет

ПОСИЛЕННЯ ПРИКЛАДНОЇ СПРЯМОВАНОСТІ КУРСУ ІНФОРМАТИКИ В ШКОЛІ

Анотація. *В роботі запропоновано використання компетентнісних задач на уроках інформатики, що сприяє підвищенню рівня підготовки учнів до життя у сучасному інформаційному суспільстві. Вирішення учнями задач практичного спрямування сприятиме їх всебічному розвитку. Пропонується застосування методу Case Study на уроках інформатики, що має значний потенціал для підвищення ефективності навчального процесу. Наведено аналіз переваг і недоліків методу Case Study. В роботі*

розглянуто конкретні приклади інтеграції прикладних завдань у шкільний курс інформатики.

Швидкий розвиток інформаційних технологій викликає необхідність в нових підходах до навчальних програм, які повинні відповідати проблемам та запитам суспільства. Одним із важливих аспектів є посилення прикладної спрямованості курсу інформатики в школі, що дозволяє учням отримувати практичні навички і знання, які можна застосовувати в реальному житті [1,2]. Прикладна спрямованість курсу інформатики має на меті підготовку учнів до використання інформаційних технологій у різних сферах діяльності. В роботі пропонується використовувати на уроках інформатикикомпетентнісні задачі [3] — це проблемні завдання з різних галузей людської діяльності, які розв'язуються засобами інформаційних технологій. Компетентнісні задачі в інформатиці спрямовані на формування та розвиток практичних навичок, логичного мислення та здатності застосовувати отримані знання в реальних життєвих ситуаціях. Вони включають задачі, що моделюють реальні проблеми, які можуть виникати в різних сферах діяльності.

Наприклад, в рамках теми «Аналіз даних» можно запропонувати таку компетентнісну задачу: Проаналізувати статистичні дані про результати тестування учнів у школі. Пропонується надати учням таблицю з результатами тестів: оцінки та час проходження тесту. Використовуючи програмне забезпечення для аналізу даних, наприклад, Excel, учні мають виявити закономірності, побудувати графіки і сформулювати висновки. В результаті розв'язання такої задачи, учні набудуть наступні компетентності: аналіз і синтез даних, робота з електронними таблицями, статистичний аналіз. Після розв'язання цієї задачі можна запропонувати учням наступну компетентнісну задачу: побудувати алгоритм сортування (наприклад, сортування бульбашкою, швидке сортування) для впорядкування списку учнів за їхніми оцінками. Компетенції: алгоритмізація, програмування, аналіз ефективності алгоритмів.

Пропонується використання на уроках інформатики такої методики навчання, як CASE (Cognitive Acceleration through Sience Education) [4]. Вона полягає у використанні конкретних випадків (ситуацій, історій) для спільного аналізу, обговорення або будування рішень учнями з певного розділу навчальної дисципліни. Робота з CASE передбачає розбір або «вирішення» конкретної ситуації з певного сценарію, який включає самостійну роботу, «мозковий штурм» в межах групи, публічний виступ із представленням та захистом запропонованого рішення, контрольне опитування учнів на предмет знання фактів кейсу, що розбирається, тощо.

Пропонується використання засобів інформаційних технологій у розв'язанні життєвих задач і задач, які виникають в різноманітних ситуаціях бізнесів за допомогою методики навчання CASE. Розглянемо конкретний приклад. В різних сферах підприємницької діяльності дуже важливим є контроль показників обладнання, техніки тощо. Для рішення таких задач контролю розробники программного забезпечення використовують дуже прості шкільні знання, а саме властивості лінійної функції. Одніею з сфер використання таких алгоритмів є сільське господарство. Наприклад, програмний код, який дозволяє контролювати об'єм палива в паливних баках сільськогосподарської техніки, що в свою чергу автоматизує процес роботи підриємства і дозволяє зменьшити кількість спожитого палива, спирається на розв'язки відповідних лінійних рівнянь. Інший приклад: розглянути на уроках інформатики можливість побудови алгоритмів, які забезпечують надійне калібрування, що покращує точність вимірювань і загальну ефективність роботи техніки.

Інтеграція прикладних завдань у курс інформатики пропонується за допомогою проектного методу навчання, створення ситуаційних задач, розробки міні-проектів, пов'язаних з реальними проблемами. Наприклад, учні можуть створювати веб-сайти, розробляти мобільні додатки, автоматизувати процеси за допомогою програмування.

Такий підхід дозволяє учням бачити результати своєї роботи, що підвищує їхню мотивацію до навчання.

Case Study або тематичне дослідження [5], є поглибленим дослідженням конкретної події. Воно дозволяє аналізувати майже кожен аспект життя та історії суб'єкта, виявляючи моделі та причини поведінки. Цей метод широко використовується в багатьох галузях, включаючи психологію, медицину, освіту, антропологію, політологію та соціальну роботу. У сфері освіти, зокрема на уроках інформатики, кейс-стаді може бути ефективним засобом для вивчення і закріплення навчального матеріалу, розвитку критичного мислення та формування практичних навичок. Використання Case Study на уроках інформатики може включати аналіз реальних ситуацій, з якими можуть стикнутися програмісти, адміністратори мереж чи інші IT-спеціалісти. Наприклад, учні можуть розглядати випадки кібербезпеки, аналізуючи причини та наслідки конкретних інцидентів, і розробляти стратегії запобігання подібним проблемам у майбутньому.

Серед переваг застосування Case Study на уроках інформатики можна вказати:

1. Кейс-стаді дозволяє застосовувати теоретичні знання на практиці, що підвищує мотивацію до вивчення предмету.
2. Учні мають можливість детально вивчати конкретні випадки, що сприяє глибокому розумінню теоретичних концепцій, що сприяє глибокому розумінню матеріалу.
3. Аналіз реальних ситуацій та пошук рішень сприяють розвитку критичного мислення та навичок вирішення проблем.
4. Використання кейсів сприяє інтеграції знань з різних галузей, що є важливим для сучасної освіти.

Однак, метод Case Study також має свої виклики, такі як суб'єктивність та часовитрати, які необхідно враховувати при плануванні навчальних занять. Успішне впровадження кейс-стаді в навчальний процес вимагає ретельного планування та підготовки, але його переваги можуть значно перевершити недоліки, забезпечуючи учням цінний досвід і знання.

Недоліки Case Study на уроках інформатики:

1. Case Study може бути суб'єктивним, що іноді ускладнює узагальнення результатів для більшого числа випадків.
2. Підготовка та аналіз кейсів вимагають значного часу, що може бути викликом в умовах обмеженого навчального часу.
3. Оцінка результатів роботи з кейсами може бути суб'єктивною та потребує ретельного підходу з боку викладача.

Середня школа має підготувати учнів до використарння теоритичних знань, їх всебічному розвитку, ефективному застосуванню набутих навичок. Такий підхід, як метод Case Study дозволяє учням не тільки закріпити теоретичні знання, але й здобути цінний практичний досвід. Таким чином, вирішення учнями задач практичного спрямування сприятиме їх всебічному розвитку, актуалізації широкого спектра знань, ефективному формуванню понять, а також глибокому усвідомленню змісту навчального матеріалу. Це підвищить зацікавленість у вивченні предмета, продемонструє можливі способи використання засобів інформаційних технологій для розв'язання життєвих задач, створить умови для реалізації компетентнісного підходу в навчанні інформатики та забезпечить формування інформатичних компетентностей.

Висновки

1. Компетентнісні задачі з інформатики є важливою складовою сучасного освітнього процесу. Вони дозволяють учням застосовувати отримані знання на практиці, розвивати критичне мислення та готують їх до вирішення реальних проблем у майбутньому.

2. В роботі запропоновано використання компетентнісних задач на уроках інформатики, що сприяє формуванню професійних компетентностей і підвищенню рівня підготовки учнів до життя у сучасному інформаційному суспільстві.

3. Пропонується застосування Case Study на уроках інформатики, що має значний потенціал для підвищення ефективності навчального процесу. Воно сприяє глибокому розумінню матеріалу, розвитку критичного мислення та практичних навичок. В роботі наведено аналіз переваг і недоліків методу Case Study.

4. В роботі розглянуто конкретні приклади інтеграції прикладних завдань у шкільний курс інформатики.

Література

1. Інноваційні технології в сучасному освітньому просторі: колективна монографія / За заг. редакцією Г.Л. Єфремової. – Суми: Вид-во СумДПУ імені А. С. Макаренка, 2020. – 444 с.

2. https://vseosvita.ua/webinar/vykorystannia-materialiv-shtuchnoho-intelektu-v-osviti-iak-ne-porushyty-akademichnu-dobrochesnist-1070.html

3. Морзе Н.В., Кузьмінська О.Г. Компетентнісні задачі з інформатики. - Науковий часопис НПУ імені М.П. Драгоманова. Серія №2. Комп'ютерно-орієнтовані системи навчання: Зб. наукових праць. / Редрада. – К.: НПУ імені М.П. Драгоманова , №6 (13), 2008.

4. http://megalib.com.ua/content/3926_Metodika_CASE.html

5. https://www.verywellmind.com/how-to-write-a-psychology-case-study-2795722

УДК 004.738.5:37.018.43

Рак М.О.
здобувач магістерського рівня вищої освіти
факультету кібербезпеки, програмної інженерії
та комп'ютерних наук
спеціальність: 014.09 «Середня освіта (Інформатика)»
misha.rak.2401@gmail.com
Міжнародний гуманітарний університет
м.Одеса,Україна
Науковий керівник
Григор'єва Т.І.
кандидат технічних наук, доцент,
завідувачка кафедри інформаційних технологій
факультету кібербезпеки, програмної інженерії
та комп'ютерних наук
tig15090808@gmail.com
Міжнародний гуманітарний університет

ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ТА СЕРВІСІВ ПРИ ВИКЛАДАННІ ІНФОРМАТИКИ

Анотація. *В даній роботі розглядається вплив хмарних технологій на процес викладання інформатики. Проведено порівняльний аналіз основних хмарних платформ: Google Workspace, Microsoft Azure та Amazon Web Services (AWS). Розглянуто їхні переваги та недоліки у контексті навчального процесу, а також можливості практичного застосування у викладанні. Запропоновано розробка віртуальної лабораторії з предмету інформатика на базі Microsoft Azure, інтегровану з інтелектуальним чат-ботом-асистентом.*

Сучасна освіта все більше інтегрується з цифровими технологіями, і хмарні сервіси відіграють в цьому процесі ключову роль [1,2]. Вони надають викладачам та учням широкий спектр можливостей: від доступу до навчальних матеріалів та спільної роботи над проектами до проведення онлайн-занять та створення віртуальних лабораторій. Хмарні технології сприяють підвищенню ефективності навчання, розвитку цифрової грамотності.

Серед ключових переваг хмарних технологій в освіті можна виділити:

1. Доступність. Хмарні сервіси забезпечують доступ до навчальних матеріалів та інструментів з будь-якого пристрою з підключенням до Інтернету, що робить навчання більш гнучким та зручним.
2. Співпраця. Хмарні платформи дозволяють учням та викладачам спільно працювати над проектами, обмінюватися ідеями та матеріалами, що сприяє розвитку навичок командної роботи та комунікації.
3. Масштабованість. Хмарні ресурси легко масштабуються, що дозволяє навчальним закладам адаптуватися до змін кількості учнів та обсягу даних.
4. Економія коштів. Використання хмарних технологій може знизити витрати на придбання та обслуговування власної IT-інфраструктури.
5. Інновації. Хмарні платформи постійно оновлюються та розширюють свої можливості, що дозволяє викладачам використовувати найсучасніші інструменти та технології у навчальному процесі.

Серед провідних хмарних платформ, які активно використовуються в освітньому середовищі, можна виділити Google Workspace [3], Microsoft Azure [4] та Amazon Web Services (AWS) [5]. Кожна з них має свої унікальні переваги та обмеження, тому вибір оптимального рішення залежить від конкретних потреб та цілей навчального закладу.

Google Workspace

Основною перевагою Google Workspace є простота та доступність. Інтуїтивно зрозумілий інтерфейс та безкоштовний базовий план роблять Google Workspace ідеальним вибором для шкіл та невеликих освітніх установ.Google Workspace пропонує такий набір інструментів: Офісні додатки (документи, таблиці, презентації), електронна пошта, календар, сховище файлів та відеоконференції забезпечують все необхідне для спільної роботи та комунікації.Інтеграція з платформою Google Classroom дозволяє легко організовувати навчальний процес, створювати завдання, тести, онлайн-опитування та проводити уроки у формі відеоконференції.Але є обмеження: функціональність Google Workspace може бути недостатньою для складних технічних завдань, а обсяг безкоштовного сховища обмежений.

Microsoft Azure

Основною перевагою Microsoft Azure є його потужність та гнучкість. Він пропонує широкий спектр сервісів для розробки, тестування та розгортання програмного забезпечення, аналізу даних, машинного навчання та штучного інтелекту. Інтеграція з платформою Microsoft Teams дозволяє проводити онлайн-заняття, організовувати спільну роботу над документами та надавати доступ до навчальних матеріалів. Azure також дозволяє створювати віртуальні лабораторії для практичних занять з програмування та інших технічних дисциплін. Проте, Azure є складнішою у використанні та вимагає певних технічних знань для налаштування та управління. Вартість використання може бути високою для невеликих установ.

Amazon Web Services (AWS)

AWS вирізняється своєю неперевершеною універсальністю, пропонуючи найбільш повний набір сервісів та інструментів для будь-яких потреб, включаючи високопродуктивні обчислення, зберігання даних, бази даних, аналітику, мобільні сервіси та безпеку. AWS також забезпечує гнучкість та масштабованість, дозволяючи налаштувати інфраструктуру під конкретні потреби та легко масштабувати її в міру зростання потреб. Проте, AWS є найскладнішою у використанні та вимагає високої

кваліфікації від користувачів. Вартість використання може бути значною, особливо для невеликих установ.

Практичне застосування хмарних технологій у викладанні інформатики

Google Workspace:

- Організація дистанційного навчання за допомогою Google Classroom.
- Спільна робота над проектами з використанням Google Docs, Sheets та Slides.
- Проведення онлайн-тестування та опитувань за допомогою Google Forms.
- Використання Google Meet для проведення уроків та консультацій у формі відеоконференцій

Microsoft Azure:

- Створення віртуальних лабораторій для практичних занять з програмування та інших технічних дисциплін.
- Використання сервісів машинного навчання та аналізу даних для навчальних проектів.
- Розробка та розгортання власних веб-додатків та сервісів.

Amazon Web Services (AWS):

- Розгортання масштабованих навчальних платформ та систем управління навчанням.
- Використання сервісів AWS для зберігання та обробки великих обсягів даних.
- Створення високонавантажених веб-додатків та сервісів для освітніх потреб

Порівнюючи три основні хмарні платформи — Google Workspace, Microsoft Azure та Amazon Web Services (AWS) — можна виділити ключові переваги і обмеження кожної з них у контексті викладання інформатики:

Google Workspace є найбільш зручним і доступним вибором для загальних навчальних цілей, особливо у школах та для базових курсів, завдяки своїй простоті використання та безкоштовному доступу до основних інструментів. Однак, її функціональність може бути недостатньою для більш складних технічних проектів.

Microsoft Azure надає потужні ресурси для навчання програмуванню та аналітиці даних. Вона є ідеальним вибором для університетів і програм технічного спрямування, але потребує значних технічних знань для ефективного використання. Azure також відзначається своєю інтеграцією з Office 365, що є перевагою для тих, хто вже використовує ці інструменти.

Amazon Web Services (AWS) відома своєю гнучкістю та різноманіттям інструментів, що робить її ідеальною для складних проектів з розробки програмного забезпечення. Проте, висока вартість і складність використання можуть стати бар'єром для новачків і навчальних закладів з обмеженими ресурсами.

Загалом, вибір хмарної платформи залежить від специфічних потреб та ресурсів навчального закладу або курсу. Для базових освітніх цілей Google Workspace є найкращим вибором. Microsoft Azure підходить для більш технічно складних завдань і програм, в той час як AWS забезпечує максимальну гнучкість і потужність для проектів, що потребують великої обчислювальної потужності.

В роботі пропонується розробити віртуальну лабораторію для вивчення предмету інформатика на базі Microsoft Azure, інтегровану з інтелектуальним чат-ботом-асистентом. Лабораторія надасть учням доступ до віртуальних машин з попередньо встановленим програмним забезпеченням, навчальними матеріалами та інструментами для спільної роботи. Чат-бот, розроблений з використанням Azure Bot Service та Cognitive Services, забезпечить інтерактивну підтримку учнів, відповідаючи на запитання, надаючи підказки та рекомендації, а також відстежуючи їх прогрес. Така інтеграція сприятиме підвищенню ефективності навчання, надаючи учням персоналізовану допомогу та зворотний зв'язок у режимі реального часу.

Висновки

1. Розглянуто вплив хмарних технологій на процес викладання інформатики.
2. Проведено порівняльний аналіз основних хмарних платформ: Google Workspace, Microsoft Azure та Amazon Web Services (AWS).
3. Розглянуто переваги та недоліки хмарних платформ у контексті навчального процесу, а також можливості практичного застосування у викладанні.
4. В роботі пропонується розробити віртуальну лабораторію з предмету інформатика на базі Microsoft Azure, інтегровану з інтелектуальним чат-ботом-асистентом.

Література

1. Інноваційні технології в сучасному освітньому просторі: колективна монографія / За заг. редакцією Г.Л. Єфремової. – Суми: Вид-во СумДПУ імені А. С. Макаренка, 2020. – 444 с.
2. Олексюк В. Теоретико-методичні основи проєктування, адміністрування та використання хмаро орієнтованого середовища навчання майбутніх учителів інформатики : Дис. … д-ра пед. наук : 13.00.10. Київ, 2023. 524 с. http://elar.ippo.edu.te.ua:8080/handle/123456789/6440
3. Google Workspace Learning Center https://support.google.com/a/users/?hl=en#topic=9247638
4. Microsoft Technical documentation https://learn.microsoft.com/en-us/docs/
5. AWS Documentation https://docs.aws.amazon.com/?nc2=h_ql_doc_do

УДК 372.851.9

Горбачов В. Е., к.т.н., доцент
Заянчуковський О. В., студент І курсу,
другого (магістерського) рівня
Міжнародний гуманітарний університет
Горбачов П. В., студент І курсу
Фаховий коледж НТІІС
physmgu@gmail.com

ЗАСТОСУВАННЯ МЕТОДУ АЛГОРИТМІЗАЦІЇ СКЛАДНОГО НАВЧАЛЬНОГО МАТЕРІАЛУ ПРИ ВИВЧЕННІ ВСТАНОВЛЕННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX

Анотація. *У роботі розглядаються особливості застосування методу алгоритмізації складного навчального матеріалу для підвищення його доступності та покращення сприйняття при вивчені послідовності операцій і команд при встановленні операційної системи Linux. Вся інформація, що вивчається по темі, розбита на шість тематичних закінчених блоків, тому що наприкінці кожного блоку студент може перевірити правильність виконаного завдання. Отриманий таким чином алгоритм чітко фіксує мету заняття, а його елементи будуть своєрідними структурними опорними сигналами по темі. Результати проведених за такою методикою занять свідчать про те, що більшість студентів за час навчання вивчають напам'ять назви шести блоків алгоритму, а сам процес встановлення ОС стає простим і навіть захоплюючим.*

Операційна система (ОС) – це набір програм, за допомогою яких електроніка комп'ютера взаємодіє з периферійними пристроями, користувачем та інтернетом. На сьогоднішній день для масового користування застосовуються три основні ОС:

- по-перше, це MS Windows, яка перевантажена пакетами сервісних програм оновлення, стеження, визначення геолокації, антивірусами, а тепер ще й штучним

інтелектом, які дуже сповільнюють роботу системи, і при цьому вона досить дорого коштує;

- по-друге, це MacOS, яка призначена для встановлення тільки на комп'ютери Mac, які значно гірші за характеристиками і не мають можливості заміни комплектуючих на кращі аналоги, крім того, менший у порівнянні з Windows вибір програм і всі вони, включаючи саму ОС , коштують вдвічі дорожче за аналоги Windows.

- по-третє, це ОС на базі ядра Linux, яка є альтернативною першим двом, оскільки має відкритий вихідний код і абсолютно безкоштовна сама і всі її програми, крім того, завдяки особливому способу запуску програм не потребує антивірусів принаймні для звичайних користувачів. У Linux встановлюються лише ті програми та додатки, які необхідні користувачеві для вирішення конкретних завдань, цим пояснюється той факт, що всі банківські термінали та сервери працюють з ОС Linux. За останні роки на базі ядра Linux створено ряд ОС, розраховані на всі види комп'ютерів та різні категорії споживачів: з максимально схожим на Windows інтерфейсом, з полегшеним варіантом встановлення та стандартним набором додатків для непідготовлених користувачів, творчі ОС для досвідчених користувачів, розроблені повні інструкції з їх застосування. Однак, незважаючи на всі ці переваги, масове використання безкоштовних ОС на базі ядра Linux відбувається дуже повільно через уявне упередження про складність установки цих ОС. Тому завдання підвищення ефективності при навчанні роботі з ОС Linux дуже актуальна в нашій країні в умовах масового використання комп'ютерів в режимі жорсткої економії коштів.

Метою даної роботи є підвищення доступності та поліпшення сприйняття складного навчального матеріалу роботи з ОС ArchLinux при використанні методу алгоритмізації.

У педагогіці є ряд методів, які дозволяють складний матеріал зробити доступнішим для сприйняття слухачів [1-3]. Застосовуються такі технології, як візуалізація інформації, що вивчається [1], скрайбінг [2], адаптивне навчання [3], і тому подібне. Вибір форм і методів організації процесу у кожному даному випадку лежить повністю на викладачі. У цій роботі застосовується системний підхід до навчання або, як його зараз прийнято називати, метод алгоритмізації.

Для ілюстрації використання методу алгоритмізації навчального матеріалу у роботі вибрано такий складний розділ інформатики, як встановлення операційної системи та графічного інтерфейсу с консолі. Прийнято вважати, що таку операцію повинні виконувати лише досвідчені користувачі, однак, використання методу алгоритмізації навчального матеріалу для спрощення розуміння дій і команд, які виконуються при встановленні ОС, робить процес засвоєння розділу більш доступним для більшої кількості студентів, які мають різний рівень підготовки.

Основні операції адміністрування, включаючи сам процес встановлення системи, в ОС ArchLinux здійснюються в консолі за допомогою введених вручну самим користувачем команд (робота з консолі). Саме це унеможливлює мимовільний запуск вірусів у Linux. Вже після встановлення системи, також з консолі, встановлюються перевірені на відсутність вірусів графічний інтерфейс, службові програми та програми, які вже мають такі звичні для користувачів Windows іконки запуску програм. Адміністрування з консолі – це ціна, яку треба сплачувати за відсутність вірусів!

Для спрощення сприйняття у роботі пропонується всю послідовність дій та команд установки ОС ArchLinux розбити на шість самостійних блоків алгоритму. Розбиття проводилося за принципом логічної завершеності певної послідовності дій. Критерієм завершеності кожного блоку вибиралася можливість виконати перевірку коректності виконання алгоритму межах даного блоку. Таким чином, не отримавши позитивного результату перевірки, студент не може приступити до виконання наступного блоку. На рис. 1 алгоритм встановлення ОС ArchLinux представлено у графічної формі.

Рисунок 1 – Графічна форма представлення алгоритму встановлення ОС ArchLinux

Така форма представлення алгоритму дозволяє студенту чітко бачити мету, яку він має досягти в результаті вивчення теми, а також засоби її досягнення. Назви шести елементів алгоритму є опорними сигналами для студента при виконанні завдання та запам'ятовуванні його змісту. На схемі алгоритму (рис. 1) зображено результати виконання перевірок правильності виконання дій у межах блоку, тому кожен із елементів є логічно закінченим і представляє самостійний елемент у процесі установки.

На рис. 2 представлена таблиця відповідності перших двох блоків графічного представлення алгоритму вказівкам що до виконання дій, які складають цей блок алгоритму.

У першому блоці розглядається процес створення завантажувального носія. Після виконання завдання блоку студент самостійно перевіряє коректність дій шляхом завантаження комп'ютера з інсталяційного носія. Позитивним результатом є початок завантаження ОС. У другому блоці вивчається процес розмітки носія, який встановлюється ОС. У роботі розглядається найпростіший випадок одного носія об’ємом 512G зі стандартом таблиці розділів GPT. В результаті виконання завдання блоку студент має отримати таблицю розділів диска із заявленими параметрами.

З рис. 2 видно, що кожен блок має ще свою структуру, і при бажанні можна подати у вигляді свого локального алгоритму. Але такий підхід структурного програмування вимагає обережного поетапного застосування, оскільки вкладені локальні алгоритми сильно захаращують вихідну схему, через що вона може втратити свою наочність, а це була наша основна мета.

Як показали результати проведених за такою методикою занять, всі студенти проходили етапи алгоритму, щоправда, з різним часом виконання. Основна причина затримок – неуважність при наборі команд та значень параметрів з клавіатури, але наявність перевірки наприкінці кожного блоку дозволяло не починати встановлення спочатку, а виправляти помилки в межах останнього блоку. У результаті, ті студенти, які кілька разів повторювали дії, напам'ять вивчили назви всіх шести блоків алгоритму.

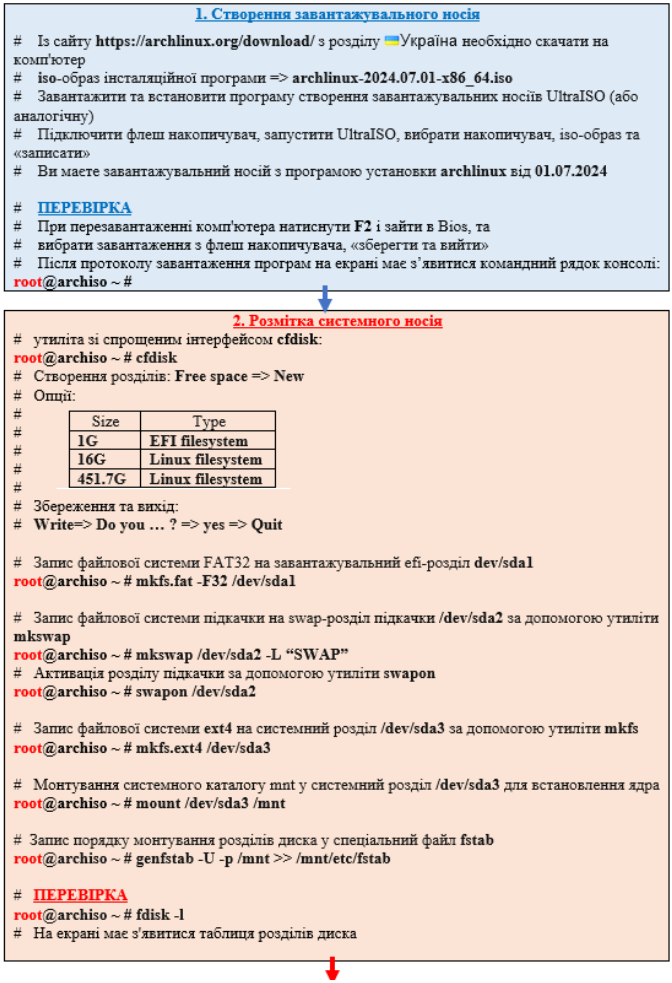


Рисунок 2 – Таблиця відповідності перших двох блоків графічного представлення алгоритму встановлення ОС ArchLinux

Література

1. Морзе Н.В. Методика навчання інформатики: навч. посіб. ч.IV: Методика навчання основ алгоритмізації та програмування / Н.В. Морзе // К.: Навчальна книга, – 2004. – 368с.

2. Семенова О.І. Шляхи формування алгоритмічних умінь і навичок учнів / О.І. Семенова // Комп'ютер у школі та сім'ї. – 2009. – № 4. – С. 24-27..

3. Носенко Ю.Г. Адаптивні системи навчання: сутність, характеристика, стан використання у вітчизняних закладах педагогічної освіти / Ю.Г. Носенко // Фізико-математична освіта. – 2018. – В. 3(17). – С. 73-78.

УДК372.862

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Воробей Євгеній Володимирович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 014 Середня освіта
Міжнародний гуманітарний університет

МЕТОДИКА ОЦІНЮВАННЯ РІВНЯ ЗНАНЬ ЗДОБУВАЧІВ, ЩО НАВЧАЮТЬСЯ ПРОГРАМУВАННЮ МІКРОКОНТРОЛЕРІВ

Анотація.*Розглянуто методику оцінювання рівня знань здобувачів, що навчаються програмуванню мікроконтролерів, на прикладі тестових завдань для дисципліни «Програмування мікроконтролерів та пристроїв інтернету речей», яка викладається здобувачам факультету кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету. Запропонована методика формує завдання, що мають три рівня складності (достатній, середній та високий) і може використовуватися як при очній, так і при дистанційній формі навчання.*

Дистанційна форма навчання вже давно стала об'єктивною реальністю нашого сьогодення, однак методики оцінювання рівня знань здобувачів, що обрали саме цю форму навчання, поки ще знаходяться у стадії пошуку найбільш оптимальних форм та методів. Традиційні форми поточного контролю, такі як усне опитування чи контрольні роботи в кінці аудиторних занять, при дистанційній формі навчання стають вельми утрудненими, а інколи і зовсім неможливими, особливо коли викладач та здобувач опрацьовують матеріал асинхронно – у різні проміжки часу.Це і обумовило мету роботи, яка полягає у пошуку методики оцінювання рівня знань здобувачів, що навчаються програмуванню мікроконтролерів, яку можна було в використовувати і при очній, і при дистанційній формах навчання.

Одним з варіантів вирішення цієї задачі є онлайн-тестування, коли здобувачу пропонується в кінці аудиторного заняття пройти опитування та одразу в автоматичному режимі оцінити власний рівень знань. Наразі засоби для створення онлайн-тестів є у більшості платформ для дистанційної освіти, у тому числі і у платформиMoodle[1] – яка використовується в Міжнародному гуманітарному університеті. Засоби саме цієї платформи і були використані для створення комплексу тестів, які використовувались під час підготовки здобувачів факультету кібербезпеки, програмної інженерії та комп'ютерних наук, що вивчали дисципліну «Програмування мікроконтролерів та пристроїв інтернету речей».

При створені тестів використовувались наступні положення:

– тестові завдання повинні матирізні рівні складності: достатній, середній та високий;

– максимальна оцінкаповинна дорівнювати100 балам;

– мінімальна оцінка, яку повинен отримати здобувач для того щоб отримати залік по поточній темі, повинна дорівнювати 60 балам;

– структура тестових завданьповинна мінімізувати імовірність неправильної оцінки рівня знань здобувачів, у тому числі і завищеної оцінки здобувачів із недостатнім рівнем знань.

Для того, щоб вирішити поставлені задачі використовувалась наступна методика складання тестових завдань:

1. Кожен тест складається із 20 завдань, за кожне з яких здобувач може отримати до 5 балів. Таким чином, максимальна оцінка за тест дорівнює 100 балам.

2. Розподілпитань по рівням складності в межах тесту виглядає наступним чином:

– достатній рівень – 12 питань із максимальною загальною оцінкою 60 балів;

– середній рівень – 5 питань із максимальною загальною оцінкою – 25 балів;

– високий рівень – 3 питання із максимальною загальною оцінкою – 15 балів.

3. Серед питань достатнього рівня є щонайменше 2 питання, які формуються випадковим чином і з малою імовірністю повторюються при повторному проходженні тесту або при проходженні тесту іншим здобувачем.

4. Для вирішення завдань середнього рівня здобувач повинен виконати певні самостійні дії, наприклад, провести обчислення за певною формулою або виконати певний програмний код. Вихідні дані при цьому змінюються при наступному проходженні тесту або при проходженні тесту іншим здобувачем.

5. Для вирішення завдань високого рівня здобувач повинен самостійно опрацювати певний матеріал, який не входить до методичного забезпечення до цієї теми, наприклад, самостійно опрацювати певний розділ технічної документації, чи знайти в мережі Інтернет технічні характеристики певного електронного приладу.

Таким чином, для того щоб отримати мінімальну оцінку 60 балів здобувачеві достатньознайти в методичних матеріалах правильні відповіді на 12 питань достатнього рівня, щонайменше два з яких при повторному проходженні тесту будуть відрізнятися від попередніх. Для отримання більш високої оцінки здобувач повинен додатково виконати п’ять завдань середнього рівня, які передбачають самостійні маніпуляції із унікальними вихідними даними, використовуючи для цього інформацію, що була надана під час аудиторних занять і знаходиться в методичному забезпеченні. Для отримання максимальноїоцінки (100 балів) здобувачеві потрібно ще додатково правильно виконати три завдання, які передбачають самостійний пошук та обробку необхідної інформації.

Завдання, що мають достатній рівень складності, зазвичай, формуються на основі питань із множинним вибором. У цьому випадку здобувач повинен обрати одну або декілька правильних відповідей. За кожну правильну відповідь здобувачеві нараховуються бали, загальна кількість яких не перевищує п’яти. За кожні неправильну відповідь здобувачеві нараховуються штрафні бали, які зменшують загальну кількість балів, отриманих за це питання. Таким чином, для отримання максимальної кількості балів за це питання здобувач повинен обрати усі правильні відповіді і не обрати жодної неправильної.

Приклад питання із достатнім рівнем складності для дисципліни «Програмування мікроконтролерів та Інтернет речей» наведений на рис. 1. У цьому питанні є лише одна правильна відповідь – «Арифметичне додавання акумулятора до регістру оперативної пам’яті». Обравши її здобувач отримає максимальну оцінку за це питання – 5 балів. Якщо здобувач відмітить будь-яку іншу відповідь, то за відповідь він отримає 0 балів.

При наступній спробі проходження тесту текст цього питання буде змінюватися. Наприклад, замість команди «addwf» може бути команда «addlw», яка виконує арифметичне додавання константи до акумулятора, або навіть неіснуюча команда, наприклад, «abbwf». В останньому випадку здобувач повинен обрати відповідь «Немає правильної відповіді» оскільки такої команди в наборі інструкційасемблера не існує[2].

Питання середнього та високого рівня складності можуть формуватися на основі розрахункових питань або питань із можливістю введення числовоївідповіді (рис. 2). Для вирішення цієї задачі здобувач повинен самостійно розібратися із особливостями функціонування конкретної частини конкретного мікроконтролера, наприклад, виконати (в уяві або на симуляторі) програмний код, що міститься в завданні.

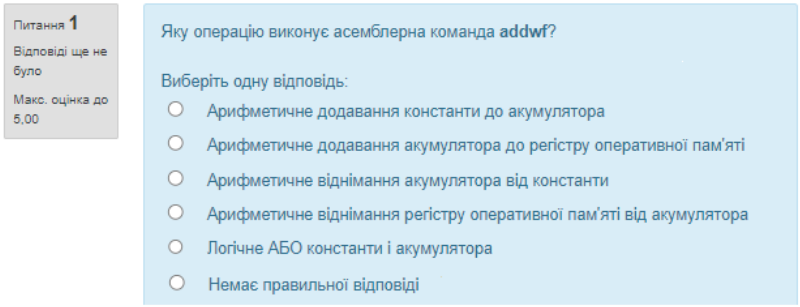


Рисунок 1 – Приклад питання із достатнім рівнем складності

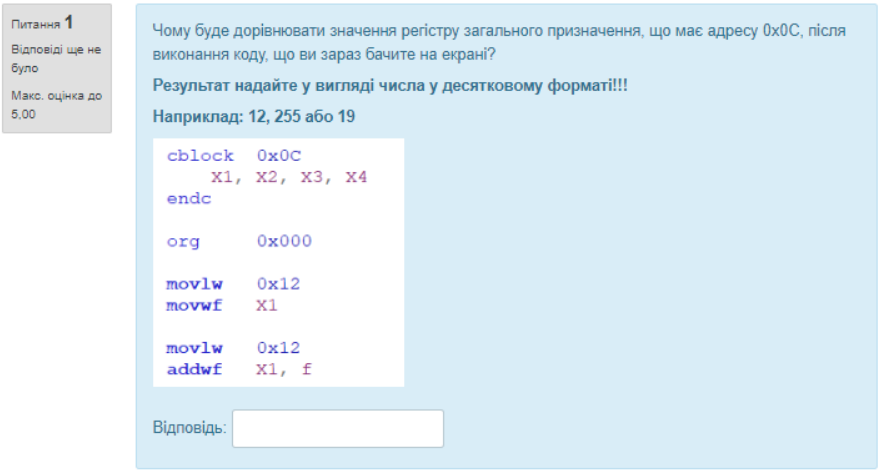


Рисунок 2 – Приклад питання із середнім або високим рівнем складності

Для завдання середнього рівня складності здобувачеві достатньо використовувати формули, рисунки та інші методичні матеріали, які розглядалися на лекційному або практичному занятті. Для завдань високого рівня складності здобувачеві потрібно використати матеріал, який виходить за межі запропонованого методичного забезпечення цієї теми. У цьому випадку для того, щоб вирішити це завдання, здобувачеві потрібно самостійно знайти та опрацювати необхідну технічну документацію.

Висновки.Запропонована методика оцінювання рівня знань здобувачів, що навчаються програмуванню мікроконтролерів може використовуватися як при дистанційній, так і при очній формах навчання. Завдяки використанню завдань із кількома рівнями складності, вона дозволяє гнучко оцінювати рівень знань здобувачів. Додатковою перевагою онлайн-тестування є можливість оперативного ознайомлення із оцінкою за кожне виконане завдання, що дозволяє здобувачам самостійно опрацювати власні проблемні місця не чекаючи вказівки викладача.

Література

1. Платформа дистанційної освіти Moodle.URL: https://moodle.org/
2. Мікроконтролери Microchip. URL: https://www.microchip.com/en-us/products/microcontrollers-and-microprocessors

УДК 371.3:371.64

Василенко О.А., кандидат педагогічних наук, доцент,
Університет прикладних наук Анхальт, місто Кьотен, Німеччина
oksana.vasylenko@hs-anhalt.de
Григор'єва Т.І., кандидат технічних наук, доцент,
Міжнародний гуманітарний університет, місто Одеса, Україна
tig15090808@gmail.com

КЛЮЧОВІ ФАКТОРИ ЕФЕКТИВНОГО ЗМІШАНОГО НАВЧАЛЬНОГО СЕРЕДОВИЩА

Анотація. *Розглядаються змішані форми навчання, їхні переваги, виклики та перспективи впровадження. Аналізується роль цифрових технологій у підтримці змішаного навчання, а також наводяться ключові фактори ефективного змішаного навчального середовища. Окрему увагу приділено моделі "Перевернутий клас" та методам її реалізації.*

Інтеграція цифрових технологій зі звичайними методами викладання та навчання є важливою особливістю сучасної освіти [1]. Цей процес швидко розвивається, що обумовлено не лише технічним прогресом, але й підвищенням цифрових навичок серед усіх учасників навчального процесу. Змішані форми навчання, що поєднують традиційні методи викладання з використанням цифрових технологій та онлайн навчання залишаються наразі найбільш популярними в освітньому середовищі. Цей підхід дозволяє забезпечити більш гнучкий та індивідуалізований процес навчання, який відповідає потребам сучасних учнів та вимогам освітнього процесу [2,3].

Основні аспекти змішаного навчання

1. Індивідуалізація навчання. Учні можуть навчатися у власному темпі, використовуючи цифрові ресурси. Можливість адаптації матеріалу під індивідуальні потреби кожного є однією з ключових переваг змішаного навчання. Використання цифрових платформ дозволяє вчителям створювати персоналізовані навчальні маршрути, які враховують рівень підготовки, інтереси кожного учня та можливий темп навчання. Це сприяє підвищенню мотивації до навчання та дозволяє досягти кращих результатів.

2.Гнучкість. Поєднання очного та онлайн-навчання дозволяє адаптувати навчальний процес до індивідуальних потреб учасників навчального процесу. Змішане навчання також дозволяє більш ефективно використовувати час на занятті. Частину теоретичного матеріалу можна опановувати самостійно за допомогою онлайн-ресурсів, відеолекцій та інтерактивних презентацій. Це звільняє час на заняттях для обговорення, практичних завдань та роботи в групах. Такий підхід сприяє розвитку критичного мислення, комунікативних навичок та вмінь працювати в команді.

Однією з найпопулярніших моделей змішаного навчання є модель «Перевернутого класу». Ця модель передбачає, що учні спочатку самостійно ознайомлюються з новим матеріалом за допомогою відео, аудіо, інтерактивних презентацій та інших навчальних ресурсів. Після того, як вони отримують базове розуміння теоретичних аспектів, на занятті вони виконують практичні завдання, які допомагають закріпити нові знання. Окрім практичних завдань, важливою частиною занять є обговорення складних питань з учителем, що дозволяє учням глибше зрозуміти матеріал і розвинути критичне мислення.

Це забезпечує можливість обміну думками та колективного розв'язання проблем, що сприяє більш ефективному навчальному процесу. Модель «Перевернутого класу» дозволяє оптимально використовувати час на занятті, оскільки учні вже підготовлені до активної роботи й можуть зосередитися на практичних аспектах та уточненні незрозумілих моментів. Крім того, така модель сприяє розвитку самостійності, відповідальності та навичок самонавчання у учнів, що є важливими компонентами сучасного освітнього процесу.

Для успішної реалізації моделі «Перевернутого класу» необхідно:

- Забезпечити доступ до якісних відео, аудіо, інтерактивних презентацій та інших навчальних матеріалів, які мають бути чіткими, змістовними та добре структурованими.
- Підтримувати інтерактивність, тобто використовувати онлайн-опитування, форуми, конференції та інші інструменти для обговорення матеріалу.
- Організувати групову роботу: сприяти активній взаємодії між учнями під час виконання завдань.

Для змішаного навчання можна використовувати і інші популярні моделі навчання. Наприклад, "Флекс-модель" дозволяє учням обирати між онлайн- та офлайн-компонентами. В рамках "Моделі з оберненою послідовністю" завдання задають перед уроком, на якому викладається теоретичний матеріал. Також можна використовувати "Гібридну модель". Важливим є гнучкий підхід до вибору моделей змішаного навчання, враховуючи специфіку предмету, потреби учнів та ресурси.

В рамках змішаного навчання викладачі можуть використовувати різноманітні інструменти та методи:

- Онлайн-платформи для розміщення навчальних матеріалів (наприклад, Moodle, Google Classroom, Coursera).
- Відео-лекції та пояснення. Наприклад, YouTube, Vimeo, Khan Academy.
- Інтерактивні завдання та вікторини. Наприклад, Kahoot, Quizlet, Socrative.
- Групові завдання, дискусії та проектні роботи.
- Зворотній зв'язок та оцінювання прогресу.

Важливо використовувати різноманітні методи для залучення слухачів до навчання, а також забезпечувати регулярний зворотній зв'язок.

3. Підвищення мотивації. Використання інтерактивних і цифрових ресурсів робить навчання більш цікавим та залучає учнів до активної участі у процесі. Застосування цифрових технологій у змішаному навчанні також сприяє розвитку цифрової грамотності учнів. Вони вчаться працювати з різними онлайн-ресурсами, використовувати інтернет для пошуку інформації та створювати власні цифрові продукти. Це є важливим елементом підготовки до життя в сучасному цифровому суспільстві.

Однак, впровадження змішаного навчання потребує певних зусиль з боку вчителів. Вони повинні володіти необхідними цифровими навичками та бути готовими використовувати нові технології в навчальному процесі. Також важливо забезпечити доступ учнів до необхідних технічних засобів та інтернету. Без цього ефективне впровадження змішаного навчання є неможливим.

Важливим аспектом є також підтримка та підготовка вчителів. Для цього необхідно проводити регулярні тренінги та семінари, які допоможуть вчителям освоїти нові технології та методики. Крім того, важливо забезпечити вчителів необхідними ресурсами та підтримкою з боку адміністрації школи.

Змішані форми навчання також вимагають змін в організації навчального процесу. Необхідно розробити нові методики оцінювання, які враховують як традиційні знання, так і навички, отримані в процесі самостійного навчання та роботи з цифровими ресурсами. Це дозволить забезпечити всебічну оцінку знань та вмінь учнів.

Дуже важливими є проведення досліджень та опитувань учасників освітнього процесу щодо їхнього досвіду використання змішаних форм навчання у середній школі.

Важливо вчасно виявляти та виправляти проблеми та впроваджувати зміни задля покращення результатів навчання.

Таким чином, змішані форми навчання є перспективним напрямом розвитку освіти, який дозволяє поєднати кращі традиційні методи з можливостями, які надають сучасні технології. Вони сприяють підвищенню ефективності навчального процесу, розвитку критичного мислення та цифрової грамотності учнів. Однак, їхнє впровадження потребує підготовки та підтримки з боку вчителів та адміністрації шкіл, а також забезпечення доступу до необхідних ресурсів та технічних засобів.

Ключові фактори ефективного змішаного навчального середовища

Змішане навчання, яке поєднує традиційні методи з цифровими технологіями, є інноваційним підходом, що значно підвищує ефективність освітнього процесу. Для досягнення максимальних результатів у змішаному навчальному середовищі необхідно враховувати кілька ключових факторів.

Перш за все, важливо забезпечити чітку структуру та організацію навчального процесу. Ретельне планування, чітка структура та детальна програма курсу допоможуть учням легко орієнтуватися в матеріалі. Необхідно забезпечити гармонійне поєднання традиційних і цифрових методів навчання, що дозволить досягти балансу між онлайн та офлайн навчанням.

Якісний цифровий контент є ще одним важливим аспектом ефективного змішаного навчального середовища. Використання відео, аудіо, інтерактивних презентацій та інших мультимедійних ресурсів допомагає зробити навчальний процес більш цікавим та доступним. Важливо також забезпечити учнів доступом до необхідних онлайн-матеріалів та навчальних ресурсів. Використання інтерактивних платформ для залучення студентів до активного навчання та обговорень дозволяє підтримувати високий рівень зацікавленості та залученості. Регулярний зворотний зв'язок та підтримка з боку викладача допоможуть учням зрозуміти свої сильні та слабкі сторони, а також сприяти їхньому академічному розвитку.

Розвиток цифрової компетентності викладачів також є важливим аспектом. Викладачі повинні постійно підвищувати свою кваліфікацію та освоювати нові технології. Вони повинні бути готові застосовувати нові методики та підходи в навчанні, що дозволить зробити навчальний процес більш ефективним та сучасним.

Технічна підтримка та інфраструктура є ще одним важливим фактором. Забезпечення надійної технічної підтримки як для викладачів, так і для учнів дозволяє уникнути багатьох проблем та забезпечити безперервність навчального процесу. Забезпечення якісного інтернет-зв'язку та доступу до необхідного обладнання також є критично важливим.

Створення мотивуючого середовища та відповідної атмосфери є ще одним ключовим фактором. Постійна підтримка сприятливого навчального клімату, який стимулює учнів до активного навчання, є важливим для досягнення високих результатів. Використання гейміфікації та інших методів для підвищення зацікавленості учнів допомагає підтримувати високу мотивацію та зацікавленість у навчальному процесі.

Оцінювання та моніторинг також є важливими аспектами. Використання різноманітних методів оцінювання для відстеження прогресу студентів дозволяє забезпечити всебічний підхід до оцінки їхніх знань та навичок. Постійний моніторинг та аналіз результатів навчання дозволяють вчасно вносити необхідні корективи та підвищувати ефективність навчального процесу.

Таким чином, ефективне змішане навчальне середовище потребує комплексного підходу, що враховує всі вищеописані фактори. Завдяки поєднанню традиційних методів навчання з сучасними цифровими технологіями можна створити динамічний, інтерактивний та ефективний навчальний процес, який відповідатиме потребам сучасних учасників освітнього процесу.

Висновки

1. Змішане навчання має значний потенціал для покращення якості освіти, адже дозволяє поєднувати традиційні методи викладання з сучасними цифровими технологіями, забезпечуючи індивідуальний підхід до кожного учня та підвищуючи їхню мотивацію до навчання. Проте для успішного впровадження змішаних форм навчання необхідно вирішити низку технічних та організаційних проблем, а також забезпечити належну підготовку вчителів.

2. Впровадження змішаних форм навчання потребує підготовки та підтримки з боку вчителів та адміністрації шкіл, а також забезпечення доступу до необхідних ресурсів та технічних засобів.

Література

1. Генсерук Г., Терещук Г., Сисоєв О., Василенко О. Змішане навчання в контексті цифрової трансформації вищої освіти // Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. Сер. Педагогіка. Тернопіль : ТНПУ ім. В. Гнатюка, 2023. № 1. С. 35-45. DOI : 10.25128/2415-3605.23.1.5

2. Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми // Зб. наук. пр. – Випуск 43 / Редкол. – Київ- Вінниця: ТОВ фірма «Планер», 2015. – 471 с.

3. Pinchuk L. M. Osvitnia tekhnologiia “Blended Learning” u konteksti osobystisno diialinisnoho pidkhodu [Educational technology “Blended Learning” in the context of a personal activity approach]. Scientific journal of the M. P. Drahomanov NPU. Series 5. Pedagogical sciences: realities and prospects. 2021. Vol. 83. P. 138–142.

УДК 621.314

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Луценко Даніїл Сергійович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 014 Середня освіта
Міжнародний гуманітарний університет

МАТЕМАТИЧНА МОДЕЛЬ ЕЛЕКТРИЧНИХ ПРОЦЕСІВ ПОНИЖУВАЛЬНИХ ПЕРЕТВОРЮВАЧІВ ІЗ ДВОМА ДЖЕРЕЛАМИ ЖИВЛЕННЯ

Анотація.*У роботі наведено приклад використання методів математичного моделювання апаратних вузлів комп’ютерної техніки, який можна використовувати в процесі підготовки фахівців в галузі інформаційних технологій та програмування. Розробленоматематичну модель електричних процесів імпульсних понижувальних перетворювачів із двома джерелами живлення, використання яких дозволить підвищити техніко-економічні показники сучасних інфокомунікаційних та комп’ютерних засобів. Наведено результати моделювання, які показують, що використання двох джерел живлення дозволить зменшити рівень перетворювальної потужності що, у свою чергу, дозволить зменшити масу, розмір та вартість перетворювачів.*

Глибинне розуміння методів математичного моделювання апаратних вузлів комп’ютерної техніки є важливим елементом підготовки фахівців в галузі інформаційних технології та програмування. Понижувальні перетворювачі напруги входять до складу більшості сучасних інфокомунікаційних та комп’ютерних засобів, у тому числі, персональних комп’ютерів, ноутбуків та смартфонів. Оскільки доволі велика кількість комп’ютерних та інфокомунікаційних пристроїв можуть власне джерело живлення,

наприклад, акумуляторну батарею, то для таких перетворювачів головним параметром є коефіцієнт корисної дії. Збільшення коефіцієнту корисної дії дозволяє не тільки зменшити рівень нагрівання пристроїв в процесі роботи, а ще й збільшити час автономної роботи.

Наразі в комп'ютерній та інфокомунікаційний техніці можуть використовуватися три типи понижувальних перетворювачів: параметричні стабілізатори (ShuntRegulators) компенсаційні стабілізатори (LinearRegulator), до переліку яких входять і стабілізатори з малим падінням напруги на регулювальному елементі (Low-DropoutRegulator, LDO), та перетворювачі, що використовують імпульсний процес перетворення електричної енергії (SwitchingRegulators). Коефіцієнт корисної дії параметричних та компенсаційних стабілізаторів залежить від співвідношення вхідної та вихідної напруг, і шляхів для його підвищення принципово не існує. Тому для застосунків, критичних до рівня втрат енергії при перетворенні напруги, використовують лише імпульсні понижувальні перетворювачі.

Найбільш поширеною схемоюімпульсного понижувального перетворювача є схема, з одним джерелом живлення (рис. 1). Ця схема має високі техніко-економічні показники [1],однак дослідження, проведені в [2], показують, що використання двох джерел живлення дозволяє зменшити як рівень перетворювальної потужності, так і рівень динамічних втрат енергії – втрат енергії, що виникають при перемиканні силових комутувальних елементів *S1* та *S2*. Однак математичні моделі і програмне забезпечення для визначення параметрів цих перетворювачів у відомій технічній літературі практично відсутні. Це і обумовило мету цієї роботи, яка полягає у створенні математичної моделі електричних процесів понижувальних перетворювачів із двома джерелами живлення.

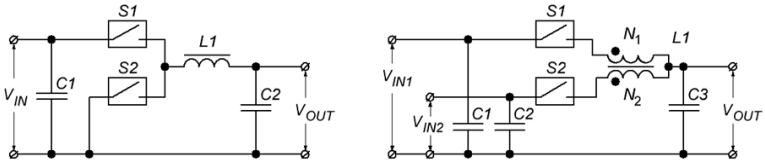


Рисунок 1 – Схеми імпульсних понижувальних перетворювачів напруги: з одним (ліворуч) та двома (праворуч) джерелами живлення

В імпульсних перетворювачах перетворення параметрів електричної енергії відбувається шляхом переміщення певної кількості енергії в магнітне поле індуктивних елементівіз подальшим поверненням її в електричну схему але вже з другими параметрами. Назвемо проміжок часу, необхідний для перетворення порції електричної енергії, *циклом перетворення*, який складається щонайменше з двох *етапів перетворення*. Різні етапи перетворення відрізняються різним станом комутувальних елементів, які можуть знаходитися або в замкненому або в розімкненому станах. Протягом етапу перетворення стан силових ключів не змінюється.

Електричні процеси, які відбуваються в перетворювачі із двома джерелами живлення наведено на рис. 2. У цій схемі, цикл перетворення складається з двох етапів. На першому етапі перетворення (Firststageofconversion), тривалість якого дорівнює t_1, обмотка дроселя *L1*із числом обвитківN_1через замкненийключ *S1*під'єднується до першого джерела живленняіз напругою V_{IN1}. Оскільки напруга V_{IN1} більша за вихідну напругу V_{OUT}, то полярність напруги $v_{N1}(t)$ на обмотці дроселя *L1*є позитивною, що призводить до зростання на величину $\Delta\Phi_1$ магнітного потоку ф(t) в магнітопроводі дроселя*L1* і, відповідно, до зростання на величину ΔI_1зв'язаного з ним струму $i_{N1}(t)$.

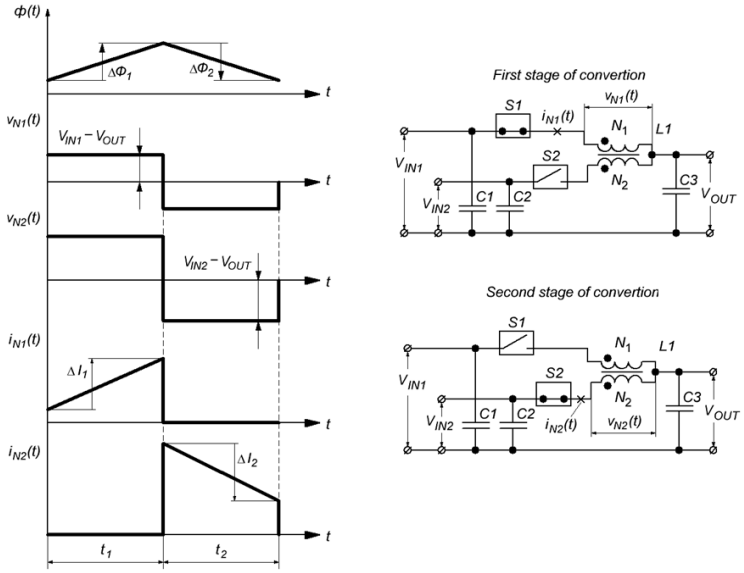


Рисунок 2 – Електричні процеси в силовій частині понижувального імпульсного перетворювач із двома джерелами живлення

На другому етапі перетворення (Secondstageofconversion), тривалість якого дорівнює t_2, обмотка дроселя *L1*із числом обвитківN_2через замкненийключ *S2*під'єднується до другого джерела живленняіз напругою V_{IN2}. Для того, щоб дросель *L1*почав віддавати енергію, накопичену на першому етапі перетворення, необхідно, щоб його магнітний потік почав зменшуватися. А це можливо лише коли напруга другого джерела живлення V_{IN2} буде менша за вихідну напругу V_{OUT}. У цьому випадку полярність напруги $v_{N2}(t)$ на обмотці дроселя *L1*стане негативною, що призведе до зменшення на величину $\Delta\Phi_2$ магнітного потоку ф(t) в магнітопроводі дроселя*L1* і, відповідно, до зменшення на величину ΔI_2 зв'язаного з ним струму $i_{N2}(t)$.

Головною умовою фізичної реалізації схем, наведених на рис. 1, є можливість роботи в квазістаціонарному режимі – коли у кожному циклі перетворення відбуваються тотожні електричні та енергетичні процеси. Вочевидь, це можливо лише за умови, коли кількість енергіїв дроселі *L1*, яка визначається величиною магнітного потоку ф(t), наприкінці циклу перетворення буде дорівнювати кількості енергії, яка в ньому знаходилася на початку, тобто:

$$\Delta\Phi_1 = -\Delta\Phi_2 . \tag{1}$$

Величини змін магнітного потоку $\Delta\Phi_{1(2)}$ можна обчислити, якщо відомі величини змін струмів $\Delta I_{1(2)}$, які відбуваються протягом етапів перетворення:

$$\Delta I_1 = \frac{V_{IN1} - V_{OUT}}{N_1^2 A_L} t_1, \qquad \Delta I_2 = \frac{V_{OUT} - V_{IN2}}{N_2^2 A_L} t_2, \tag{2}$$

де A_L – конструктивний параметр магнітопроводу дроселя *L1*.

На основі закону повного струму можна записати:

$$\Delta I_1 N_1 = -\Delta I_2 N_2 . \tag{3}$$

Після підстановки у формулу (3) формул (1) та (2) отримаємо формулу, що зв'язує співвідношення вхідних та вихідної напруг із параметрами процесу перетворення та параметрами силової частини:

$$V_{OUT} = \frac{V_{IN1} t_1 N_2 + V_{IN2} t_2 N_1}{t_1 N_2 + t_2 N_1} . \tag{4}$$

Головною перевагою понижувальних схем, наведених на рис. 1, є наявність електричного зв'язку вхідних та вихідних кіл, що дозволяє перетворювати лише частину енергії. Для понижувального перетворювача із двома джерелами живлення, величина перетворювальної потужності P_{CONV} – кількості енергії за одиницю часу, що проходить через магнітне поле дроселя *L1* – визначається наступною формулою:

$$P_{CONV} = P_{OUT} \frac{(V_{OUT} - V_{IN2})(V_{IN1} - V_{OUT})}{V_{OUT}(V_{IN1} - V_{IN2})} , \tag{5}$$

де P_{OUT} – вихідна потужність перетворювача.

Залежність відносної перетворювальної потужності перетворювача із двома джерелами живлення від співвідношення його вихідної та вхідних напруг наведено на рис. 3. Як видно з рисунку, якщо напруга другого джерела живлення дорівнює нулю ($V_{IN2} = 0$) то схема перетворюється у звичайний понижувальний перетворювач з одним джерелом живлення і його перетворювальна потужність визначається відомим формулами [1, 2].

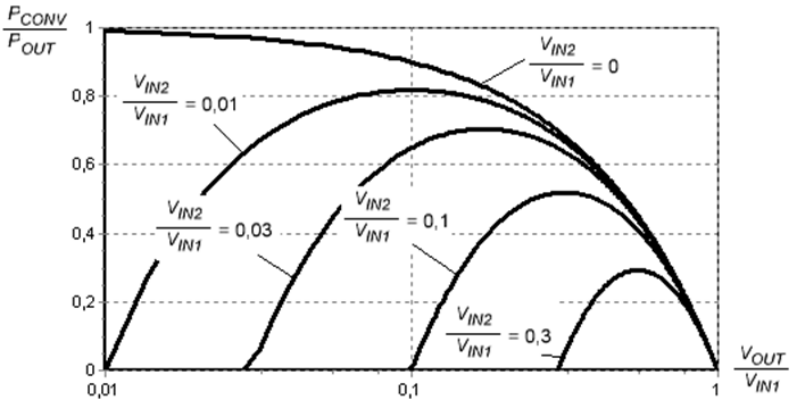


Рисунок 3 – Залежність відносної перетворювальної потужності перетворювача із двома джерелами живлення від співвідношення його вихідної та вхідних напруг

Введення додаткового другого джерела живлення з ненульовою напругою ($V_{IN2} \neq 0$) призводить до додаткового зменшення рівня перетворювальної потужності P_{CONV}. Таким чином, за однакої вихідної потужності P_{OUT} та однакових вхідної V_{IN1} та вихідної V_{OUT} напругах, введення додаткового джерела живлення, V_{IN2}, що задовольняє умові

$$V_{IN2} < V_{OUT} < V_{IN1}, \quad (6)$$

дозволить зменшити рівень перетворювальної потужності P_{CONV}, що, у свою чергу, призведе до покращення техніко-економічних показників перетворювача: маси, розміру, вартості, а також до можливого підвищення коефіцієнту корисної дії за рахунок зменшення динамічних втрат в силових ключах *S1*і*S2*, через те, що вони тепер будуть перемикатися при менших напругах.

Висновки. Процес отримання співвідношень розробленої математичної моделі є яскравим прикладом використання методів математичного моделювання апаратних вузлів комп'ютерної техніки, який доцільно використовувати в процесі підготовки фахівців в галузі інформаційних технологій та програмування. Запропоновану математичну модель, та отримані результати аналізу перетворювальної потужності можна використовувати для розрахунку параметрів імпульсних понижувальних перетворювачів електричної живлення із двома джерелами живлення, оскільки ці схеми можуть мати більш високі техніко-економічні показники, порівняно із відомими схемами з одним джерелом живлення.

Література

1. Zehendner M., Ulmann M. Power Topologies Handbook. Texas Instruments, 2016. 216c.

2. Kadatskyy A.F., Rusu A.P. Analysis of conversion power of switched-mode buck converters with two power sources.*Наукові праці ОНАЗ ім. О. С. Попова*. 2019, №2. С. 52-60.

УДК 372.862

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Меланич Ігор Володимирович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 014 Середня освіта
Міжнародний гуманітарний університет

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЛАТФОРМ ДЛЯ НАВЧАННЯ РОБОТОТЕХНІЦІ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Анотація.*Виконано порівняльний аналіз платформ для навчання робототехніці в закладах вищої освіти. Розроблено рекомендації щодо вибору платформ для закладів освітирізних рівнів. Показано що в закладах середньої та передвищої освіти для навчання робототехніці рекомендується використовувати платформу «Ардуіно», а в закладах вищої освіти – більш професійні рішення, наприклад, рішення компанії STMicroelectronics, оскільки вони забезпечують більш грунтовну підготовку здобувачів.*

Робототехніка зараз находиться в стадії бурхливого розвитку.Наразі в світі існуєсталий попит на фахівців, що розуміються на роботизованих пристроях, томупідготовка фахівців з робототехніки є актуальним питанням, що стоїть перед керівниками навчальних закладів усіх рівнів освіти. Популярність робототехніки призвела до того, що зараз майже всі виробники електронних компонентів пропонують свої набори та інструменти для розробки роботів. Велике різноманіття існуючих апаратних та програмних продуктів призводить до певних проблем із вибором методів навчання, що і обумовило мету цією роботи, яка полягає в порівнянні різних платформ для вивчення робототехніки.

Однією із найвідоміших платформ, яку можна використовувати в закладах освіти для навчання робототехніки, є платформа «Ардуіно»[1]. Головною перевагою цієї платформи є те, що вона з самого початку створювалась для навчання, робототехніці та електроніці. Тому для того, щоб почати знайомство із робототехнікою достатньо мінімального рівня знань як в галузі робототехніки, так і галузі програмування. Протеця платформа ізолює розробника роботів від наявних апаратних та програмних ресурсів, що потім стає суттєвою перешкодою на шляху подальшого професійного розвитку майбутнього фахівця. Тому платформу «Ардуіно» краще використовувати для навчання здобувачів змінімальним рівнем знань в галузях електроніки та програмування, наприклад, в закладах середньої, передвищої, у тому числі і фахової передвищої, освіти.

Рисунок 1 – Зовнішній вигляд роботів на основі платформи «Ардуіно»

На більш високих рівнях освіти слід відмовитися від використання платформи «Ардуіно» і перейти на більш продуктивні платформи, що забезпечують розробнику повний доступ до апаратних та програмних ресурсів комп'ютерних засобів. Однією із таких платформ є платформа, що надається компанією STMicroelectronics[2]. Ця компанія пропонуєзасоби розробки на основі 8- та 32-розрядних мікроконтролерів, які цілком придатні для створення роботів.

Перевагою цих мікроконтролерів є те що вони мають одне з найкращихспіввідношень ціна/продуктивність.Порівняльний аналізплатформ «Ардуіно» та STM8, що відносяться до початкового рівня освоєння електроніки та робототехніки, показує що мікроконтролери STM8 мають дещо гірші параметри по обсягу пам'яті програм, оперативної пам'яті та продуктивності (табл. 1). Однакціна цих мікроконтролерів відрізняється майже на порядок. Станом на 2024 рік, роздрібна ціна самого дешевого мікроконтролера STM8 в Україні становить близько 20 грн, у той час як мікроконтролер ATmega, що використовується в оригінальній платі «Arduino Nano» коштує приблизно 250 грн.

Таблиця 1 – Порівняльний аналіз платформ «Ардуіно» та STM8

	Arduino Nano	**STM8**
Мікроконтролер	ATmega328	STM8S003F3P6
Пам'ять програм	32 KB	8 KB
Оперативна пам'ять	2 KB	1KB
Пам'ять даних	1000 B	640 B
Швидкодія	~20 MIPS	~16 MIPS
Периферійні модулі	UART, TT, 3 таймери	SPI, I2C, UART, 4 таймери
Ціна мікроконтролера	250 грн	18 грн
Ціна плати для розбробки	923 грн	87 грн

Використання замість платформи «Ардуіно» рішень інших виробників (MicrochipTechnology [3], TexasInstruments [4], Renesas [5] тощо), відкриває розробнику повнийдоступ до усіх наявних ресурсів мікроконтролера, що дозволяє створювати

програмне забезпечення із можливостями, які на платформі «Ардуіно» створити доволі важко. Проте для опанування цих можливостей потрібен певний рівень знань в галузі робототехніки та цифрової схемотехніки. Тому використовувати більш складні і потужні платформи слідів закладах передвищої (на старших курсах) та вищої освіти, коли здобувачі вже мають певний рівень теоретичної та практичної підготовки.

Слід зауважити, що перехідна новий рівень стосується лише програмної частини – апаратна частина, що використовується для створення робота (двигуни, приводи, датчики тощо), не залежить від програмної платформи. Тому для переходу на більш розвинені програмні інструменти, у більшості випадків, достатньо лише замінити плату керування.

Висновки. В закладах середньої та передвищої освіти для навчання робототехніці рекомендується використовувати платформу «Ардуіно», оскільки вона дозволяє створювати роботів із мінімальним рівнем знань в галузях електроніки та програмування. В закладах вищої освіти для більш ґрунтовної підготовки здобувачів слід використовувати більш професійні рішення, наприклад, рішення компанії STMicroelectronics, мікроконтролери яких на сьогоднішній день мають найкраще співвідношення ціна/продуктивність.

Література

1. Офіційний сайт компанії Arduino. URL: https://www.arduino.cc/
2. Офіційний сайт компанії STMicroelectronics. URL: https://www.st.com/
3. Офіційний сайт компанії MicrochipTechnology. URL:https://www.microchip.com/
4. Офіційний сайт компанії TexasInstruments. URL: https://www.ti.com/
5. Офіційний сайт компанії Renesas Electronics. URL: https://www.renesas.com/us/en

УДК 621.314

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Холоша Ігор Віталійович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 014 Середня освіта
Міжнародний гуманітарний університет

ОСОБЛИВОСТІ НАВЧАННЯ НИЗЬКОРІВНЕВОМУ ПРОГРАМУВАННЮ ЗДОБУВАЧІВ В ГАЛУЗЯХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ТА РАДІОТЕХНІКИ

Анотація.*Розглянуто особливості навчання низькорівневому програмуванню здобувачів в галузях інформаційних технологій, електронних комунікацій та радіотехніки. Обґрунтовано використання для цієї задачі мікроконтролерів PICсереднього сімейства (PIC10, PIC12, PIC16) виробництва компанії Microchip Technology. Розглянуто можливість використання віртуальних лабораторних макетів для перевірки працездатності розробленого програмного забезпечення, що дало можливість вивчати низькорівневе програмування здобувачам, що навчаються за дистанційною формою навчання.*

Навчання програмуванню є важливою складовою підготовки фахівців в галузях інформаційних технологій, електронних комунікацій та радіотехніки. На сьогоднішній день, найбільш поширеними мовами для створення програмного забезпечення є мови високого рівня, наприклад, PythonабоC/C++, використання яких значно спрощує процес

створення програмного забезпечення та зменшує час написання програмного коду. Однак у деяких випадках, наприклад, при обмежених обсягах апаратної пам'яті, зумовлених необхідністю здешевлення кінцевого застосунку, або при жорстких вимогах до часу реакції системи на події, що відбуваються в реальному часі, «накладні витрати» мов високого рівня не дозволяють у повній мірі реалізувати технічне завдання та створити програмне забезпечення із необхідним функціоналом. У цих випадках програмісту доводиться опускатися на найнижчий рівень програмування – рівень машинних інструкцій, який дозволяє повністю контролювати час виконання програмного коду і апаратні ресурси комп'ютерної системи.

На жаль, створення коду на рівні апаратних інструкцій вимагає від програміста більш високого рівня концентрації та більш розвиненої уяви, оскільки у цьому випадку потрібно враховувати та контролювати більшу кількість апаратних та програмних об'єктів, що збільшує імовірність помилок, які важко знайти та виправити, та збільшує час написання програмного коду. Однак з іншого боку, перехід на найнижчий рівень програмування дозволяє здобувачу краще зрозуміти принципи побудови і функціонування комп'ютерних пристроїв та систем і, завдяки формуванню низки навичок, які дуже важко здобути при використанні мов високого рівня, істотно підвищити свій професійний рівень.

Таким чином, опанування методів низькорівневого програмування є, безумовно, корисним для майбутнього фахівця, однак для цього потрібно використовувати особливий підхід, оскільки здобувач може вже на початковому етапі втратити орієнтування в питаннях, що розглядаються на заняттях. Цей і обумовило мету цієї роботи, в якій розглядаються особливості навчання ниькорівневому програмуванню, які використовуються на факультеті кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету при підготовці здобувачів з галузях інформаційних технологій, електронних комунікацій та радіотехніки.

Особливості низькорівневого програмування найкраще вивчати та досліджувати на реальних застосунках, коли є можливість на власні очі побачити результат роботи програми та інструментально виміряти час її виконання. Тому в Міжнародному гуманітарному університеті низькорівневе програмування використовується на курсах, пов'язаних із вивченням застосунків, що працюють під керівництвом мікроконтролерів, наприклад, у курсі «Програмування мікроконтролерів для пристроїв інтернет речей», який використовується для підготовки здобувачів зі спеціальності 123 – Комп'ютерна інженерія. У цьому курсі перевірка працездатності низькорівневого програмного коду, створеного на мові асемблеру для мікроконтролерів, що вивчаються у курсі.

Використання мікроконтролерів для навчання низькорівневому програмуванню є одним із найкращих рішень, оскільки мікроконтролери в простих застосунках працюють у реальному часі без втручання операційних систем, які ізолюють програму від апаратних та програмних ресурсів, додаючи до часу виконання програми деякий довільний час, який важко прогнозувати. Крім того, більшість сучасних мікроконтролерів побудовані за архітектурою зі скороченим набором команд (ReducedInstructionSetComputing, RISC), що додатково зменшує час на здобуття необхідних навичок.

Кількість інструкцій для мікроконтролерів залежить від конкретної моделі і сімейства. Наразі для низькорівневого програмування можна використовувати мікроконтролери PIC та AVR виробництва компанії Microchip Technology [1] або STM виробництва компанії STMicroelectronics[2]. Порівняльний аналіз кількості машинних інструкцій цих мікроконтролерів (табл. 1) показує, що для первинного знайомства із низькорівневим програмуванням найкраще підходять мікроконтролери PICсереднього сімейства (PIC10, PIC12, PIC16), що мають до 35 машинних інструкцій.

Таблиця 1 – Кількість машинних інструкцій в різних типах мікроконтролерів

Виробник	Мікроконтролери	Сімейство	Кількість інструкцій
Microchip Technology	PIC	PIC10, PIC12	33
		PIC16	35
		PIC18	75
		PIC24	83
		dsPIC30	84
		dsPIC33	86
	AVR	ATtiny	89
		ATmega	133
STMicroelectronics	STM	STM8	80
		STM32	≈ 250

При вивченні низькорівневого програмування здобувач створює програмне забезпечення в будь-якому інтегрованому середовищі для розробки програмного забезпечення, що підтримує мікроконтролери, що розглядаються у курсі. Наприклад, для мікроконтролерів PICможна використовувати інтегроване середовище для розробки MPLAB X[3]. Після компіляції розробленого асемблерного коду створюється закодований файл («прошивка»), який або за допомогою програматора завантажується у мікроконтролер, підключений до реального електричної схеми, або завантажується у віртуальний аналог електронної схеми. Після подачі живлення схема починає працювати, що дає можливість здобувачеві перевірити працездатність створеного програмного забезпечення.

Використання замість фізичних макетів їх віртуальних аналогів (рис. 1) дозволяє вирішити проблему дистанційного навчання, коли у здобувачів немає фізичної можливості для відвідання спеціалізованих аудиторій, обладнаних необхідними для фізичного моделювання лабораторними макетами та вимірювальними приладами. Крім того, віртуальне моделювання дозволяє уникнути можливого фізичного пошкодження апаратної частини через помилки у програмі або підключенні мікроконтролера.

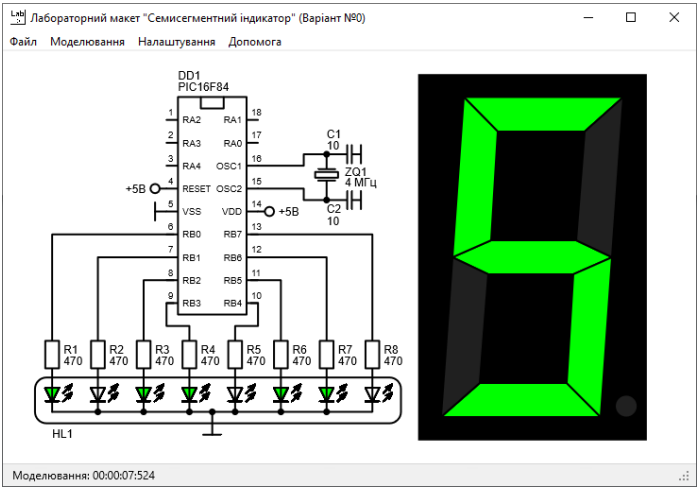


Рисунок 1 – Зовнішній вигляд віртуального лабораторного макету для перевірки працездатності низькорівневого програмного забезпечення

Передумовами для початку вивчення низькорівневого програмування є навички, отримані здобувачами на попередніх курсах. Перед початком вивчення курсу здобувачі вже повинні знати базові речі, що використовуються для створені програм: алгоритми, константи, змінні, безумовні та умовні переходи, цикли, умовну адресацію тощо. Крім того для покращення засвоєння навчального матеріалу необхідно щоб здобувачі мали досвід з програмування на будь-якій з мов високого рівня – це дозволить краще розуміти внутрішні механізми низькорівневого програмування.

Навчання низькорівневому програмування відбувається поступово – від простих програм до більш складних. На першому занятті здобувачі створюють найпростішу програму («Hello, world!»), головним завданням якої є опанування середовища для розробки та тестування програмного забезпечення та особливостями написання коду на асемблері. Після цього протягом курсу складність завдань збільшується, і здобувачам поступово показується як технічно реалізовуються об'єкти, які використовуються в мовах високого рівня: змінні, операції присвоєння, арифметичні та логічні операції, умовні та безумовні переходи тощо. Кінцевим результатом вивчення низькорівневого програмування є розуміння того, що рівень та мова програмування впивають лише на швидкість створення програмного коду та точність його роботи, а алгоритми та структура програми залишаються незмінними.

Висновки. Розроблений підхід до навчання низькорівневому програмуванню здобувачів в галузях інформаційних технологій, електронних комунікацій та радіотехніки показав свою працездатність та високий рівень розумінняяк серед здобувачів, так і серед викладачів. При цьому завдяки використанню віртуальних лабораторних макетів з'явилася можливість проводити заняття дистанційно без зниження якості навчання.

Література

1. Офіційний сайт компанії Microchip Technology. URL: https://www.microchip.com/
2. Офіційний сайт компанії STMicroelectronics. URL: https://www.st.com/
3. Integrated Development EnvironmentMPLAB X. URL: https://www.microchip.com/en-us/tools-resources/develop/mplab-x-ide