ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ
ГАЛИЦЬКИЙ КОЛЕДЖ ім. В. ЧОРНОВОЛА
КОМПАНІЯ «АРІКО»

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2019)

науково-практичної конференції

молодих вчених, аспірантів та студентів

Тернопіль

Збірник матеріалів наукової конференції «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2019). –Тернопіль. –2019. –170с.

Редакційна колегія:

Яцків В.В. – доктор технічних наук, доцент, завідувач кафедри кібербезпеки, ТНЕУ.

Николайчук Я.М. – доктор технічних наук, професор, завідувач кафедри спеціалізованих комп'ютерних систем, ТНЕУ.

Чешун В.М. - кандидат технічних наук , доцент кафедри комп'ютерних систем та мерех, ХНУ.

Муляр І.В. - кандидат технічних наук , доцент кафедри комп'ютерних систем та мерех, ХНУ.

Тимошенко Л.М. – кандидат економічних наук, доцент, кафедри інформатики та управління захистом інформаційних, ОНПУ.

Матіїшнн Ю.С. - відповідальний за добір персоналу, компанія «Apiko».

Івасьєв С.В.- кандидат технічних наук ТНЕУ.

Якименко І.З.- кандидат технічних наук, доцент, ТНЕУ.

Касянчук М.М.- кандидат фізико-математичних наук, доцент, ТНЕУ.

Яцків Н.Г. - кандидат технічних наук, доцент, ТНЕУ.

Сегін А.І.- кандидат технічних наук, доцент, ТНЕУ.

Стефурак Н.А. - кандидат фізико-математичних наук, Галицький коледж ім. В.Чорновола.

Гуменний П.В. - кандидат технічних наук, ТНЕУ.

Цаволик Т.Г.- кандидат технічних наук, ТНЕУ.

Волинський О.І.- кандидат технічних наук, Надвірнянський коледж НТУ.

Давлетова А.Я. – здобувач кафедри СКС, ТНЕУ.

Редактор коректор: Гуменний П.В.
Технічний редактор: Давлетова А.Я.

Адреса редакції:

Тернопільський національний економічний університет
кафедра кібербезпеки
вул. Чехова 8, м. Тернопіль 46000

Контактний телефон
тел. (0352) 50-17-87

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

СПЕЦІАЛІЗОВАНІ КОМП'ЮТЕРНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 004.855.5

В.В. Посвятовський

Тернопільський національний економічний університет

АЛГОРИТМ ПІДБОРУ ВІДЕОФІЛЬМІВ НА ОСНОВІ МАШИННОГО НАВЧАННЯ ТА ХМАРНИХ ОБЧИСЛЕНЬ

Вступ. На даний час, коли безмежно зростають обсяги інформації, що пропонуються для користувача, перед усім постає проблема фільтрації даних. Ця проблема особливо актуальна у надзвичайно прибутковій сфері розваг, коли необхідно запропонувати користувачу саме той контент, що, з високою ймовірністю, буде йому цікавим.

Великий вибір програмних методів та засобів реалізації задач по створенню рекомендаційних систем дає можливість ефективно та обґрунтовано обрати необхідні для вирішення визначеного кола завдань, а також на їх основі реалізувати систему з використанням прогресивних технологій . При функціонуванні подібних систем особливе значення надається організації збереження великих масивів інформації з допомогою надійних хмарних сервісів та можливість використання їх з різноманітних пристроїв. Безперервний розвиток програмних та апаратних засобів ставить до сучасних рекомендаційних систем високі вимоги щодо доступності модернізації та вдосконалення.

Таким чином, у будь-якій сфері, де користувачам пропонується контент в тому чи іншому вигляді, надання рекомендацій по його вибору – найважливіший елемент інформаційної системи..

Метою роботи є дослідження та розробка алгоритму підбору відеофільмів на основі машинного навчання та хмарних обчислень.

1. Дослідження вимог до алгоритмів для рекомендаційних систем

Важливе значення рекомендаційні системи відіграють в вирішенні питань максимального задоволення потреб споживачів. Тому суб'єкти ринку, інформаційного зокрема, докладають значних зусиль і коштів для дослідження, розвитку і удосконалення методів та засобів побудови рекомендаційних систем. Дослідження у напрямку розвитку і удосконалення методів та засобів побудови рекомендаційних систем проводять такі провідні компанії як Yahoo!, Google, Amazon. Розвиток

рекомендаційних систем в Україні відповідає, розпорядженню Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні»

Питання оптимального алгоритму для рекомендаційних систем, що віднайшли широке застосування в таких сферах як електронна комерція, соціальні мережі, веб-додатки тощо, де акцент робиться на користувача даних [1] є питомо актуальним.

Відповідний алгоритм для реалізації рекомендаційної систем дозволяє забезпечити пропонування необхідного контенту. Крім цього використання методів та засобів штучного інтелекту дозволить постійно покращувати якість рекомендацій за допомогою машинного навчання. При використанні в рекомендаційній системі хмарних обчислень можна отримати як високий рівень надійності, так і перспективності.. [3].

2. Розробка структури автоматизованої системи навігації на парковці

Відповідно до проведеного дослідження методів та засобів навчання нейронних мереж для побудови рекомендаційної системи для її реалізації було обрано трьохрівневу клієнт-серверну архітектуру на базі згорткової нейронної мережі з використанням хмарних обчислень[10].

На рисунку 1 наведена загальна структура рекомендаційної системи.

Рисунок 1 – Загальна структура рекомендаційної системи

Після вибору загальної архітектури системи, на основі проведеного попередньо аналізу було реалізовано алгоритм нейронної мережі, необхідний для забезпечення аналізу інформації та надання користувачу релевантних відповідей на запити. Проведене дослідження дає підставу використати бібліотеку Surprise, написану на мові програмування Python.

Дану реалізацію було перенесено в хмарну технологію Azure Machine Learning Studio. Ця технологія дає можливість використовувати набір готових модулів для обробки даних, роботи з зовнішними веб сервісами, також є набір готових алгоритмів для машинного навчання. Основною перевагою цього сервісу є використання віддалених апаратних ресурсів для виконання всіх операцій, що дає можливість заощадити на розгортанні локальної інфраструктури, необхідної для проведення обчислень.

Для взаємодії між фронтенд додатком та алгоритмом обробки даних застосовано веб сервіс, що приймає дані, які надходять від клієнта та передає їх на хмарний сервіс. Після цього, алгоритм проводить необхідні обчислення та повертає дані. Даний веб сервіс розроблено за допомогою ASP.NET Web, який спеціально призначений для роботи з REST (Representation State) –архітектурою.

Для реалізації серверної частини додатку обрано Microsoft Azure.— хмарну платформу та інфраструктуру корпорації Microsoft, що призначена для розробників застосунків хмарних обчислень для створення онлайнових застосунків та використання як в додатках, що працюють локально на комп'ютерах користувачів і додатків, які працюють в хмарі. Windows Azure дозволяє створювати застосунки як за допомогою Microsoft .NET Framework і Visual Studio, так і за допомогою інших інструментів. Операційна система працює на серверах Microsoft, доступ до неї можна отримати за протоколами HTTP, Representational State Transfer (REST), WS- і Atom Publishing Protocol (AtomPub).

Платформа Azure Services Platform включає п'ять основних компонентів. Це сама операційна система Windows Azure, що керує дисковим простором, застосунками і мережами, і Microsoft SQL Services для роботи з базами даних.

Також в платформу входять Microsoft .NET Services, Live Services, і бізнес-компонент, що включає Microsoft SharePoint Services і Microsoft Dynamics CRM Services.

Застосування концепції хмарних обчислень дає можливість використання обчислювальних потужностей, дискового простору і каналів зв'язку «обчислювальної хмари» для виконання трудомістких завдань. Навантаження між комп'ютерами, що входять в цю хмару, розподіляється автоматично. Більшість хмарних застосунків працюють у браузері.

Основою взаємодії з клієнтом є мобільний додаток. Для реалізації використано технологію розробки кросс-платформених додатків Xamarin — фреймворк для кроссплатформенної розробки мобільних додатків (iOS, Android) з використанням мови C #.

На рисунку.2 представлено програмний код, за допомогою якого реалізовано елементи користувацького інтерфейсу сторінки авторизації.

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
    android:orientation="vertical"
    android:layout_width="match_parent"
    android:layout_height="match_parent">
    <TextView
        android:text="Авторизація через Facebook"
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
        android:id="@+id/textView1"
        android:layout_marginLeft="100dp"
        android:layout_marginTop="200dp" />
    <Button
        android:text="Авторизуватись"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:id="@+id/auth_button"
        android:layout_marginLeft="120dp" />
</LinearLayout>
```

Рисунок 2 — Код сторінки авторизації

Висновки.

Часто пошукові системи повертають значно більше інформації, ніж користувач може обробити. З ростом обсягів даних, що зберігаються у мережі і пропонуються користувачу, зростає актуальність проблеми випередження запиту користувача шляхом пропонування йому потенційно цікавої інформації. Цю проблему розв'язують системи надання рекомендацій. Основна відмінність алгоритмів систем надання рекомендацій від алгоритмів пошуку даних полягає у пропонуванні

відповіді без явного запиту з боку користувача водночас, як пошукові алгоритми дають відповідь на конкретний запит користувача.

Провідні компанії-розробники пошукових систем (Yahoo!, Google) зазначають, що майбутнє всесвітньої мережі саме у системах надання рекомендацій[6].

Реалізований алгоритм рекомендаційної система підбору відеофільмів дозволяє інформувати користувача відповідно до його уподобань в обраній предметній області. Це допомагає в найкоротший час знайти необхідну інформацію в досліджуваній області за допомогою хмарних обчислень.

Подальше вдосконалення алгоритму та покращення якості рекомендацій дає можливість розвитку даної рекомендаційної системи та широкого розповсюдження.

Перелік джерел.

1. Adit Deshpande. A Beginner's Guide To Understanding Convolutional Neural Networks. URL: https://adeshpande3.github.io/A-Beginner%27s-Guide-To-Understanding-Convolutional-Neural-Networks/(дата звернення: 13.01.2019).

2. F. Chollet, Keras, URL: https://github.com/fchollet/keras, (дата звернення: 23.02.2019).

3. M. Abadi, A. Agarwal et al., "Tensorflow: Large-scale machine learning on heterogeneous distributed systems," arXiv preprint arXiv:1603.04467, Mar. 2016. URL: Available: https://arxiv.org/abs/1603.04467(дата звернення: 23.02.2019).

4. Model-based methods for recommender systems / [Stekh Y., Lobur M., Artsibasov V. // International Journal of Advanced Research in Computer Engineering & Technology – 2015. – v.4. – p.3061-3066

5. NicolasHug/Surprise. URL: https://github.com/NicolasHug/Surprise/ (дата звернення: 27.02.2019).

6. Гифт Ной. Прагматичный ИИ. Машинное обучение и облачный технологии: серия «Для профессионалов». СПб : Питер, 2019, 304с.

7. Згорткова нейронна мережа URL: http://uk.wikipedia.org/wiki/ (дата звернення: 13.01.2019)..

8. Іван Гудфелов, Йоша Бенгіо, Арон Коурвілле. «Машинне навчання» MIT Press, 2016. URL: http://www.deeplearningbook.org (дата звернення: 1.02.2019).

9. Классификация нейронных сетей. URL: http://www.aiportal.ru/articles/neural-networks/classification.html/ (дата звернення: 30.01.2019).

10. Посвятовський.В.В Дослідження актуальних методів та алгоритмів озпізнавання об'єктів. Галицький коледж імені В'ячеслава Чорновола. Дні науки 2019.: збірник наукових тез за матеріалами студентських науких читань :ернопіль: Навчально-виробнича майстерня редакційно-видавничих технологій Галицького коледжу імені В'ячеслава Чорновола, 2019. С. 86–89

11. Рекомендательные системы: Часть 1. Введение в подходы и алгоритмы [Електронний ресурс]. — Режим доступу:https://www.ibm.com/developerworks/ru/library/os-recommender1/(дата звернення: 10.03.2019).

УДК 519.7

С.М. Подганюк[1], Д.М. Безух[1], О.Й. Осадчук[2], О.О. Скриник[3]

[1]Тернопільський національний економічний університет

[2]Тернопільський обласний онкологічний диспансер

[3]Чортківська загальноосвітня школа І-ІІІ ступенів №7 Тернопільської області

ПРОГРАМНА ПІДСИСТЕМА ДИСКРЕЦІЙНОГО РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ. Бурхливий розвиток інформаційних технологій [1] призвів до інформаційної революції, внаслідок чого основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. За таких обставин забезпечення інформаційної безпеки (ІБ) поступово виходить на перший план у проблематиці національної безпеки [2].

З одного боку, використання інформаційних технологій дає ряд очевидних переваг: підвищення ефективності процесів управління, обробки і передачі даних і т.д. У наш час вже неможливо уявити велику організацію без застосування новітніх інформаційних технологій, починаючи від автоматизації окремих робочих місць і закінчуючи побудовою корпоративних розподілених інформаційних систем. З іншого боку, розвиток мереж, їх ускладнення, взаємна інтеграція, відкритість призводять до появи нових загроз [3], збільшенню числа зловмисників, які мають потенційну можливість впливати на систему.

Метою роботи є розробка програмної підсистеми дискреційного розмежування прав доступу в системах захисту інформації**.**

1. Визначення функцій програмної підсистеми та розробки схеми взаємозв'язку програмних модулів

Виходячи з мети роботи, спочатку необхідно визначити перелік функцій, які буде виконувати програмний продукт: установка прав доступу на відповідні каталоги, в яких розташовуються ресурси; перевірка виникнення нових каталогів, зокрема, каталогів співробітників установи; динамічне отримання користувачів і груп за допомогою аутентифікації користувачів.

У відповідності до цих функцій був розроблений алгоритм програмного засобу управління розмежуванням прав доступу, згідно якого працює програмний засіб: спочатку встановлюється час запуску програми, після чого програма очікує значення встановленого часу. Як тільки значення стає рівним заданому, то програма робить запит списку каталогів, розташованих на файловому сервері. При першому запуску створюється файл, що містить список каталогів на сервері. Його вміст порівнюється з отриманим результатом запиту. У випадку появи нових каталогів проводиться додавання в файл списку каталогів. Далі здійснюється запит для отримання списку користувачів і груп. Після цього проводиться зіставлення каталогів і користувачів. Результат зіставлення записується в окремий файл. Використовуючи результати зіставлення, записані в окремий файл, проводиться редагування списків. Схема зв'язку модулів та робочих файлів наведена на рисунку 1.

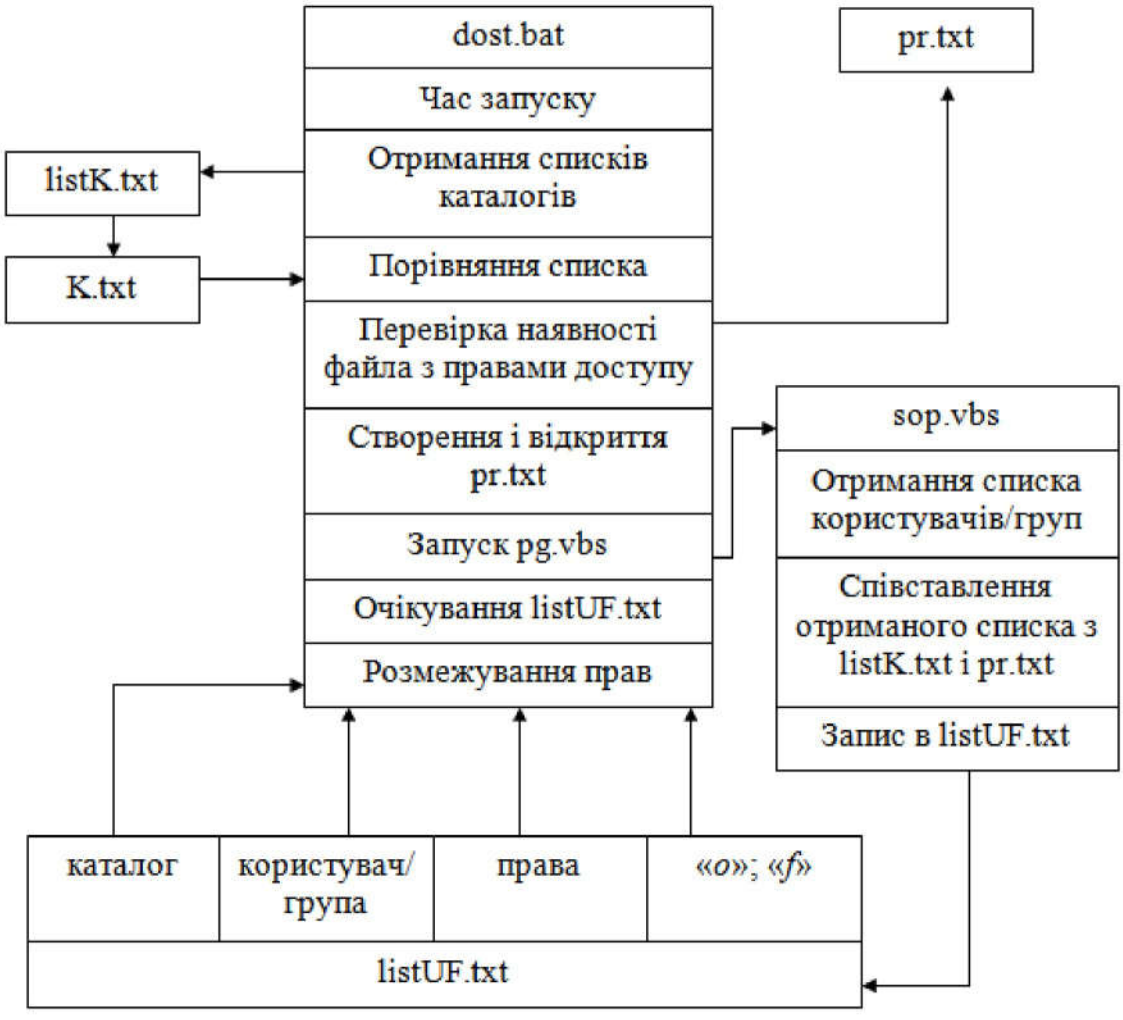


Рисунок 1 – Схема зв'язку модулів та робочих файлів

2. Інтеграція розробленого програмного засобу в існуючі комп'ютерні системи

Програмний засіб складається з двох взаємозв'язаних модулів: dost.bat - основна частина програмного засобу; sop.vbs - модуль отримання користувачів і груп з їх каталогами та правами доступу.

Модуль dost.bat являє собою основну частину програмного засобу. У цьому модулі реалізовані наступні функції програмного засобу для розмежування прав доступу:

1) установка часу запуску;

2) отримання списку каталогів на сервері і його порівняння з listK.txt;

3) розмежування прав доступу.

Основною особливістю програмного засобу являється відсутність інтерфейса і виконання функцій програмного засобу в фоновому режимі. Настройки програмного продукту встановлюються шляхом зміни відповідних значень вихідного коду і подальшого його збереження.

Програмний засіб не вимагає попередньої установки. Після першого запуску програмний засіб працює автономно і не вимагає додаткових маніпуляцій.

Інтеграція програмного засобу проходить в три етапи:

1) попереднє настроювання;

2) запуск програмного засобу;

3) перевірка появи робочих файлів.

Висновки.

Розроблена програму для дискреційної моделі розмежування прав доступу, яка характеризується більшою ефективністю в порівнянні з існуючими. Розроблено інструкції користувача та програміста для роботи з програмою дискреційної моделі розмежування прав доступу

Перелік джерел.

1. Бождай А.С. Сетевые технологии / А.С. Бождай, А.Г. Финогеев. - Пенза: Изд-во ПГУ, 2005. - 107 с.

2. Биячуев Т.А. Безопасность корпоративных сетей / Т.А. Биячуев. - СПб.: СПбГУ ИТМО, 2004. - 161 с.

3. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО ТИД Диа Софт, 2004. – 992 с.

УДК 004.056.5

***Д.Ю. Редванський*[1], *Н.М. Смольський*[1], *А.М. Гринчук*[1], *В.Я.Скриник*[2]**

[1]*Тернопільський національний економічний університет*

[2]*Чортківська загальноосвітня школа І-ІІІ ступенів №7 Тернопільської області*

МОДЕЛЬ ЗАХИЩЕНИХ ВЕБ-ТРАНЗАКЦІЙ НА ОСНОВІ ПРОТОКОЛУ SSL/TLS

Вступ. На даний час важко знайти установу, яка не була б під'єднана до Інтернету, що дає можливість скористатися його перевагами і ресурсами, включаючи обмін електронною поштою, поширення інформації серед зацікавлених осіб, проведення досліджень тощо. Приєднання до Всесвітньої павутини може дати досить значні переваги, хоча при цьому потрібно серйозно враховувати відповідні питання, пов'язані з безпекою з'єднання [1]. Тому опрацювання питань, пов'язаних з мережевою безпекою, зокрема, безпекою Web–транзакцій, та загрозами для протоколу SSL, знаючи принципи роботи якого та існуючі атаки можна забезпечити потрібний захист даних, є актуальною задачею.

Метою роботи є розробка моделі захищених веб-транзакцій на основі протоколу SSL/TLS, а також дослідження особливостей встановлення та налаштування SSL-з'єднання.

1. Особливості встановлення SSL-з'єднання

Протокол SSL знаходиться на рівні додатків моделі TCP/IP. Завдяки цьому SSL може бути розгорнутий майже на будь-якій операційній системі, що підтримує TCP/IP, без будь-якої правки ядра системи або TCP/IP стека. В результаті SSL має переваги перед іншими протоколами, такими як IPSec (IP Security Protocol), який вимагає підтримки модифікованого TCP/IP стека ядром системи [2]. Крім того, SSL легко пропускають брандмауери, проксі і NAT (Network Address Translation - перетворення мережних адрес).

На рисунку 1 показаний спрощений покроковий процес установки SSL-з'єднання між клієнтом (зазвичай, веб-браузер) і сервером (найчастіше, SSL веб-сервер). Процес установки кожного нового SSL-з'єднання починається з обміну параметрами шифрування, а потім (опційно) відбувається аутентифікація серверів (через SSL

Handshake Protocol - рукостискання). Якщо «рукостискання» вдалося і обидві сторони погодилися на один і той же алгоритм і ключі шифрування, то дані програми (зазвичай, HTTP) можуть бути передані по зашифрованому каналу (використовується SSL

Record Layer).

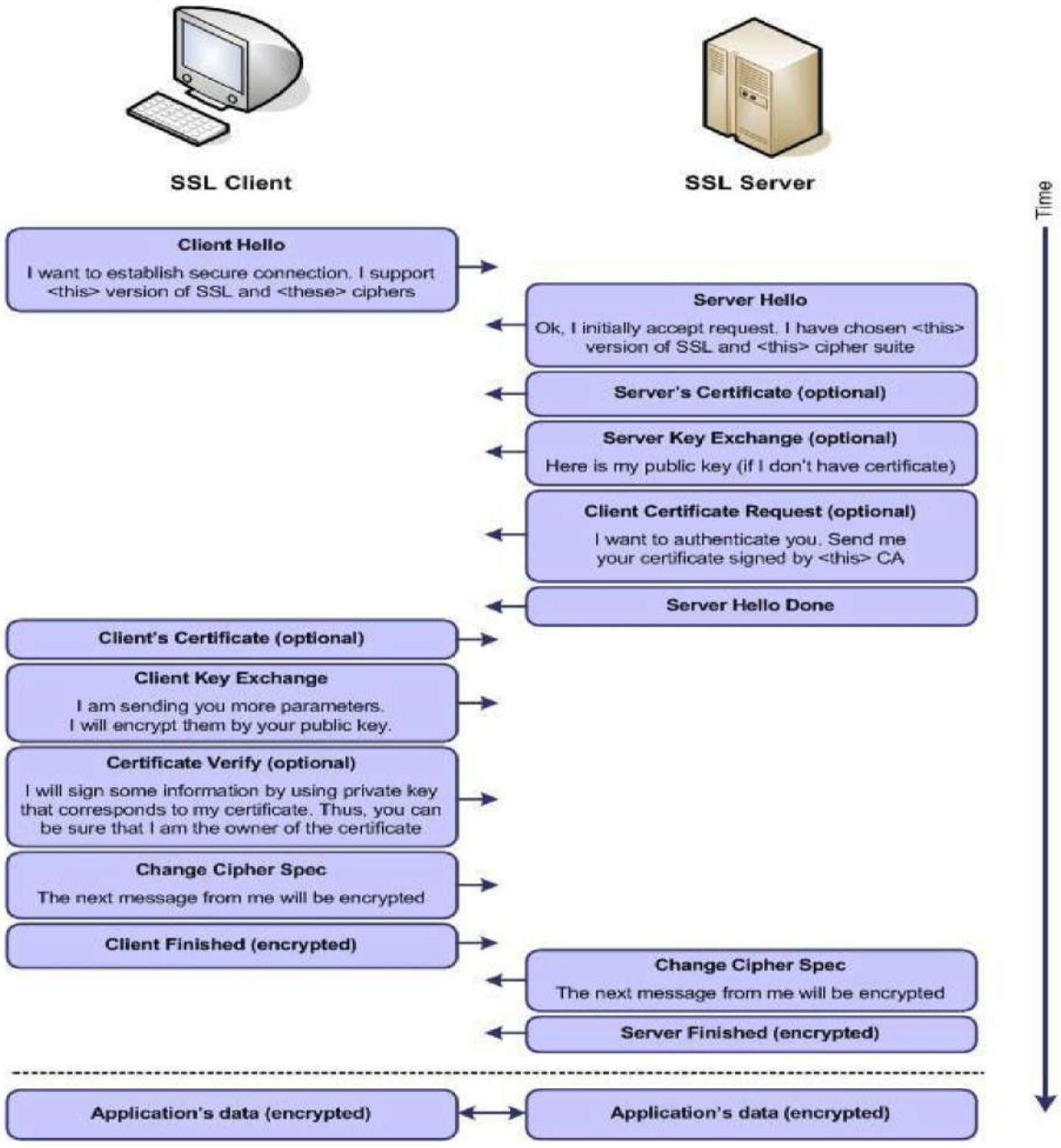


Рисунок 1 – Покрокова установка SSL-з'єднань

Якщо розглядати реальну ситуацію, то процес, описаний вище, виглядає набагато складніше. Щоб уникнути непотрібних «рукостискань», деякі параметри шифрування кешуються. При цьому можуть бути надіслані попереджувальні повідомлення. Також можуть бути змінені блоки шифру. Першим кроком у встановленні сервера з

підтримкою SSL/TLS є настройка і установка веб-сервера та створення користувача і групи з відповідним ім'ям. Далі потрібно включити mod_ssl і mod_setenvif для сумісності з деякими версіями MS Internet Explorer.

Потім треба підготувати структури директорії для приватних ключів веб-сервера, сертифікатів та списків анульованих сертифікацій (CRLs - certification revocation lists). Далі створюється самопідписаний серверний сертифікат, який використовується тільки для тестів, оскільки справжній сертифікат має бути від достовірного центра сертифікації, (наприклад, Verisign).

2. Запуск веб-сервера з підтримкою SSL/TLS

Після запуску сервера з підтримкою SSL/TLS веб-браузер потрібно направити на URL: https://ім'я сервера. Через деякий час повинно з'явитися попереджувальне повідомлення проте, що в ході перевірки аутентифікації веб-сервера виникла проблема.

Якщо не можна отримати доступ до веб-сайта, то можна скористатися корисною утилітою "s_client" від бібліотеки OpenSSL. Вона має багато корисних опцій, наприклад, включення/виключення окремого протокола (-ssl2, -ssl3, -tls1), вибір окремого алгоритма шифрування (-cipher), запуск режиму налаштування (-debug), перегляд статистик і повідомлень SSL/TLS (-state, -msg) і деякі інші, які зможуть допомогти знайти причину несправності. Крім того, можна використати Ethereal или ssldump. Завдяки цим утилітам відбувається пасивне спостереження SSL-повідомлення «рукостискань».

Висновки.

Досліджено процес встановлення та налагодження SSL-з'єднання, а також налаштування сервера на основі протоколу SSL/TLS при використання клієнтських сертифікатів для захисту від можливих криптоаналітичних атак. Запропонована система дає змогу обгрунтувати вибір відповідного методу захисту від криптоаналітичної атаки на протокол SSL/TLS.

Перелік джерел.

1. Васильев Г.А. Политика безопасности при работе в Internet / Г.А. Васильев. – СПб.: Питер, 2007. – 848 с.

2. Дейт К. Протокол TSL / К. Дейт. – СПб.: Питер, 2008. – 241 с.

УДК 004.056.53

***В.А. Черняк*[1], *А.Г. Стоян*[1], *Г.В. Сеньків*[2], *І.А. Сеньків*[2]**

[1]*Тернопільський національний економічний університет*

[2]*Іванівська загальноосвітня школа І-ІІІ ступенів Теребовлянського району Тернопільської області*

АЛГОРИТМ ПРОТИДІЇ СКАНУВАННЮ ПРОГРАМНИХ ЗАСОБІВ НА ОСНОВІ ЕЛЕКТРОННОГО КЛЮЧА

Вступ. На даний час необхідність використання різного роду систем для захисту програмного продуктів (ПП) зумовлена рядом причин, серед яких виділяються такі, як незаконне їх використання, що є інтелектуальною власністю виробника, несанкціонований доступ, використання та модифікація програмного забезпечення, незаконне його поширення та збут [1].

Вирішення задачі розробки математичних моделей для оцінки стійкості до злому ПП має певні труднощі [2]. По-перше, необхідно відзначити, що, як правило, відсутні строго адекватні моделі і методи оцінки таких систем. Практика показує, що методи оцінки переважно створюються для кожної моделі індивідуально, що дозволяє враховувати різні аспекти використання. По-друге, частина інформації, необхідна для розробки способів протидії засобам сканування, недоступна із-за недокументованості коду операційної системи. У зв'язку з цим задача розробки надійних програмних систем захисту інформації (ПСЗІ) є актуальною.

Метою роботи є розробка, реалізація та дослідження алгоритму протидії скануванню програмних засобів на основі електронного ключа.

1. Алгоритм протидії скануванню програмних засобів

Стійкість до злому ПСЗІ багато в чому визначається стійкістю до злому програмної підсистеми захисту логіки роботи (ППЗЛР), яка є складовою будь-якої ПСЗІ. На рисунку 1 показано структуру програмної підсистеми захисту логіки роботи і місця впровадження розроблених способів протидії.

Стрілки схеми показують місця впровадження розроблених способів протидії в ППЗЛР. Для протидії відладчикам режиму ядра використовується структурна обробка виключень. Всі відладчики використовують для своєї роботи, принаймні, два вектори переривань: перший і третій. Отже, для успішної протидії необхідно використовувати цей факт.

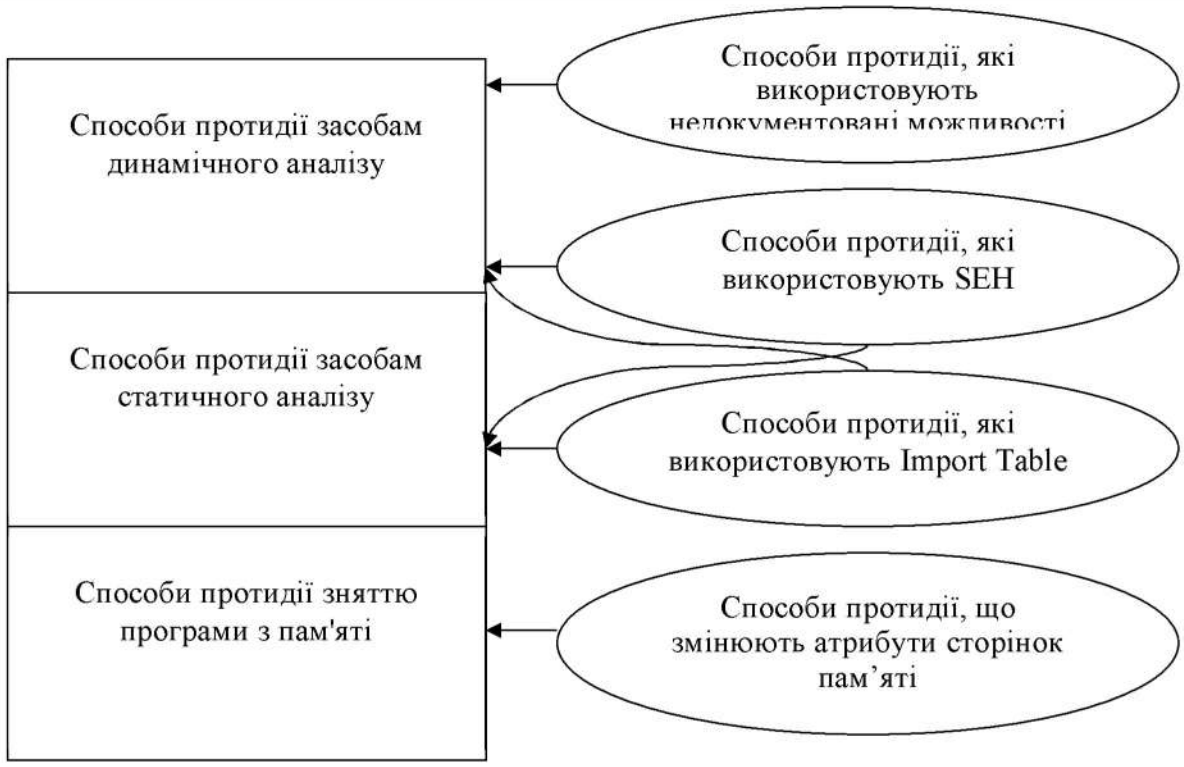


Рисунок1 – Структура програмної підсистеми захисту логіки роботи і місця впровадження розроблених способів протидії

Розроблені способи протидії засобам сканування можуть бути реалізовані у вигляді електронного ключа, який запобігає незаконному використанню і прихованому скануванню програми.

2. Розробка електронного ключа для протидії скануванню програмних засобів

Електронний ключ – це пристрій, який під'єднується до одного з портів комп'ютера, зазвичай до LPT або USB. Пам'ять електронного ключа містить інформацію про його характеристики, а також дані користувача. Алгоритм роботи електронного ключа наступний: при запуску і в процесі роботи захищена програма передає електронному ключу інформацію, так званий "запит"; електронний ключ її обробляє і повертає назад – "відповідь"; програма на основі повернених даних ідентифікує ключ.

Роботу пристрою можна представити таким чином. По передньому фронту імпульсу починається відлік. Під час вступу заднього фронту імпульсу або перевищенні заданого інтервалу часу відлік зупиняється, що відбувається при невірному значенні відповіді на запит програми. Якщо значення в лічильнику перевищує задану межу, на панелі відображення виводиться сигнал «помилка».

До складу структурної схеми (рисунок 2) входять наступні елементи: детектор фронтів; схема підрахунку тактових імпульсів; тактовий генератор; схема перетворення паралельного коду в послідовний; схема відображення.

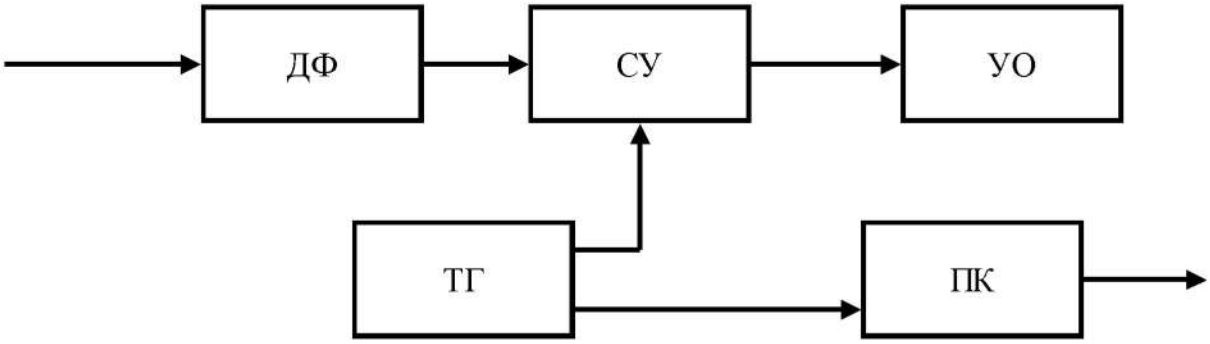


Рисунок 2 – Структурна схема електронного ключа

Під час вступу переднього фронту вимірюваного імпульсу детектор фронтів (ДФ) формує керуючий сигнал на початок відліку. Сформовані тактовим генератором (ТГ) імпульси поступають на схему підрахунку тактових імпульсів (СУ). Під час вступу заднього фронту вимірюваного імпульсу ДФ формує сигнал, який зупиняє відлік. При цьому кількість підрахованих імпульсів виводиться на схему відображення (УО) і через схему перетворення паралельного коду в послідовний (ПК) в пристрій обробки.

Проведене тестування показало високу ефективність розроблених способів протидії. Падіння швидкодії після впровадження розроблених способів протидії складає всього 3.1%. Проведений на основі розробленої математичної моделі розрахунок показав, що ефективність протидії засобам сканування при використанні розроблених способів протидії збільшується на 20%.

Висновки.

Запропоновані алгоритм та система протидії несанкціонованому скануванню програмних засобів на основі електронного ключа дозволяє збільшити ефективність роботи системи в порівнянні з аналогами.

Перелік джерел.

1. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. - СПб.: БХВ-Петербург, 2006. - 384 с.

2. Гаврилин Ю.В. Преступления в сфере компьютерной информации: квалификация и доказывание / Ю.В. Гаврилин. - М.: Высшая школа. - 2016. - 240 с.

УДК 681.32

М.Л. Глинська[1], Д.В. Лісковецький[2], С.В. Івасьєв[2]

[1]Галицький коледж ім. В. Чорновола

[2]Тернопільський національний економічний університет

АЛГОРИТМ КОДУВАННЯ ПРОСТИХ БАГАТОРОЗРЯДНИХ ЧИСЕЛ

Вступ. При реалізації алгоритмів опрацювання багаторозрядних простих чисел в задачах вибору системи взаємно простих модулів для процесорів теоретико-числових базисів (ТЧБ) Крестенсона, пошуку найбільшого спільного дільника, виявлення квадратичного лишку, виконання арифметичних операцій модульної арифметики виникає необхідність зберігання та генерування великих масивів багаторозрядних простих чисел. Генерування та зберігання багаторозрядних простих чисел, представлених повнорозрядними двійковими кодами, є неефективним у зв'язку з тим, що потребує великих об'ємів пам'яті.

1. Дослідження розподілу простих чисел.

Теорема про розподіл простих чисел стверджує, що кількість $\pi(n)$ простих чисел на відрізку від 1 до n зростає із зростанням n, як $\frac{n}{\ln n}$, тобто $\frac{\pi(n)}{n/\ln n} \to 1,\ n \to \infty$. Оцінка об'ємів пам'яті згідно наведеної теореми приведена в таблиці 1.

Таблиця 1 – Верхня оцінка розподілу простих чисел

Розрядність	Кількість	Об'єм пам'яті
2^8	64	64 байти
2^{10}	256	2 КБ
2^{16}	16384	32 КБ
2^{32}	1073741824	4 Гб
2^{64}	4611686018427387904	36 Гб
2^{128}	8,5070591730234615865843651857942e+37	2^{213} Терабайт
2^{256}	2,894802230932904885589274625217 2e+76	2^{426} Йотабайт
2^{512}	3,351951982485649274893506249551 5e+153	*
2^{1024}	4,494232837155789769323262976972 6e+307	*

Зростання верхньої оцінки об'єму пам'яті для повнорозрядного зберігання простих двійкових чисел показано на рисунку 1.

Побудований графік із змінною шкалою, в якому відображені верхні оцінки необхідного об'єму для збереження простих чисел.

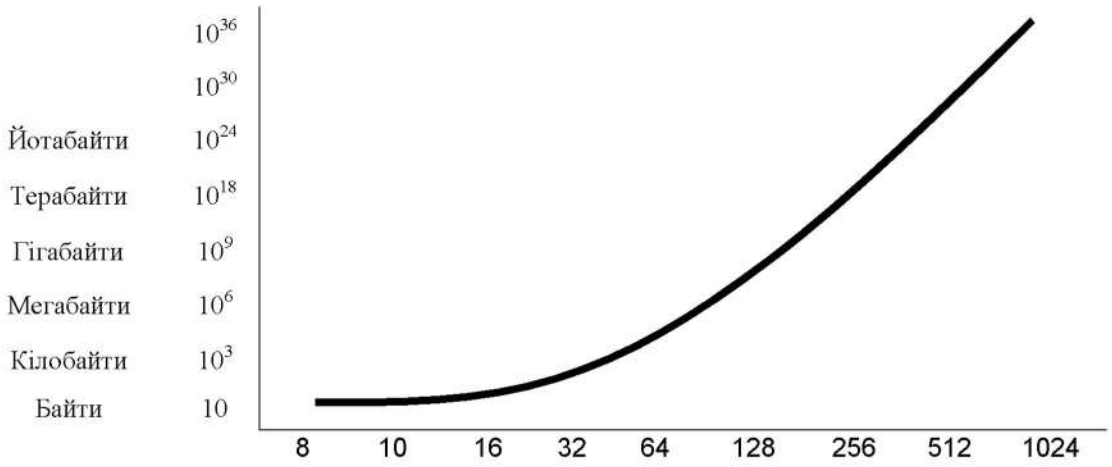


Рисунок 1 - Оцінка об'єму пам'яті для повнорозрядного зберігання простих двійкових чисел

З графіка видно, що об'єм пам'яті, необхідний для зберігання n-розрядних простих чисел до 32 розрядів, становить 4 Гб , для 64 розрядів - 36 Гб, а при 128 - 2^{213} Терабайт, оскільки при опрацюванні окремих задач теорії чисел розрядність простих чисел може сягати 512 біт, що відповідає надзвичайно великим об'ємам необхідної пам'яті, тому актуальною є наукова задача більш компактного зберігання великих масивів багаторозрядних простих чисел.

Можливість більш компактного зберігання простих багато розрядних чисел (БРЧ) може бути реалізована за рахунок надлишковості багаторозрядних двійкових кодів, оскільки різниця між двома простими БРЧ може не перевищувати 10-20 біт. Причому інформативна частина простого числа знаходиться в 20-30 бітах молодших розрядів при ідентичності сотень старших бітів, починаючи з 32 -64 біт. Для прикладу візьмемо числа з інтервалу $2^{20} \div 2^{64}$:

1052629_{10} =10000000111111010101 (2^{20});

2147487701_{10}=10000000000000000000111111010101 (2^{32});

9223372036854779861_{10}=10000000000000000000000000000000000000000000000000000000111111010101(2^{64});

При цьому в двійкових кодах багаторозрядних простих чисел (БРПЧ)

при активній зміні бітів молодших розрядів в старших розрядах велике число одиниць або нулів може обчислюватись тисячами, що є основою методу компактного кодування БРПЧ. В роботах [1, 2] запропонований метод компактного кодування БРПЧ, суть якого полягає в тому, що в пристроях пам'яті запам'ятовується певне число молодших розрядів, а 1 біт використовується для ідентифікації наскрізних переносів у старші розряди, а коди старших розрядів визначаться шляхом підрахунку числа переносів, які ідентифіковані бітом синхронізації, розподіл якого в середньому до 20 простих чисел. Тобто у діапазоні до 2^{1024} буде знаходитись 2^{51} бітів синхронізації.

Таблиця 2 – Послідовність простих чисел з однаковим закінченням

4194389 100000000000 0000101 0101	4195493 100000000000 1001010 0101
4194581 100000000000 0010001 0101	4195573 100000000000 1001111 0101
4194661 100000000000 0010110 0101	4195589 100000000000 1010000 0101
4194677 100000000000 0010111 0101	4195621 100000000000 1010010 0101
4194917 100000000000 0100110 0101	4195861 100000000000 1100001 0101
4195157 100000000000 0110101 0101	4195973 100000000000 1101000 0101
4195189 100000000000 0110111 0101	4196149 100000000000 1110011 0101
4195253 100000000000 0111011 0101	4196341 100000000000 1111111 0101

Висновки.

Таким чином, для зберігання об'єму простих чисел розрядністю до 1024 за попередніми оцінками потрібно 1048576 байт. Для збереження цілого числа в двійковій системі використовуються всі байти, які несуть значення числа. В результаті проведених досліджень та аналізу переліку простих чисел отримано результати, які свідчать про те, що числа з однаковими молодшими бітами можна представити у вигляді трьох частин. Їх розміри залежать від розрядності простого числа та кількості бітів в обраному закінченні (таблиця 2).

Перелік джерел.

1. Івасьєв С.В. Метод зберігання простих великорозрядних чисел у базисі Радемахера / С.В. Івасьєв, М.М. Касянчук, І.З. Якименко // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2013. – С. 142-144.

2. Gbolagade K.A. Residue Number System Operands to Decimal Conversion for 3-Moduli Sets, / K.A.Gbolagade, S. D. Cotofana // Proceedings of 51st IEEE Midwest Symposium on Circuits and Systems (MWSCAS-08). - Knoxville, USA.,2008. - P. 791-794.

3. Івасьєв С.В. Метод організації компактної бібліотеки простих чисел великої розрядності / С.В. Івасьєв //Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління» (ICSM) – Тернопіль, 2014. – С. 86-89.

УДК 681.3

Д.І. Подедвірний[1], Г.В. Якименко[2], А.В. Кипибіда[3]

[1]Тернопільський національний економічний університет,

[2]Медичний центр "Клініка професора Хміля",

[3] Тернопільська загальноосвітня школа І-ІІІ ступенів ім. В. Левицького №16

УЗАГАЛЬНЕНА МОДЕЛЬ ФУНКЦІОНУВАННЯ БЕЗПІЛОТНИХ ТРАНСПОРТНИХ ЗАСОБІВ

Вступ. Існуючі дослідження в галузі забезпечення цілісності інформації спрямовані в першу чергу на верхні рівні моделі OSI. При такому підході, питання, пов'язані із забезпеченням цілісності на нижніх рівнях моделі OSI, протидія різних перешкод, робота з особливостями фізичного середовища передачі даних, особливості адресації повідомлень, не розглядаються в більшості досліджень.

Дослідження в області забезпечення цілісності інформації груп безпілотних транспортних засобів (БТЗ) приймають за допущення, що цілісність повідомлень на нижніх рівнях моделі OSI забезпечується шляхом застосування традиційних методів і протоколів. Розглядаються питання, пов'язані з подальшою обробкою повідомлень, а в якості основи групи БТЗ розглядаються мережі стійкі до розривів, що гарантує не тільки доставку повідомлень, а й відсутність порушень синтаксичної цілісності в них. Однією з основних завдань є протидія порушенням семантичної цілісності інформації. Існуючий науково-методичного апарат (НМА) в даній області не дозволяє гарантувати відсутність порушень семантичної цілісності інформації.

Метою роботи є дослідження узагальненої моделі функціонування транспортних засобів.

1. Узагальнена модель функціонування безпілотних транспортних засобів

Розглянемо групу БТЗ, що складається з n елементів:$E = \{e_0, \dots, e_n\}$. $\forall_e \in E$ характеризується набором властивостей $P = \{p_0, \dots, p_m\}$, при цьому $P \neq \emptyset$. Співвідношення властивостей елементів дозволяє говорити про однорідність елементів. Нехай $e_t, e_j \in E, i \neq j$, тоді:

1. $P_i = P_j \Leftrightarrow e_i$ і e_j – гомогенні;

2. $P_i \subset P_j \Leftrightarrow e_j$ розширює і доповнює властивості та функції, які характеризують елемент e_i;

3. $P_i \cap P_j = \emptyset \Leftrightarrow e_i$ та e_j – гетерогенні.

Співвідношення властивостей 1-3 вірні тоді і тільки тоді, коли серед розглянутих властивостей відсутні властивості просторових характеристик.

Крім того, з точки зору інформаційного впливу (ІВ), можна виділити базові властивості зв'язку (Peon), характерні для всіх БТЗ:

- отримання;
- перетворення;
- передача;
- зберігання.

Виходячи з існуючих теоретичних розробок [1-5], вірне твердження:

$$\forall e_i, e_j \in, i \neq j \Rightarrow P_{con_i} = P_{con_j}.$$

Отже, співвідношення 3 не виконується, якщо розглядати серед усіх властивостей властивості зв'язку БТЗ. Крім того, можна говорити про гомогенність БТЗ з точки зору ІВ.

Кожен БТЗ виконує дві базові функції:

- обчислювальні функції;
- виконавчі функції.

Обчислювальні функції - функції, що дозволяють виробити план дій, необхідних для виконання завдань / переміщення в просторі. Виконавчі функції - функції, що дозволяють виконати завдання, ґрунтуючись на раніше розроблений план. Таким чином, обчислювальний пристрій кожного БТЗ виробляє план дій, який виконується відповідними фізичними пристроями БТЗ (двигун, осі і т.д.).

Можна уявити БТЗ наступним чином

$$-e_i = e_i^{inf} \cup e_i^{phy},$$

де e_i^{inf} - обчислювальні пристрої (ОП) БТЗ e_i, e_i^{phy} - фізичні пристрої (ФП) БТЗ e_i. Варто відзначити, в залежності від способу реалізації БТЗ внутрішні елементи можуть бути представлені як одним пристроєм, так і безліччю. В такому випадку, графічне представлення групи демонструється на рисунку 1.

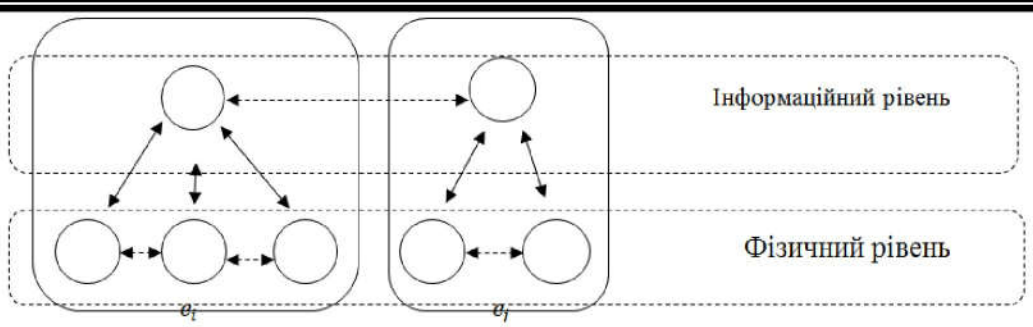


Рисунок 1 – Графічне представлення групи БТЗ з поділом кожного ТЗ на обчислювальні і фізичні пристрої

Пунктирні стрілки - ІВ пристроїв одного рівня, суцільні стрілки - ІВ елементів різних рівнів $\forall e_i, e_j \in E, i \neq j$ здійснюють ІВ $\Rightarrow \exists C_{i_j}$ - стійкий канал зв'язку. Необхідність існування стійкого каналу для здійснення ІВ є обов'язковою умовою функціонування групи БТЗ згідно роботам [161-165]. При цьому стійкий канал зв'язку повинен існувати між ОП різних БТЗ, а між фізичним пристроєм (ФП) канал передачі повідомлень може не існувати. Крім того, кожен ОП має канал зв'язку як мінімум з одним ФП.

Припустимо, $e_i \in E$ тоді $\forall e_j \in E, i \neq j$ і $\exists C_{i_j} \Leftrightarrow e_j \in E_{nei_{e_i}}$, де $E_{nei_{e_i}}$ – множина БТЗ-сусідів, що мають можливість здійснювати безпосередню ІВ з БТЗ e_i. Тоді $E_{nei_{e_i}} \subseteq E$. Якщо $E_{nei_{e_i}} = E$, то e_i може здійснювати ІВ з будь-яким БТЗ. Якщо група БТЗ є повнозв'язною, то $|E| = \left|U_{i=0}^{n} E_{nei_{e_i}}\right|$, зворотне – неправильно. При цьому розглядається лише взаємодія між ОП різних БТЗ.

Грунтуючись на вищенаведених тезах, можна представити групу БТЗ у вигляді графа *G(E)*, де $\{e_i\}$ – множина вершин графа ($e_i \in E$), $\left\{C_{i_j}\right\}$ – множина стійких каналів зв'язку між $e_i, e_j \in E$. Графічне представлення графів приведено на рисунку 2.

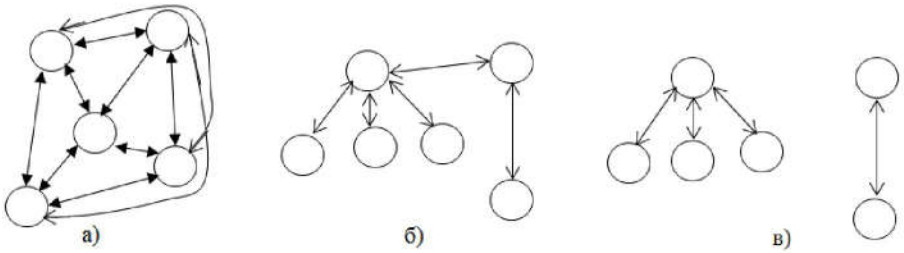


Рисунок 2 – Граф на основі групи БТЗ. Стрілки - стійкий канал зв'язку між ОП, кола – БТЗ а) і б) - графи на основі повнозв'язних груп БТЗ, в) - граф на основі груп БТЗ без повного зв'язку.

Таким чином, якщо група БТЗ є повнозв'язною, то G (E) є зв'язковим, тобто $\forall e_i, e_j \in E, i \neq j \exists \langle e_i, e_j \rangle$ - шлях від вершини e_i до вершини e_j (рисунок 2 а) і б)).

Проте не кожна група БТЗ є повнозв'язною (рисунок 2 в)), отже, між БТЗ не завжди існує можливість здійснити ІВ. Якщо не існує шляху, який зв'язує будь-які два елементи системи, слід говорити про наявність підгруп в рамках групи БТЗ, заснованих на можливості ІВ.

$E_{sub} \subseteq E$- підгрупа групи БТЗ $\Leftrightarrow \mathrm{E_{sub}} \neq 0$ i $\forall \mathrm{e_i, e_j} \in \mathrm{E_{sub}}, \mathrm{i} \neq \mathrm{j} \exists \langle \mathrm{e_i, e_j} \rangle$, при цьому $\nexists \langle \mathrm{e_i, e_k} \rangle \forall \mathrm{e_k} \in \mathrm{E}$ i $\mathrm{e_k} \notin \mathrm{E_{sub}}$. Отже, $E = U_{sub=1}^{k} E_{sub}$,

де k - кількість підгруп групи БТЗ. Крім того, повнозв'язна група БТЗ має тільки одну підсистему, що виділяється по можливості ІВ.

Висновки.

Запропоновано модель функціонування групи БТЗ на основі децентралізованої мультиагентної системи. В рамках запропонованої моделі група БТЗ розглядається як однорангова мережа з точки зору ІВ

Перелік джерел.

1. Zhao W., Ammar M., Zegura E. Controlling the mobility of multiple data transport ferries in a delay-tolerant network //INFOCOM 2005. 24th annual joint conference of the IEEE computer and communications societies. Proceedings IEEE. – IEEE, 2005. – Т. 2. – С. 1407-1418

2. Burgess J. et al. Maxprop: Routing for vehicle-based disruption tolerant networks //INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings. – IEEE, 2006. – С. 1-11.

3. Fall K. A delay-tolerant network architecture for challenged internets //Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. – ACM, 2003. – С. 27-34.

4. Farrell S. Endpoint Discovery and Contact Graph Routing in Space and Terrestrial DTNs //Advanced satellite multimedia systems conference (ASMA) and the 11th signal processing for space communications workshop (spsc), 2010 5th. – IEEE, 2010. – С. 89-93.

5. Pereira P. R. et al. From delay-tolerant networks to vehicular delaytolerant networks //IEEE Communications Surveys & Tutorials. – 2012. – Т.14. – №. 4. – С. 1166-1182.

6. Botelho S. C., Alami R. M+: a scheme for multi-robot cooperation through negotiated task allocation and achievement //Robotics and Automation, 1999. Proceedings. 1999 IEEE International Conference on. – IEEE, 1999. – Т. 2. – С. 1234-1239.

7. Давыдов О. И., Платонов А. К. Робот и Искусственный Интеллект. Технократический подход //Препринты Института прикладной математики им. МВ Келдыша РАН. – 2017. – №. 0. – С. 112-24.

8. Давыдов О. И., Платонов А. К. База данных для семантической модели операционной среды мобильного сервисного робота //Препринты Института прикладной математики им. МВ Келдыша РАН. – 2017. – №. 0. – С. 7-24.

УДК 681.32

Ю.П. Молявчик , О.Я. Лотоцький

Тернопільський національний економічний університет

АЛГОРИТМ ПОШУКУ ЗАЛИШКУ БАГАТОРОЗРЯДНОГО ЧИСЛА

Вступ. Одним із шляхів удосконалення алгоритмів асиметричної криптографії (зокрема, алгоритмів RSA, Рабіна, Ель-Гамаля, з використанням еліптичних кривих, електронного цифрового підпису, дослідження порядку еліптичної кривої за допомогою алгоритму Шуфа тощо)[1] є застосування системи залишкових класів, і звідси – знаходження залишків багаторозрядних чисел[2]. У зв'язку з цим актуальною задачею, яка розглядається в даній роботі, є розробка алгоритму пошуку залишку залишку багаторозрядного числа.

Метою роботи є розробка ефективного алгоритму знаходження залишків багаторозрядних чисел, який дозволяє зменшити часові складності пошуку залишків в порівняні із класичним підходом.

1. Схема алгоритму пошуку залишку багато розрядного числа

Особливістю даного алгоритму є використання властивостей залишків та модулярних операцій, що приводить до зменшення кількості ітерацій.

Слід відмітити, що реалізація представленої процедури пошуку залишку в двійковій системі числення зводиться до обчислення різниці двох чисел, розрядність яких на кожному кроці зменшується вдвічі, що дозволяє суттєво зменшити часову складність виконання зазначеної операції:

$$Y \bmod P = U \bmod F = H .$$

На рисунку 1 подано розроблену блок-схему алгоритму пошуку залишку багаторозрядних чисел запропонованим методом.

Основними перевагами даного алгоритму [3, 4] є зменшення надлишкового використання пам'яті та кількості порівнянь.

Існуючі алгоритми пошуку залишку знаходять залишок за допомогою операції віднімання. Обчислення залишку багаторозрядного числа проходить згідно алгоритмів описаних в бібліотеках для роботи з великими числами. Розроблений алгоритм виконує операції з

використанням бібіліотеки Ленстра. Подальші дослідження часових характеристик розробленого та існуючих алгоритмів проводились з використанням вище зазначеної бібліотеки Ленстра, котра спеціально розроблена для роботи з криптографічними перетвореннями.

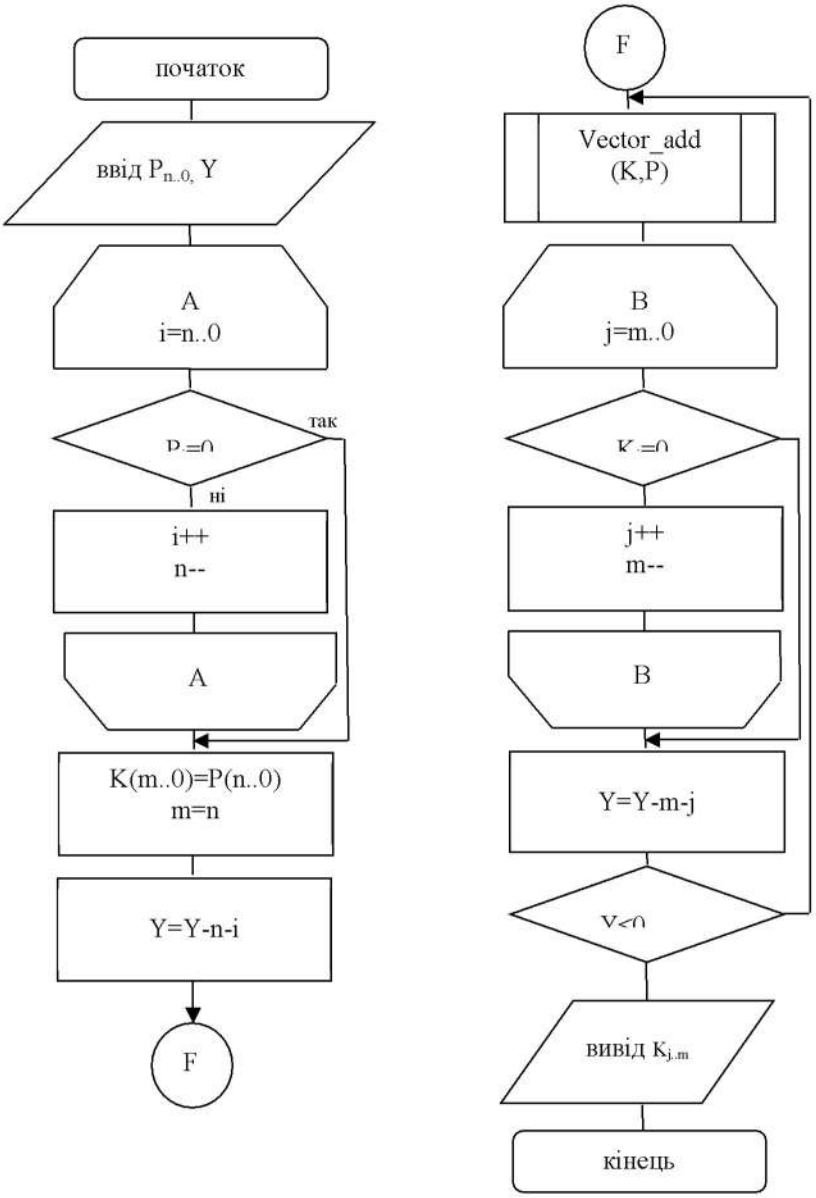


Рисунок 1 - Схема алгоритму пошуку залишку довільного багаторозрядного числа

2. Приклад роботи алгоритму

На рисунку 2 зображено як програмно реалізований алгоритм пошуку залишку довільного багато розрядного числа. Для реалізації алгоритму та подальше проведення тестів було створено програмне забезпечення на мові високого рівня C++. Мову C++ було обрано, оскільки вона надає

можливість провести емуляції та тестування розробленого алгоритму в найбільш ефективному середовищі.

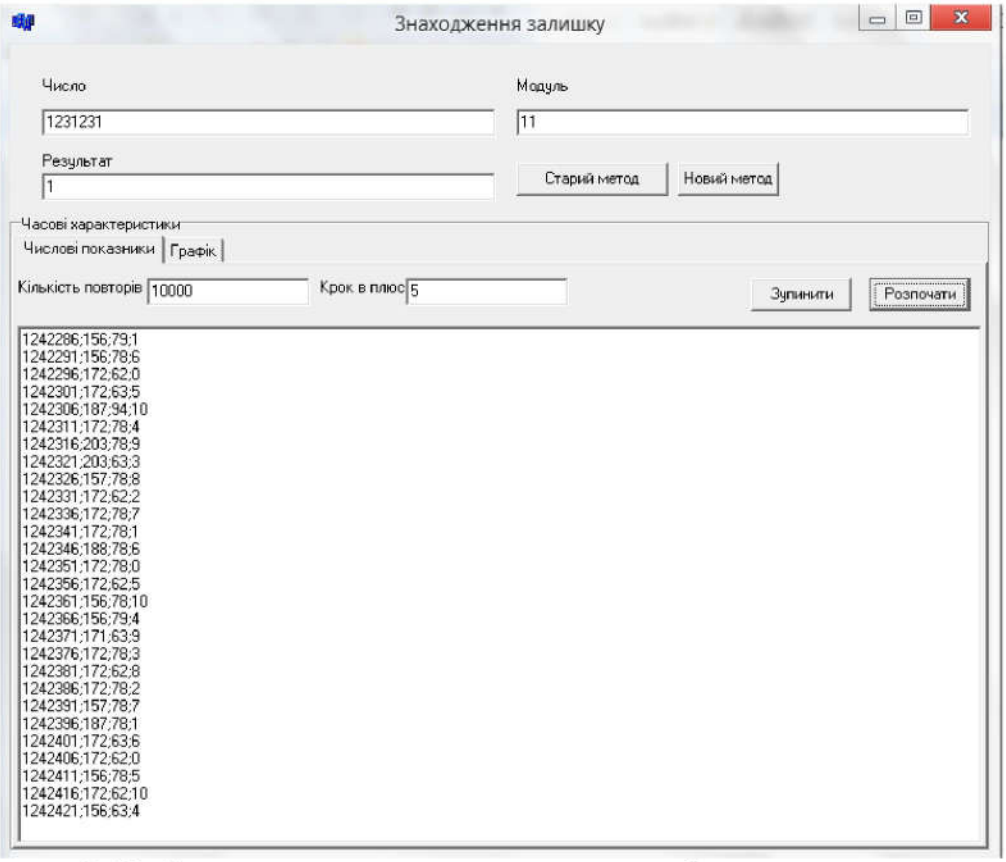


Рисунок 2. Робота алгоритму пошуку залишку багаторозрядного числа

Висновки.

За допомогою розробленого алгоритму вдалося збільшити швидкість обробки даних при пошуку залишків у багаторозрядних числах. Впровадження запропонованого підходу при обчисленні залишку в системах захисту та обробки потоків даних призведе до зростання їх ефективності.

Перелік джерел.

1. Ya. M. Nykolaychuk, M.M. Kasianchuk, I.Z. Yakymenko "Theoretical Foundations of the Modified Perfect Form of Residue Number System", Cybernetics and Systems Analysis, 2016, V.52(2), p. 219-223.

2. M.N. Kasianchuk, Ya.N. Nykolaychuk, I.Z. Yakymenko "Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes", Journal of Automation and Information Sciences, 2016, Vol.48, №8, p.56-63.

3. S. Ivasiev, M. Kasianchuk, I. Yakymenko, R. Shevchuk, M. Karpinski, O. Gomotiuk Effective Algorithms for Finding the Remainder of Multi-Digit Numbers, 2019 9th International Conference on Advanced Computer Information Technologies (ACIT). P. 175-178.

4. Л.М. Тимошенко, С.В. Івасьєв, О.Я. Лотоцький, В.М. Гаврилей, Алгоритми пошуку залишків довгих чисел для задач асиметричної криптографії, Інформатика та математичні методи в моделюванні, Том 8, номер 4, 2018. Одеса - С.324-334

УДК 681.32

Н.А. Стефурак, С.В Івасьєв., Р.Б Димашевський., О.Я Лотоцький., Ю.П. Молявчик

Тернопільський національний економічний університет

ЕФЕКТИВНИЙ АЛГОРИТМ ВИЗНАЧЕННЯ ЗАЛИШКУ БАГАТОРОЗРЯДНОГО ДВІЙКОВОГО ЧИСЛА

Вступ. Знаходження залишків від ділення чисел великої розрядності є важливою фундаментальною задачею теорії чисел, успішне вирішення якої дозволяє вдосконалити алгоритми широкого класу прикладних задач [algebra]. Особливо це стосується задач захисту інформаційних потоків в комп'ютерних системах з використанням асиметричної криптографії, зокрема, алгоритмів RSA [1], Рабіна [2], Ель-Гамаля [1], електронного цифрового підпису, використанням математичних основ еліптичних кривих [кінець]. Значну роль операція пошуку залишків відіграє при використанні системи залишкових класів (СЗК) (або модулярної арифметики) [1] та проектуванні відповідних пристроїв [2]. СЗК володіє високим паралелізмом і часто використовується при опрацюванні багаторозрядних даних для пришвидшення процесу обчислень.

Формування модулярного базису може відбуватися на основі різних підходів. Наприклад, в [3] розроблено теоретичні основи досконалої форми СЗК, в [4] – модифікованої досконалої, у яких уникається обчислювально складна процедура пошуку оберненого елемента за модулем [5]. В [6-9] здійснюється використання спеціальних модулів типу $2^n \pm k$ або чисел Мерсена та Ферма, які володіють перевагами при проектуванні операцій модулярної арифметики. Ще одним підходом є вибір великого числа модулів малої розрядності, особливо для багаторозрядних вхідних даних [9]. Для довільних модулів розроблено універсальне рішення для реалізації прямого перетворювача з позиційної системи в модулярний код [9].

Найбільш розповсюдженим для пошуку залишків у позиційній системі числення є алгоритм, згідно якого виділяється ціла частина від ділення багаторозрядного числа на модуль. Отриманий результат множиться на модуль і добуток віднімається від заданого числа. Інший спосіб полягає у послідовному відніманні модуля від заданого

багаторозрядного числа. [10] Їх недоліками є також велика кількість ітерацій, бітових операцій та порівнянь.

Вказані алгоритми пошуку залишку є ефективними лише при використанні апаратних засобів та чисел, що відповідають розрядності процесора. При створенні складних програмних систем, виникає необхідність опрацювання багаторозрядних чисел з допомогою використання спеціалізованих бібліотек[10], в яких операція знаходження залишку має значну обчислювальну складність.

У зв'язку з цим актуальною задачею є розробка алгоритмів пошуку залишків багаторозрядних чисел, які дозволяють досягнути покращення часових характеристик та зменшити часову складність пошуку залишку за рахунок зменшення кількості арифметичних операцій.

Метою роботи є реалізація алгоритмів знаходження залишків багаторозрядних чисел на основі використання властивостей модулярної арифметики, який дозволяє зменшити розрядність чисел, над якими виконуються арифметичні операції, в порівнянні з класичним підходом та, відповідно, зменшити часові складності пошуку залишків.

1. Алгоритм знаходження залишку довільного багаторозрядного числа

В основу запропонованого методу пошуку залишку $Y \bmod P = H$ покладено представлення багаторозрядного числа Y та модуля P у двійковому коді $P = \sum_{i=0}^{k-1} p_i 2^i$, $Y = \sum_{i=0}^{n-1} y_i 2^i$, де p_i, y_i=0, 1.

На першому етапі до молодших розрядів модуля P дописується n-k-2 нулів, в результаті чого отримується двійковий вектор $S = (p_{k-1}, p_{k-2}, \ldots, p_0, 0, \ldots, 0)$. Якщо k-1 старших розрядів Y не перевищує P, то знаходиться $Y \bmod S$ шляхом віднімання $Y - S = M$ і записується $M = \sum_{i=1}^{n-k-2} M_i 2^i, M_i = 0,1$, відповідно у двійковій формі $M = (M_{n-k-2}, M_{n-k-3}, \ldots, M_1, M_0)$.

Якщо $M \geq P$, то формується двійковий вектор L, в якому n-$2k$-3 молодших розрядів є нулями, а старші являють собою двійкове представлення числа P:

$$L = (p_{k-1}, p_{k-2}, \ldots, p_0, 0, \ldots, 0). \quad (1)$$

Далі якщо виконується нерівність $M > L$, то обчислюється значення $U=M \bmod L=M - L$, яке записується у двійковій формі

$U = \sum_{l=1}^{n-k-2} U_l 2^l, U_l = 0,1$ або у вигляді двійкового вектора $U = (U_{n-2k-3}, U_{n-2k-4}, \ldots, U_1, U_0)$. Причому, якщо $U \geq P$, то в молодший розряд модуля P дописується n-$3k$-4 нулів і знову ж формується такий двійковий вектор:

$$F = (p_{k-1}, p_{k-2}, \ldots, p_1, p_0, 0, \ldots, 0), \quad (2)$$

У разі виконання нерівності $U \geq F$ знаходиться значення $U \bmod F = U - F = H$ і формується двійковий вектор $H = (H_{n-3k-4}, H_{n-3k-5}, \ldots, H_1, H_0)$. Дана процедура продовжується доти, поки двійковий вектор H не буде меншим за P.

Слід відмітити, що реалізація представленої процедури пошуку залишку в двійковій системі числення зводиться до обчислення різниці двох чисел, розрядність яких на кожному кроці зменшується вдвічі, що дозволяє суттєво зменшити часову складність виконання зазначеної операції:

$$Y \bmod P = U \bmod F = H. \quad (3)$$

На рисунку 1 подано розроблену блок-схему алгоритму пошуку залишку багаторозрядних чисел запропонованим методом.

Основними перевагами даного алгоритму в порівнянні з описаними в роботах [1, 2] є зменшення надлишкового використання пам'яті та кількості порівнянь.

Нехай, наприклад, потрібно обчислити $10989_{10} \bmod 7_{10} = 6_{10}$ або відповідно у двійковій формі

$$10101011101101_2 \bmod 111_2 = 110_2.$$

На першому етапі здійснюється побітовий зсув значення залишку до тих пір, поки кількість розрядів модуля не буде перевищувати розрядність числа:

$$10101011101101_2 - 1110000000000_2 = 111011101101_2.$$

На наступній ітерації від отриманого значення віднімається значення залишку, яке формується за рахунок побітового зсуву, кількість бітів якого менша розрядності проміжного результату віднімання:

$$111011101101_2 - 111000000000_2 = 11101101_2.$$

Аналогічна процедура здійснюється на насупному кроці:

$$11101101_2 - 11100000_2 = 1101_2.$$

В результаті обчислень запропонованим методом отримується шукане значення залишку:

$$1101_2 - 111_2 = 110_2,\ 110_2 < 111_2.$$

Особливістю даного алгоритму є використання властивостей залишків та модулярних операцій, що приводить до зменшення кількості ітерацій.

2. Експериментальні дослідження алгоритму пошуку залишку довільного багаторозрядного числа

Досліджено експериментальні результати часу виконання операції знаходження залишку багаторозрядного числа розробленим та класичним методами для відомих багаторозрядих чисел Мерсена.

Для нівелювання випадкових впливів на час роботи усі обчислення значення залишку для чисел різної розрядності повторювалися 10000 разів, що дало змогу отримати масштабовану різницю часових характеристик та виділити швидший алгоритм.

В результаті чисельного експерименту побудовано графіки часових характеристик розробленого та відомого алгоритмів для 32– (рисунок 2) та 1024-бітних (рисунок 1) чисел, де q – порядковий номер чисел, s – час в секундах.

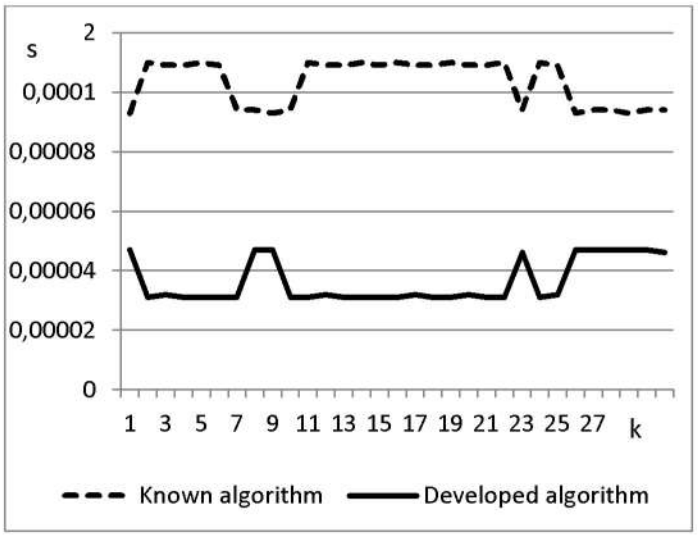


Рисунок 1. Часові харакетеристики розробленого та відомого алгоритму для 32 – бітних чисел

Дослідження показали, що із збільшенням розрядності числової вибірки часові характеристики мають лінійний характер, а швидкодія обчислення операції залишку залежить від хемінгової ваги числа.

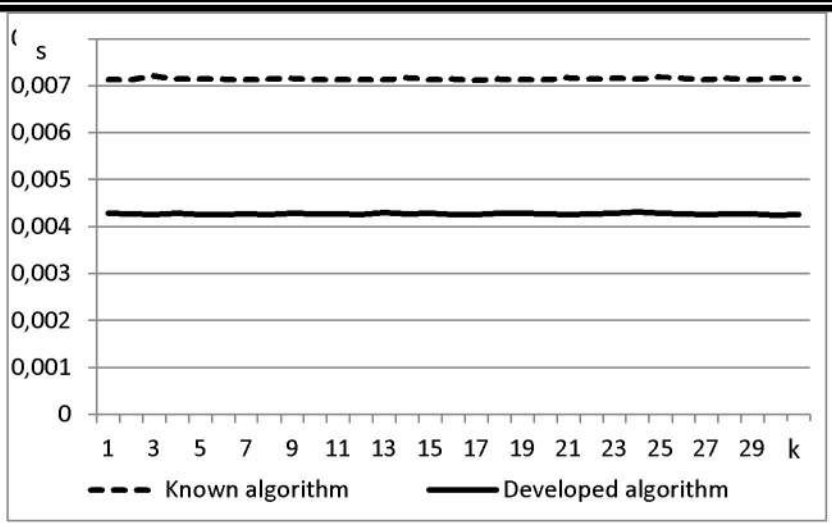


Рисунок 2 - Часові характеристики розробленого та відомого алгоритмів для 1024 – бітних чисел.

3. Алгоритм знаходження залишку багаторозрядного числа Ферма

Для пошуку залишку чисел спеціального виду (Мерсена або Ферма) доцільно використовувати модифікований алгоритм, який буде враховувати властивості чисел відповідної групи. Розглянемо n-розрядне число Ферма $M = 2^n+1$. Представимо його та модуль у двійковій формі: $M_{(2)}$=100000…01, $P = \sum_{i=0}^{k-1} p_i 2^i$, де p_i=0,1, причому вважаємо, що $P>>n$. Далі потрібно здійснити розклад $M_{(2)}$ у добуток:

$$M_{(2)}=100..00\ldots00\times100..00\ldots00\times \ldots \times100..00\ldots00. \quad (6)$$

Кількість бітів кожного множника у розкладі буде дорівнювати n+1.

У (6) кількість однакових множників з розрядністю n+1 буде рівна

$$l = \left\lceil \frac{P}{n} \right\rceil .$$

Для знаходження $2^p \bmod p$ необхідно обчислити залишки кожного з множників рівності (6) шляхом віднімання. У випадку, якщо l – парне, то на наступному етапі залишки $M_{(2)}^2$ групуються попарно і перемножуються, тобто шукаються квадрати $\left(M_{(2)}^2\right)^2$.

В результаті таких операцій отримується l залишків $M_{(2)}^2$ і останній множник у записі (6).

Коли l – непарне, то попарно групуються l-1 залишків $M_{(2)}^2$, які,

аналогічно до попереднього випадку, підносяться до квадрату, і один залишок з останнім множником у формулі (6).

Покрокове виконання запропонованого алгоритму реалізується таким чином:

1. Вхід: n-розрядне число Ферма M та модуль P.
2. Шукається різниця $M_{(2)}^2=2^{n+1}-P$.
3. Шукається ціла частина від ділення $l=P/n$ та $U=2^{\,p-l\cdot n+1}$.
4. Якщо l - парне, то обчислюється $res=(M_{(2)}^2)^2 \bmod P$ та відбувається побітовий зсув змінної l, тобто $l=l/2$. Якщо l - непарне, тоді $l=l-1$, $U=(U\cdot M_{(2)}^2) \bmod P$.
5. Якщо l – парне, тоді $res=(res\cdot res) \bmod P$ та виконується побітовий зсув змінної l, тобто $l=l/2$. Якщо l – непарне, тоді $l=l-1$, $U=(U\cdot M_{(2)}^2) \bmod P$.
6. Якщо $l>0$, тоді відбувається перехід на крок 5.
7. Відбувається операція модулярного множення та присвоєння $res=(res\cdot U) \bmod P$.

Нехай, наприклад, потрібно обчислити $x=2^{100}+1 \bmod 13$.

Оскільки розрядність модуля дорівнює 4, то число 2^{100} розкладається на 18 п'ятирозрядних добутків та закінчення числа, яке відрізняється від множників. Далі шукається залишок одного з множників за заданим модулем: $16 \bmod 13 = 3$.

Обчислюється проміжний залишок, який отримався в молодших розрядах числа:

$$2^{10}+1 \bmod 13 = 11.$$

Отже, рівність набула такого вигляду:

$$x=2^{100}+1 \bmod 13 = (3\times 19 + 11) \bmod 13.$$

Після цього відбуваються рекурентні ітерації розробленого алгоритму, оскільки другий множник для багаторозрядних чисел може бути досить великим.

Якщо кількість множників непарна, то аналогічно до попереднього число рекурентно перетворюється в набір множників та обчислюється проміжний залишок

$$x= (3\times 18 + 1) \bmod 13.$$

В результаті обчислень рівність набуває такого вигляду:

$$x= (6 \times 9 + 1) \bmod 13.$$

Аналогічні дії приводять до остаточного результату:

$x = (12 \times 4 + 7) \bmod 13$, $x = (11 \times 2 + 7) \bmod 13$, $x = (9 \times 1 + 7) \bmod 13 = 3$.

Слід відмітити, що обчислення залишку 100 розрядного числа відбулось за 5 ітерацій, причому операції виконувались над числами значно меншої розрядності.

4. Порівняння часових складностей розроблених та відомих алгоритмів

Часова складність розробленого алгоритму пошуку залишку довільного багаторозрядного числа становить $O2(n) = \frac{n}{2} \cdot \log_2 n$.

При реалізації алгоритму для пошуку залишку чисел Ферма потрібно $\log_2 l$ кроків, на кожному з яких відбувається перевірка на парність кількості залишків. Така процедура призводить до виконання на кожному кроці двох операцій модулярного множення, які можна виконати векторно-модульним методом [11] з часовою складністю $O(2 \log_2 n)$.

На рисунку 3 представлено графічні залежності обчислювальних складностей відомого та запропонованих методів.

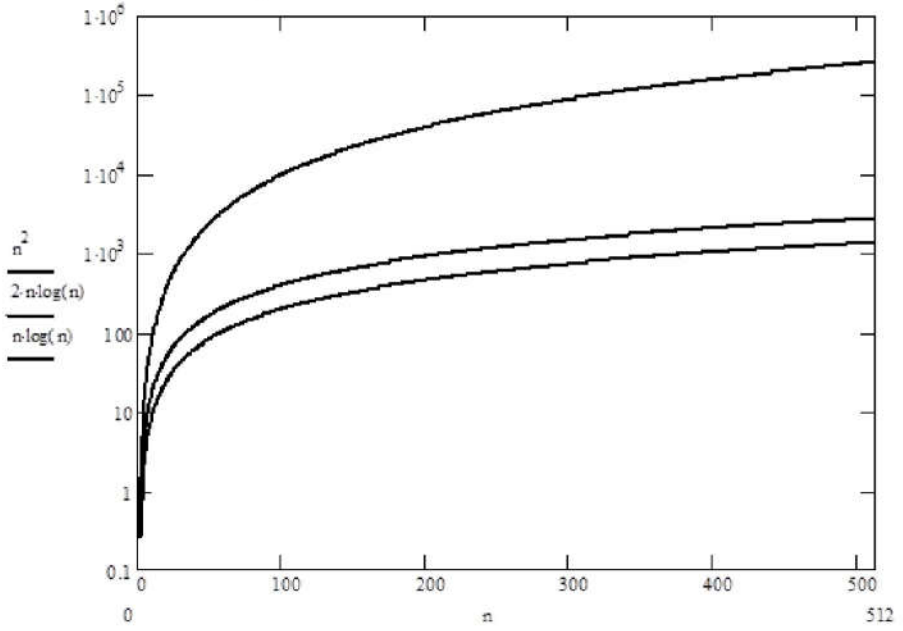


Рисунок 3 - Графічні залежності обчислювальних складностей відомих та запропонованого методу

Чисельний експеримент та оцінка часових складностей відомих і розроблених методів пошуку залишків багаторозрядних чисел, які використовуються при виконанні модульних операцій в асиметричних криптоалгоритмах, переведенні чисел з десяткової системи числення в

систему числення залишкових класів, показує, що при виконанні модульних операцій слід використовувати запропоновані методи.

Висновки.

На основі проведених експериментальних та аналітичних досліджень встановлено, що розроблені методи пошуку залишку багаторозрядних чисел характеризуються нижчою часовою складністю в порівнянні з існуючими. Впровадження запропонованих підходів до виконання операції обчислення залишку в системах захисту та опрацювання інформаційних потоків призведе до зростання їх ефективності.

Перелік джерел.

1. S. Lang, Algebra. 3rd ed. New York: Springer-Verlag; 2002.
2. I.Z. Yakymenko, M.M. Kasianchuk, S.V. Ivasiev, A.M. Melnyk, Ya.M. Nykolaichuk, "Realization of RSA cryptographic algorithm based on vector-module method of modular exponention", Proceedings of the XIV–th International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET–2018).–L'viv–Slavske.– 2018, p.550-554.
3. M. Kasianchuk, I. Yakymenko, I. Pazdriy, A. Melnyk, S. Ivasiev, "Rabin's modified method of encryption using various forms of system of residual classes", The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2017), 21-25 February, 2017, Polyana-Svalyava, p.222-224.
4. A.E. Okeyinka, Computational Speeds Analysis of RSA and ElGamal "Algorithms on Text Data", Proceedings of the World Congress on Engineering and Computer Science (WCECS 2015) – San Francisco, USA –V. I. – October 21-23, 2015, p.237-242.
5. L. Washington, "Elliptic Curves Number Theory and Cryptography", Series Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008, 524 p.
6. A. Omondi, B. Premkumar, "Residue Number System: Theory and Implementation". Imperial College Press, 2007, 296 p.
7. P.V. Ananda Mohan, "Residue number systems: algorithms and architectures", Springer Science+Business Media, NewYork, LLC, 2002, 378 p.
8. M. Kasianchuk, I. Yakymenko, I. Pazdriy and O. Zastavnyy "Algorithms of findings of perfect shape modules of remaining classes system" , XIII International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)", Polyana-Svalyava (Zakarpattya), Ukraine, 2015, p.168-171.
9. Ya. M. Nykolaychuk, M.M. Kasianchuk, I.Z. Yakymenko "Theoretical Foundations of the Modified Perfect Form of Residue Number System", Cybernetics and Systems Analysis, 2016, V.52(2), p. 219-223.
10. M.N. Kasianchuk, Ya.N. Nykolaychuk, I.Z. Yakymenko "Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes", Journal of Automation and Information Sciences, 2016, Vol.48, №8, p.56-63.
11. T. Rajba, A. Klos-Witkowska, S. Ivasiev, I. Yakymenko, M. Kasianchuk, "Research of Time Characteristics of Search Methods of Inverse Element by the Module", Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2017) – Bucharest, Romania. – V.1. – September, 2017, p.82–85.

УДК 681.32

Н.Г. Гавришків[1], О.І. Карпюк[2]

[1]Галицький коледж ім. В. Чорновола

[2]Тернопільський національний економічний університет

ДОСЛІДЖЕННЯ МІЖБАЗИСНИХ ПЕРЕХОДІВ З СИСТЕМИ ЧИСЛЕННЯ ЗАЛИШКОВИХ КЛАСІВ В ДВІЙКОВУ

Вступ. Відновлення десяткового числа по його залишках є важливим результатом для сучасної алгебри і теорії чисел [1]. Така взаємно однозначна відповідність на практиці дозволяє працювати не з багаторозрядними числами, а з наборами залишків, які є менші від вибраних основ або модулів системи [2]. Крім того, обчислення можна виконувати паралельно по кожному залишку [3]. Дані властивості лежать в основі побудови системи числення залишкових класів, яка дозволяє підвищити швидкодію обчислювальних систем за рахунок розпаралелення процесу виконання арифметичних операцій [4], здійснювати контроль за помилками в задачах завадозахищеного кодування, визначати цілочисельні корені рівняння на основі принципу Хассе , виконувати швидке перетворення Фур'є на основі простих чисел тощо. Система залишкових класів має безліч застосувань в сучасних криптографічних алгоритмах, наприклад, в шифрах Віженера та Рабіна. В криптосистемі RSA шукаються залишки від ділення на велике число, яке є добутком двох простих чисел. Відповідно, обчислення можна здійснювати за модулем цих простих множників, які мають вдвічі меншу бітову довжину. Тому розробка методів та алгоритмів, які дозволяють зменшити часову складність при відновленні десяткового числа за його залишками є на даний час актуальною задачею.

Метою роботи є дослідження міжбазисних переходів з системи числення залишкових класів в двійкову.

Дослідження існуючих алгоритмів для між базисних перетворень

Теоретичною основою при відновленні десяткового числа за його залишками є алгебра і теорія чисел [4], зокрема китайська теорема про залишки (КТЗ). Будь-яке ціле невід'ємне десяткове число N можна представити у вигляді залишків b_i від ділення на натуральні попарно взаємно прості числа p_i, які називаються модулями:

$$b_i = N \bmod p_i. \qquad (1)$$

При виконанні умови $N < P = \prod_{i=1}^{k} p_i$, де k - кількість модулів, згідно КТЗ число N можна однозначно відновити за такою формулою:

$$N = \left(\sum_{i=1}^{k} m_i P_i b_i \right) \bmod P, \qquad (2)$$

де $P_i = \frac{P}{p_i}$, $m_i = P_i^{-1} \bmod p_i$.

На рисунку 1 приведено схему роботи для між базисного переходу запропоновану в [4].

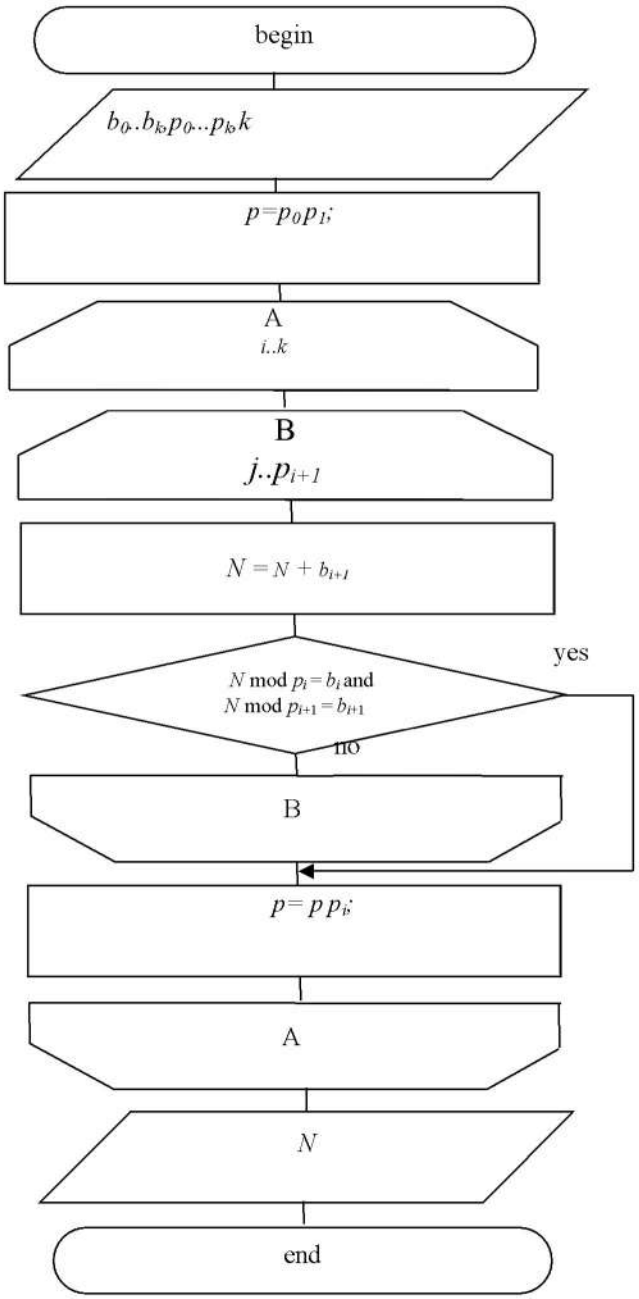


Рисунок 1 - Схема роботи алгоритму переходу з СЗК в позиційну систему числення

Ще одним способом відновлення десяткового числа по його залишках є алгоритм Гарнера, згідно якого

$$N = n_0 + n_1 p_1 + n_2 p_1 p_2 + \ldots + n_{n-1} p_1 p_2 \ldots p_{i-1}, \quad (3)$$

де $0 \le n_i < p_{i+1}$, $i=0, 1, \ldots, k-1$,

$$n_i = \frac{b_{i+1} - \left(n_0 + n_1 p_1 + \ldots + n_{i-1} p_1 p_2 \ldots p_{i-1}\right)}{p_1 p_2 \ldots p_i} \bmod p_{i+1}. \quad (4)$$

Таким чином, коефіцієнти n_i можуть бути один за одним послідовно обчислені на основі рекурентної формули (4). Крім того, алгоритм Гарнера придатний для аналогічних операцій з поліномами.

Недоліками розглянутих вище методів відновлення десяткового числа по його залишках є неможливість їх розпаралелення (або строго послідовна структура), виконання операцій над багаторозрядними числами (зокрема, обчислення залишку за модулем P), та необхідність пошуку мультиплікативного оберненого елемента за модулем.

Для знаходження останнього найбільш поширеними є методи перебору всіх можливих варіантів, за допомогою розширеного алгоритму Евкліда, на основі функції Ейлера. Всі вони характеризуються значною обчислювальною складністю. Подібним чином можна обчислювати і коефіцієнти n_i в алгоритмі Гарнера.

Висновки.

В роботі розроблено алгоритм відновлення десяткового числа за його залишками на основі додавання добутку модулів з можливістю розпаралелення обчислень та уникнення процедури пошуку мультиплікативного оберненого елемента. При цьому результати проміжних обчислень не будуть виходити за межі встановленого діапазону, що усуває необхідність виконання операції знаходження залишку за модулем P.

Перелік джерел.

1. S. Lang, Algebra. 3rd ed. New York: Springer-Verlag; 2002.

2. A. Omondi, B. Premkumar, "Residue Number System: Theory and Implementation". Imperial College Press, 2007, 296 p.

3. P.V. Ananda Mohan, "Residue number systems: algorithms and architectures", Springer Science+Business Media, NewYork, LLC, 2002, 378 p.

4. М. Касянчук, І. Якименко, С. Івасьєв, Н. Стефурак, Методи відновлення десяткового числа за його залишками на основі операції додавання, ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р. – К.: НАУ, 2019. – С.38-40

УДК 681.3

П.В. Олійник[1], В.В. Пекельна[1], В.Р. Слободянн[1], С.В. Терещенко[2]

[1]Тернопільський національний економічний університет

[2]Опорний заклад Теребовлянська загальноосвітня школа І-ІІІ ступенів №1 Теребовлянської міської ради

АЛГОРИТМ АЛГЕБРАЇЧНОГО АНАЛІЗУ ЗА ДОПОМОГОЮ МЕТОДУ РОЗШИРЕНОЇ ЛІНЕАРИЗАЦІЇ ІЗ ЗАСТОСУВАННЯМ МЕТОДУ ВИКЛЮЧЕННЯ ГАУСА

Вступ. До оцінки захищеності конфіденційної інформації при використанні алгоритмів на основі операцій заміни та додавання по модулю 2^n існує два основних підходи: оцінка теоретичної стійкості і оцінка практичної (обчислювальної) стійкості.

Теоретичний підхід до оцінки стійкості був запропонований К. Шенноном в роботі [1]. Даний підхід заснований на доказ існування безумовно стійких (бездоганних) систем захисту інформації. В роботі [2] запропоновано класифікацію систем на обчислювально стійкі, імовірно стійкі і обчислювально нестійкі системи. У роботі розглядається задача оцінки стійкості алгебраїчними методами аналізу. В цьому випадку, під стійкістю алгоритмів найчастіше мається на увазі здатність даних алгоритмів протистояти відомим методам аналізу і при цьому забезпечувати конфіденційність інформації протягом певного (заданого спочатку) терміну.

Метою роботи є дослідження алгоритму алгебраїчного аналізу за допомогою методу розширеної лінеаризації із застосуванням методу виключення Гауса.

1. Алгоритм виключення Гауса для булевих рівнянь

Заключним кроком методу розширеної лінеаризації є рішення лінійної системи методом виключення Гауса.

Суть методу виключення Гауса полягає в приведенні системи лінійних рівнянь до трикутного увазі, шляхом послідовного виключення невідомі з рівнянь.

Розглянемо детальніше загальний алгоритм вирішення лінійних систем даними способом.

Нехай задана система рівнянь $A \cdot \overline{x} = \overline{b}$ над полем $GF(2)$ виду:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \\ a_{1m} & \dots & a_{nm} \end{pmatrix},$$

$$x = (x_1 x_2 \dots x_n), \quad (1)$$

$$b = \begin{pmatrix} b_1 \\ \dots \\ b_m \end{pmatrix},$$

де $x_1 \dots x_n$ – невідомі,

$a_1, \dots, a_{nm}$ – коефіцієнти, що приймають значення 0 або 1,

$b_1, \dots, b_n$ – вільні члени рівнянь,

n – число невідомих системи,

m – число рівнянь системи.

В ході вирішення системи над полем $GF(2)$ можна використовувати такі перетворення матриці:

– додавання одного рядка матриці до іншої;
– перестановка рядків матриці;
– перестановка стовпців матриці.

Нехай в перших двох рівняннях системи коефіцієнти $a_{11}, a_{21} = 1$:

$$x_1 \oplus a_{12}x_2 \oplus \dots \oplus a_{1n}x_n = b_1,$$

$$x_1 \oplus a_{22}x_2 \oplus \dots \oplus a_{2n}x_n = b_2.$$

Тоді висловлюючи x_1 з першого рівняння і підставляючи його в друге, отримуємо рівняння виду:

$$(a_{12} \oplus a_{22})x_2 \oplus \dots \oplus (a_{1n} \oplus a_{2n})x_n = b_1 \oplus b_2$$

Таким чином, відбувається виключення невідомого x_1 з другого рівняння. Таке перетворення відповідає:

$$A^1 = \begin{pmatrix} 1 & \dots & a_{1n} \\ 0 & a_{12} \oplus a_{22} & a_{1n} \oplus a_{2n} \\ a_{1m} & \dots & a_{mn} \end{pmatrix},$$

$$x = (x_1 x_2 \dots x_n), \quad (2)$$

$$b^1 = \begin{pmatrix} & b_1 & \\ b_1 & \oplus & b_2 \\ & \dots & \\ & b_m & \end{pmatrix},$$

Для виконання прямого хід методу виключення Гауса потрібно знайти рядок, в якій перший елемент дорівнює одиниці (якщо такої немає, то треба переставити стовпчики) і додати її до інших рядках, що містить одиницю в першому стовпці. Продовжуючи цей процес для всіх невідомих

$$x = (x_1, \dots, x_n),$$

матрицю призводять до трикутного вигляду:

$$\begin{array}{c} 1 \quad 2 \quad \cdots \quad k \quad k+1 \quad \cdots \quad n \quad n+1 \\ \begin{pmatrix} 1 & & & * & * & & & b'_1 \\ & 1 & \cdots & * & * & \cdots & & \cdots \\ & & \cdots & \cdots & \cdots & \cdots & & \cdots \\ & & & 1 & \cdots & \cdots & \cdots & \cdots \\ & & & & \cdots & \cdots & \cdots & \cdots \\ & & & & & 1 & \cdots & \\ & & & & & & \cdots & \cdots \\ & & & & & & 0 & b'_m \end{pmatrix} \end{array} = (A', b'). \qquad (3)$$

Тепер сформована система рівнянь $A'x = b'$, яка має теж безліч рішень, що і вихідна система (можливо зі зміненим порядком нумерації змінних, якщо відбувалося переміщення стовпців).

Зворотний хід методу виключення Гауса полягає в послідовному обчисленні значень невідомих, $x = (x_1, \dots, x_n)$ починаючи з $x_n = b'_n$.Якщо деякі з елементів $b'_{n+1}, \dots, b'_m$ відмінні від нуля, то система лінійних рівнянь не має рішення. Якщо рядки матриці з *k+1* по m рівні 0, то система має не більше 2^{n-k} рішень.

Для їх знаходження фіксуються довільним чином невідомі $x_{k+1}, \dots, x_n$ (можливо 2^{n-k} способів завдання), а потім знаходять значення x_k-ого рівняння, x_{k-1} із *(k-1)* рівняння і т. д. Таким чином, знаходяться всі можливі рішення вихідної системи рівнянь.

Висновки.

Розроблено алгоритм алгебраїчного аналізу за допомогою методу розширеної лінеаризації із застосуванням методу виключення Гауса для рішення систем булевих нелінійних рівнянь, приведених до лінійного вигляду.

Перелік джерел.

1. Shannon C.E. «A mathematical theory of communication» // Bell system technical journal, vol. 27 – 1948– pp.–379-423.

2. Ростовцев А.Г. «Два подхода к анализу блочных шифров» // А.Г. Ростовцев, Е.Б. Маховенко / Проблемы информационной безопасности. Компьютерные системы – 2002 – №1–49–54 с.

УДК 681.3

О.А. Додь[1], В.Й. Пемковський[2], Ю.Я. Кірдей[2], Л.Є. Смолінська[2]

[1]Тернопільський національний економічний університет

[2]Опорний заклад Теребовлянська загальноосвітня школа І-ІІІ ступенів №1 Теребовлянської міської ради

АЛГОРИТМ ОТРИМАННЯ ВЕКТОРА ОЗНАК НА ОСНОВІ МЕТОДУ ПЕРЕТВОРЕННЯ ЗОБРАЖЕННЯ

Вступ. Широко досліджуваною задачею є розпізнавання рукописного тексту. На даний момент досягнута точність нижча, ніж для рукописного "друкарського" тексту. Рукописні підписи теж можуть розглядатися як рукописні слова, проте найчастіше вони більше відповідають малюнкам, оскільки підписант намагається зробити свій підпис унікальним і використовує не лише символи імені і прізвища, але і додаткові графічні елементи.

Хоча може здатися, що підробити підпис досить просто, проте, практично неможливо повторити швидкість написання і чинений при цьому тиск. Так що, системи розпізнавання підписів, що використовують самі передові технології, стають ідеальною заміною для паролів в операціях, наприклад, з корпоративними банківськими рахунками. Проте, як і в усіх інших методів ідентифікації, і тут є свої недоліки. Один з головних недоліків полягає в тому, що залежно від обставин кожен з нас може підписуватися по-різному. Щоб система була практичною, важливо вміти відрізняти, наприклад, повільно зроблений підпис в результаті якоїсь травми або в результаті спроби підробити його.

Метою роботи є дослідження алгоритму отримання вектора ознак на осснові методу перетворення зображень.

1. Методи оптимізації розпізнавання образів

Для збільшення якості розпізнавання образів використовують різні метод обробки зображень з текстом, наприклад, метод шумозаглушення [1]. Джерелом шуму на зображеннях можуть бути:

- аналогові шуми:
- забрудненість, пил;
- подряпина;
- цифрові шуми;
- шуми теплової матриці;

- шум перенесення зарядів;
- шум квантування.

При цифровій обробці зображення застосовують просторове шумозаглушення.

Виділяються наступні методи:

- метод адаптивної фільтрації;
- використання лінійного усереднення пікселів по сусіднім пікселям;
- медіанної фільтрації;
- математичної морфології;
- метод розмиття по Гаусу;
- методи на основі дискретних вейвлет-перетворень;
- метод головної компоненти;
- анізотропної дифузії;
- фільтр Вінера.

Після розпізнавання може бути виконана додаткова корекція, яка дає можливість збільшення якість розпізнавання спірного символу (тобто символу, у якого є кілька кандидатів з приблизно однаковими оцінками ступеня відповідності стандартам) на основі таких методів:

- аналіз буквосполучень, які характерні для мови;
- словник мови;
- граматичний аналіз.

2. Розпізнавання підписів

Розпізнавання підпису використовують в самих різних галузях в рамках повномасштабного програмного рішення (розпізнавання, формування пакетів документів, обробки документів, експорту даних), так і впроваджують як окреме рішення. Наприклад, при формуванні пакетів документів для отримання кредитів у банку, крім інших операцій, слід реалізувати верифікацію підпису клієнта: еталонну підпис з паспорта автоматично порівнюють з усіма підписами на документі і виносять рішення про справжність, також система повинна показати відсоток збігу.

Мета розпізнавання рукописного підпису складається в ідентифікації особистості людини з метою розпізнавання і / або верифікації. Розпізнаванням називають ідентифікацію особистості власника підпису, а верифікація – це прийняття рішень, чи будуть дані підписи істинними або

підробленими. Завдання розпізнавання і верифікації має важливе значення також в галузі судово-медичних експертиз, а також відіграє ключову роль в системі безпеки банків і інших організацій зі збільшеними вимогами безпеки до біометричної системи контролю та управління доступом.

Система для статичного розпізнавання рукописного підпису є більш важкореалізовуваною, ніж система з динамічним розпізнаванням, так як остання має додаткові характеристиками, наприклад, тривалості атомарних операцій (наприклад, процеси листи), сили натискання, вектора направлення листа і іншими, які дають можливість спрощення остаточних процесів ідентифікації особистості. Однак система статичного розпізнавання володіє ще однією важливою перевагою - вона не вимагають доступу до додаткового пристрою обробки даних, що надходять (датчик, таймер і т. д.).

3. Алгоритм розпізнавання рукописного підпису на основі штучних нейронних мереж

Система розпізнавання рукописного підпису включає ряд модулів на основі штучних нейронних мереж, кожен з яких реалізує певний етап процесу розпізнавання (рисунок 1).

Рисунок 1 - Архітектура системи розпізнавання рукописного підпису

На цьому рисунку показано, що архітектура системи включає два рівня: навчання і тестування.

Навчання реалізується шляхом послідовності кроків: введення підписів, які використовуються для навчання, попередня обробка зображення, отримання векторів ознак, побудова мережі класифікаторів, отримання результатів навчання (шаблонів).

При тестуванні реалізується наступна послідовність кроків: введення підпису, який буде розпізнаватися, попередня обробка зображення, отримання векторів ознак, розпізнавання (верифікація) підписи.

4. Алгоритм отримання вектора ознак при розпізнаванні підпису

Для отримання вектора ознак використовується алгоритм, заснований на методі перетворення зображення, яке передбачає наступні етапи [2]: виділення зовнішнього контуру зображення, пошук опорних точок на зображенні зовнішнього контуру, обчислення координат векторів, побудова векторної моделі, перетворення векторної моделі (ущільнення і нормалізація), класифікація векторної моделі і віднесення її до одного з класів.

Виділення контуру зображення здійснюється шляхом накладення фільтра Робертса на бінарне зображення рукописного символу, отриманого в результаті попередньої обробки [3]. Фільтр Робертса є перетворення такого вигляду (передбачається, що сканування зображення йде зліва направо і зверху вниз):

$$A' = |A - D| + |B - C| \text{ або } A' = \sqrt{(A - D)^2 + (B - C)^2}, \quad (1)$$

де A '- нове значення яскравості поточного пікселя,

A - значення яскравості поточного пікселя,

B - значення яскравості пікселя знизу від поточного пікселя,

D - значення яскравості пікселя праворуч від поточного пікселя.

За допомогою цього алгоритму здійснюється побудова зовнішнього контуру зображення рукописного символу від першої знайденої опорної точки до останньої опорної точки, яка належить цьому ж контуру. При цьому вважається, що сканування зображення відбувається зліва направо і зверху вниз, а також враховується зв'язність поточну і наступну опорних точок.

Після знаходження опорних точок і занесення їх в таблицю будується векторна модель, що представляє собою набір векторів виду:

$$Model = \{V_1, V_2, \dots V_i, V_{(i+1)} \dots V_n\}. \quad (2)$$

Тут початок кожного наступного вектора $V_{(i+1)}$ збігається з кінцем попереднього вектора V_i, утворюючи замкнутий контур.

Кожен вектор характеризується парою координат: довжина вектора (*len*) і кут між горизонтальною лінією (*alfa*). Визначення координат вектора $V_i = (Len_i, Alfa_i)$ здійснюється шляхом переходу від декартових координат з отриманої таблиці до полярних координат за такими формулами:

$$Len_i = \sqrt{x_i^2 + y_i^2}, Alfa_i = arctg\frac{y_i}{x_i}, \quad (3)$$

де x_i, y_i- відносні координати вектора $x_i = x_{i+1} - x, y_i = y_{i+1} - y_j$,

ax_j, y_i - координати поточної опорної точки, взятої з таблиці,

x_{i+1}, y_{i+1} - координати наступної опорної точки.

Отримана таким чином модель складається з великої кількості векторів, незначно відрізняються один від одного.

Для того щоб оптимізувати отриману векторну модель, пропонується піддати її процедурам нормалізації і ущільнення. Процедура ущільнення застосовується перед нормалізацією і являє собою видалення несуттєвих векторів, що з'єднують точки які близько стоять.

Ця процедура працює за наступною схемою:

1) $i = 1$;

2) вибирається V_i вектор моделі;

3) якщо довжина V_i менше деякого порогового значення EPS, то даний вектор видаляється з моделі. $Len_i < EPS$ -умова видалення вектора з моделі;

4) $i = i + 1$;

5) якщо $i < N$, то здійснюємо перебір всіх векторів моделі в циклі.

Отже, отримана модель дозволяє ефективно визначати вектор ознак, який є основою при розпізнаванні підпису.

Висновки.

Розглянутий у статті алгоритм отримання вектора ознак заснований на методі перетворення зображення і дозволяє виділити зовнішній контур зображення, знайти опорні точки на зображенні зовнішнього контуру, обчислити координати векторів, побудувати векторну модель, перетворення векторної моделі (ущільнення і нормалізація), класифікувати векторну модель і віднесення її до одного з класів.

Перелік джерел.

1. Lange M.M. Classification of 2D Grayscale Objects in a Space of the Multiresolution Representation // M.M. Lange, S.N. Ganebnykh/ – 2005 – 27 с.

2. Горошкин А Н. Застосування векторного підходу до розпізнавання рукописних символів // УДК, 2006, http: //cyberleninka.ru/article/n/primenenie - vektornogo-podhoda-k-raspoznavaniyu-rukopisnyh-simvolov.

3. Колядин Д.В. (2005). Алгоритм виділення екстремальних точок стосовно до задачі біометричної верифікації рукописного підпису.// Д.В.Колядин, І.Б.Петров / Електронний журнал «витрачаються на дослідження в Росії, №4(45) –2005 – 17-22 с.

УДК 681.32

В.М. Кузик[1], С.В. Івасьєв[2], Н.З. Кульчинська[1], Л.І. Маланчук[1]

[1]Галицький коледж ім. В. Чорновола

[2]Тернопільський національний економічний університет

СПОСОБИ КОДУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ НА ОСНОВІ ТЕОРЕТИКО - ЧИСЛОВИХ БАЗИСІВ РАДЕМАХЕРА ТА КРЕСТЕНСОНА

Вступ. Способи кодування інформаційних потоків визначаються теоретико числовими базисами (ТЧБ), які застосовуються для їх представлення [1]. Найбільш поширеними ТЧБ в сучасних КС є наступні: унітарний, Хаара, Грея, Радемахера, Крестенсона та Галуа.

Світовий досвід створення процесорів для КС, поряд з застосуванням ТЧБ Радемахера, що призводить до породження двійкової системи числення, за останні роки демонструє тенденцію застосування інших ТЧБ. Реалізація спеціалізованих, кореляційних, спектральних, ентропійних, спецпроцесорів на базі Галуа та проблемно-орієнтованих процесорів цифрової обробки даних часто виконується на базі сумісного використання комбінацій названих ТЧБ, наприклад Радемахера - Крестенсона, Радемахера - Хаара, Крестонсона - Галуа та ін [2].

У зв'язку з цим існує проблема глибокого дослідження характеристик різних ТЧБ та граничних можливостей їх застосування для реалізації компонентів як спеціалізованих, так і універсальних процесорів. При цьому перспективним, крім розповсюдженого одновимірного (векторного) представлення чисел та виконання арифметико-логічних операцій у базисі Радемахера, є застосування змішаного базису Радемахера- Крестенсона [3,4].

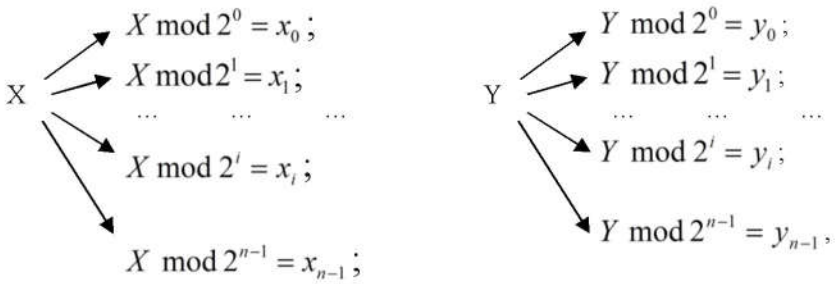
Метою роботи є дослідження способів кодування інформаційних потоків в комп'ютерних системах на основі теоретико - числових базисів радемахера та крестенсона

1. Дослідження базису Радемахера

Арифметичні операції над двома числами у двійковій системі числення базису Радемахера описуються наступними виразами:

$$X = \sum_{i=0}^{n-1} x_i 2^i ,\ x_i \in \overline{0,1};\ Y = \sum_{i=0}^{n-1} y_i 2^i ,\ y_i \in \overline{0,1}.$$

Тобто двійкові коди чисел X і У: $X=(x_{n-1},x_{n-2},\ldots,x_i,\ldots,x_0)$; $Y=(y_{n-1},y_{n-2},\ldots,y_i,\ldots,y_0)$ визначаються на основі модульних операцій згідно аналітичних виразів:



Приведені характеристики кодових матриць ТЧБ Радемахера, Крестенсона, які найширше використовуються для кодування та цифрової обробки даних в інформаційних системах, мають властивості мінімальної надлишковості по відношенню до наступних базисів: унітарного, Хаара, Крейга, Уолша та Грея [2].

У таблиці 1.2 N – діапазон представлення чисел, $p_1, p_2, \ldots, p_i, \ldots, p_m$ – набір взаємо простих модулів СЗК базису Крестенсона, $a_i=p_i-1$.

Система числення залишкових класів базису Крестенсона, детально описана Акушським І.Я. та Юдіцьким Д.І. [3].

Таблиця 1 – Характеристики кодових матриць ТЧБ

	Радемахера	Крестенсона
Кодові матриці	$M_{Rad}=\begin{vmatrix}000\ldots00\\000\ldots01\\000\ldots10\\000\ldots11\\\ldots\ldots\ldots\\111\ldots11\end{vmatrix}$	$M_{Cres}=\begin{vmatrix}P_1 & P_2 & \ldots & P_m\\0 & 0 & \ldots & 0\\1 & 1 & \ldots & 1\\2 & 2 & \ldots & 2\\0 & 3 & \ldots & 3\\\ldots & \ldots & \ldots & \ldots\\2 & 4 & \ldots & 6\end{vmatrix}$
n - число активних кодових елементів	$n=\frac{N\cdot\log_2 N}{2}$	$n=\prod_{i=1}^{m}P_i$
V – об'єм кодової матриці	$V=N\cdot\log_2 N$	$V=\sum_{i=1}^{m}\log_2(P_i-1)$

Результати досліджень часової складності реалізації операції множення над числами в базисах Радемахера (O1(n)) та Радемахера - Крестенсона (O2(n)) приведені на рисунку 1 [3].

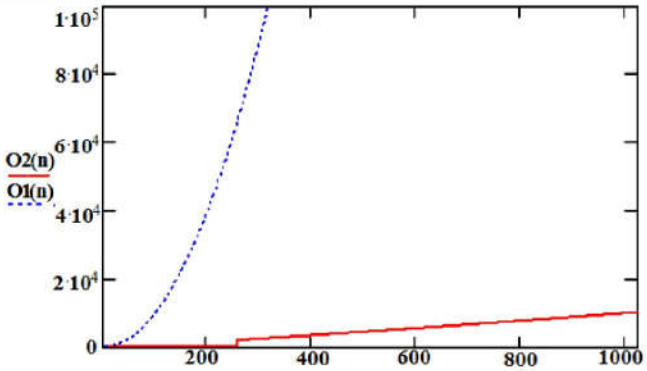


Рисунок 1 – Часова складність реалізації операції множення в базисах Радемахера (O1(n)) та Радемахера - Крестенсона (O2(n))в залежності від розмірності

Нормалізована форма СЗК, запропонована науковою школою проф. Николайчука Я.М., найбільш поширена в телекомунікаційних процесорах інформаційних систем нафтогазової промисловості [3].

З рисунка 1 видно, що методи множення у базисі Радемахера - Крестенсона характеризується суттєвим збільшенням швидкодії, що є важливою перевагою його застосування шляхом використання спеціалізованих процесорів та контролерів.

В роботі [4] проведено дослідження та розробка операції експоненціювання (рисунок 2). В результаті у роботі [3] розроблено метод модулярного експоненціювання, який з допомогою використання особливостей базису Радемахера – Крестенсона (O4(n)) призводить до кардинального зменшення обчислювальної складності порівняно з базисом Радемахера (O3(n)), що ілюструє рисунок 2.

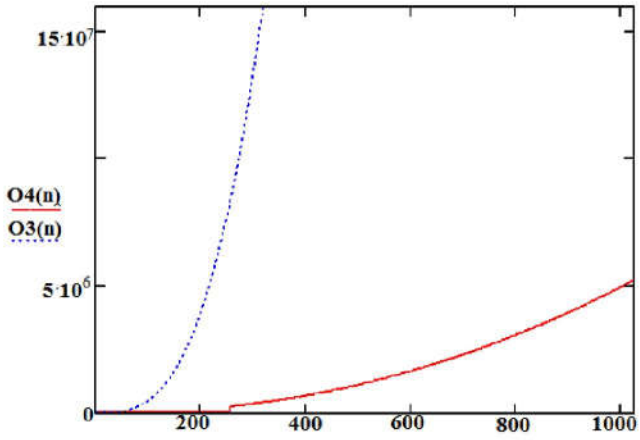


Рисунок 2 – Порівняння характеристики виконання модулярного експоненціювання БРЧ в базисах Радемахера (O3(n)) та Радемахера – Крестенсона (O4(n))

Проведені дослідження показують перспективність використання мультибазисних методів опрацювання багаторозрядних інформаційних потоків в прикладних задачах теорії чисел.

2 Аналіз існуючих бібліотек для роботи з багаторозрядними числами, постановка задачі дослідження

Серед сучасних програмних засобів опрацювання БРЧ виділяються ряд бібліотек для реалізації відповідних алгоритмів [3], а саме: бібліотека для роботи з БРЧ Ленстра, Arageli, NTL, GMP, Crypto++ та інші. Наведемо особливості організації деяких з них.

В роботі [2] наведений порівняльний аналіз швидкодії реалізації алгоритмів опрацювання БРЧ з використанням різних бібліотек (таблиця 2).

В результаті дослідження отримані відповідні значення RANK[4] та наведені в таблиці 2. Для кожного алгоритму було виконано 100 тестів та встановлено відносні показники продуктивності.

Таблиця 2 - Характеристики швидкодії алгоритмів з використанням різних бібліотек опрацювання БРЧ

Бібліотека	*RANK(ALG$_i$)*				AES-192	TDES	RSA (2048)		ECDSA (F2m=283)		HMAC SHA-1	SHA-1 (/&=256)	RANK
	MUL	POWMOD	xGCD	ECMUL			*sign*	*verf*	*sign*	*Verf*			
NTL	1,01	1,18	1,0	-	-	-	-	-	-	-	-	-	1,06
MIRACLE	3,58	2,62	3,15	1	1,00	-	2,29	1,72	2,02	2,76	-	1,12	1,40
Botan	3,41	5,21	1,09	1,42	2,16	1,98	1,00	1,00	1,60	1,95	1,15	1,13	1,67
Crypto++	4,49	5,04	16,82	4,35	2,68	1,90	1,12	1,15	1,00	1,00	1,05	1,07	2,19
OpenSSL	2,80	2,43	12,49	1,15	4,49	3,39	1,68	1,51	1,85	2,53	1,00	1,00	2,26
OpenPGP	2,87	2,31	3,11	1,41	1,12	1,37	2,35	1,73	1,54	2,00	-	1,06	1,79
GNU Crypto	1,0	1,0	1,01	1,24	1,38	1,00	2,71	1,80	1,75	2,13	1,06	1,08	1,35
CryptLib	5,25	4,17	8,59	1,7	1,03	1,47	1,09	1,08	1,07	2,05	1,02	1,06	1,82
LenstraLib	1,02	1,15	1,03	1,3	-	-	-	-	-	-	-	-	1,12

Для роботи з БРЧ бібліотека Lenstra є досить гнучким інструментом, що забезпечує найбільш ефективне використання обчислювальних ресурсів, а також реалізацію основних арифметичних та криптографічних алгоритмів, тому для реалізації розроблених методів обрана саме вона.

Факторизацію доцільно застосовувати для підбору модулів у СЗК [2], яка на даний час є однією з альтернатив двійковій системі числення, що дозволяє застосовувати нові підходи до організації обчислювальних систем при виконанні елементарних математичних операцій [3]. Хоча СЗК не позбавлена недоліків, до яких відносяться, зокрема, відсутність ділення та порівняння чисел, необхідність визначення умов переповнення розрядної сітки, однак її успішно можна застосовувати для додавання, віднімання та множення цілих багаторозрядних чисел. Безсумнівною перевагою СЗК є можливість виконання операцій над числами, які менші за вибрані модулі, розпаралелення процесу обчислень та відсутність міжрозрядних переносів.

СЗК – це непозиційна система числення, десяткові числа в якій представляються невід'ємними залишками від ділення на кожен з системи взаємно простих модулів p_i. Додавання, віднімання і множення в СЗК відбуваються незалежно по кожному модулю без переносів між розрядами. Зворотне перетворення з СЗК у десяткову систему числення ґрунтується на використанні китайської теореми про залишки і є досить громіздким процесом, що є ще одним недоліком СЗК, який стримував її розвиток і поширення:

$$N = \left(\sum_{i=1}^{n} b_i B_i \right) \bmod P, \qquad (1)$$

де $B_i = M_i m_i$, $M_i = \dfrac{P}{p_i}$, базисні числа m_i шукаються з виразу $(M_i m_i) \bmod p_i = 1$.

Необхідність обчислення базисних чисел $m_i = M_i^{-1} \, mod \, p_i$ істотно збільшує складність переведення чисел з СЗК у десяткову систему. Спрощення цієї задачі відбувається у досконалій формі СЗК (ДФ СЗК), коли модулі p_i підібрані таким чином, що усі m_i=1. У роботах [2] була розвинута теорія ДФ СЗК і запропоновано метод для визначення системи модулів ДФ СЗК. Однак у випадку обмеженої кількості модулів або необхідності використання модулів, які мало відрізняються один від одного, цей метод непридатний. У роботі була запропонована модифікована ДФ СЗК (МДФ СЗК), у якій базисні числа m_i=±1, що також виключає необхідність пошуку оберненого числа.

У [3] показано, що після відповідних математичних перетворень можна отримати умову, яка повинна виконуватися для визначення набору модулів для ДФ та МДФ СЗК:

$$\left(p_2p_3...p_{n-2}+p_1p_3...p_{n-2}+...+p_1p_2...p_{n-3}-p_1p_2...p_{n-2}\right)+\left(p_1p_2...p_{n-2}\right)^2=ab. \quad (2)$$

$$\left(p_2p_3...p_{n-2}+p_1p_3...p_{n-2}+...+p_1p_2...p_{n-3}-p_1p_2...p_{n-2}\right)+\left(p_1p_2...p_{n-2}\right)^2=\pm ab. \quad (3)$$

Це означає, що ліва частина (1.4), (1.5) повинна бути факторизована, на основі чого визначаються параметри a та b для визначення будь-якої кількості модулів.

Висновок. Отже, вирішення задач теорії чисел дозволить спростити процес перетворення з СЗК у позиційну систему числення, що, в свою чергу, можна ефективно використовувати в ряді прикладних задач обчислювальної техніки.

Перелік джерел.

1. Бекчанова Ш.Б. Принципы построения высокопроизводительных вычислительных структур / Ш.Б. Бекчанова, Х.Н. Зайнидинов // Тезисы докладов НТК «Мафкуравий жараёнлар ва Узбекистонда фанлар ривожининг долзарб муаммолари», Андижон. - 2002. – С. 441.

2. Виноградов И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981. – 176с.

3. Грибанов Ю.И. Автоматические цифровые корреляторы./ Ю.И. Грибанов, Г.П. Веселова, В.Н Андреев. – М.: Энергия, 1971. – 240с.

4. Задірака В.К. Комп'ютерна арифметика багаторозрядних чисел: Наукове видання / В.К. Задірака, О.С. Олексюк. – Київ. –2003. – 264 с.

5. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов.– Казань: Казан. ун. 2011.– 190 с.

6. Івасьєв С.В. Збіжність екстремумів залишкової функції в околі розв'язку задачі факторизації/ С.В.Івасьєв, Я.М. Николайчук, І.З.Якименко, І.Р.Колісник // Вісник Хмельницького національного університету. Технічні науки. – 2015, №4. - С.157-164.

7. Мельник А. О. Програмовані процесори обробки сигналів / А.О.Мельник. – Львів: Вид-тво Національного університету "Львівська політехніка", 2000. –55 с.

8. Николайчук Я.М. Методы цифровой обработки шумоподобных сигналов на основе кодовых систем / Я.М. Николайчук, Б.М. Шевчук – Киев, Сб. тр. ИКАН УССР, 1988.

9. Николайчук Я.М. Проблеми реорганізації структури процесорів у різних теоретико-числових базисах / Я.М. Николайчук // Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління» (ICSM-2014). - Тернопіль,2014.- С.110-114.

10. Палагин А.В. Реконфигурируемые структуры на ПЛИС / А.В. Палагин, В.Н. Опанасенко, В.Г. Сахарин // УсиМ. – 2000. – № 3. – С. 33-43.

11. Палагин А.В. Опыт разработки микропроцессорных распределенных систем реального времени. / А.В. Палагин, Я.Н. Николайчук // – Киев: Знание, – 1988. – 19 с.

УДК 681.3

І.В. Антонюк[1], Р.П. Луцків[2], О.М. Ліщинська[2], І.О. Юрчишин[3]

[1]Тернопільський національний економічний університет

[2]Опорний заклад Теребовлянська загальноосвітня школа І-ІІІ ступенів №1 Теребовлянської міської ради

[3]Чортківська загальноосвітня школа І-ІІІ ступенів №6

ПРОЦЕДУРИ КОНТРОЛЮ ТА ВИМІРЮВАННЯ РИЗИКІВ

Вступ. У сучасному високотехнологічному суспільстві практично неможливо уявити некеровані або частково керовані об'єкти. В якості одного із способів управління пропонується застосовувати механізм аудиту, який добре зарекомендував себе багаторічною практикою застосування стандартів ISO ([1], [2], [3]) і галузевої сертифікації (наприклад, ISAGO [5]). Крім того, доречно зазначити, що за даними експертів на території Україні розміщені понад 4500 потенційно небезпечних об'єктів, для яких питання ефективного управління вельми критичні. Тому оцінка ризиків при застосуванні механізмів аудиту є актуальною науковою задачею.

Метою роботи є дослідження процедури контролю та вимірювання ризиків при застосуванні механізмів аудиту.

1. Оцінка ризиків

У літературних джерелах відмічені кілька видів аудиту, що виконують цілі процедури контролю, вимірювання ризику та встановлення ступеня допустимості ризику. Зокрема, у роботі приводяться два «класичних» підходи - засновані на ідеї оцінки «соціального ризику» (запропонований в 1967 р.) З управлінням F / N кривими (співвідношення числа поражених при кожному сценарії від кожного джерела небезпеки, більшою мірою і частотою події F) і системного «загального ризику», представленого в стандартах ISO. Розглянемо приклади управління соціальним ризиком (рисунок 1). Як показано в работах І.Б. Шубинского і Замишляєва А.М. (АО «НІІАС») за допомогою управління ризиками на залізничному транспорті, зручно застосовувати термін «допустимий рівень ризику», який трактується у відповідності з ALARP як рівень ризику, для якого затрати на його досягнення є економічно ефективними (рисунок 2).

$$R = f(p,C),\ R = \sum_{i=1}^{n} R_i,\ R = p \cdot C,$$

якщо С=(1 – смерть, 0 – життя), то $R = p$.

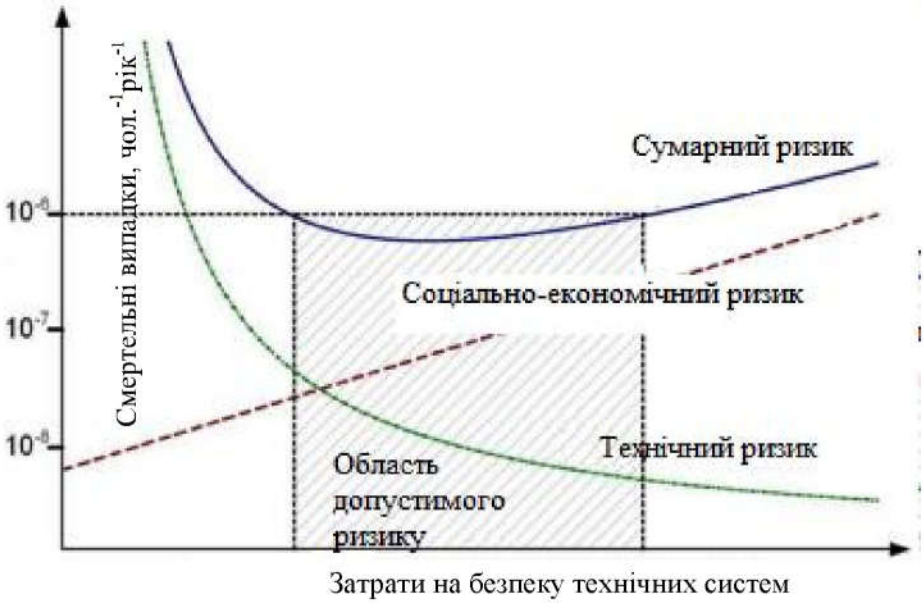


Рисунок 1 – Приклад управління «соціальним ризиком»

Стосовно до кривих F / N Фармера управління ризиком за принципом ALARP зводиться до побудови та аналізу області ALARP (рисунок 2).

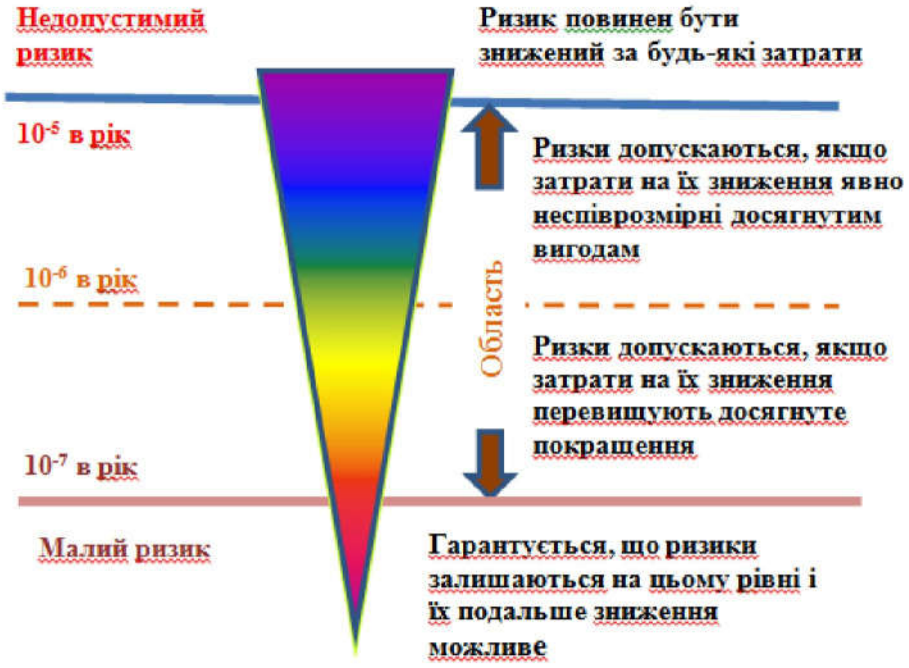


Рисунок 2 – Приклад керування ризиком по принципу ALARP

Оцінка ризиків (по будь-наведеною методикою) повинна дозволяти формувати адекватну (наскільки це можливо) оцінку по кожному аналізованому об'єкту для подання ОПР.

Зокрема, можна скористатися методом, запропонованим проф. М. А.

Шахраманьяном [6] і визначати ризик як інтеграл віддаленості людини від об'єкта і ймовірності ураження людини, наприклад:

$$R = \int_{L=0}^{L=\infty} P(L) \int_{\sigma=0}^{\sigma=2\pi} r(\sigma, L) P(\sigma) d\sigma dL \qquad (1)$$

де $r(\sigma, L)$ – віддаль від об'єкту до точки в полярних координатах (σ, L), $P(\sigma, L)$ – ймовірність поражения человека в точке с координатами (σ, L).

Крім того $P(\sigma, L)$ визначається як:

$$P(\sigma, L) = \alpha(\sigma)\, \beta(L, \sigma)$$

де: $\alpha(\sigma)$ – ймовірність напрямку вітру в момент аварії

$\beta(L, \sigma)$ – ймовірність ураження в напрямку σ на відстані L .

Цілком можливо на базі формули (1) запропонувати формулу оцінки ризиків, яка буде враховувати сукупність факторів (не тільки «соціальний ризик»), наприклад - вартість пошкоджених (знищених) активів організації або третіх осіб, якщо в результаті аварії була порушена прилегла територія. Такий підхід може бути застосований на базі сучасних стандартів ([1], [2], [3], [4],). Таким чином, при формуванні проблеми обґрунтування доцільності аудиту складних об'єктів можливо прийняти до уваги власні функціональні властивості об'єктів.

Висновки.

В даній статті приведені приклади управління соціальним ризиком на основі кривих Фармера та за принципом ALARP, який зводиться до побудови та аналізу області ALARP. Це дозволяє формувати адекватну (наскільки це можливо) оцінку по кожному аналізованому об'єкту.

Перелік джерел.

1. ISO/IEC 20000-1:2011 «Information technology - Service management - Part 1: Service management system requirements».

2. ISO 22301:2012 «Societal security. Business continuity management systems. Requirements», International Organization for Standardization, 2011. – 24 pages.

3. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013. – 23 pages.

4. ISO 50001:2011 Energy management systems – Requirements with guidance for use, International Organization for Standardization, 2011. – 22 pages.

5. ISAGO Standards Manual Effective, January 2014 3rd Edition.

6. Шахраманьян М.А. Комплексная оценка риска от чрезвычайных ситуаций природного и техногенного характера // М.А. Шахраманьян, В.И. Ларионов, Г.М. Нигметов и др./ Безопасность жизнедеятельности. 2001. № 12. – С. 8–14.

УДК 004.67

С.В. Кулина

Тернопільський національний економічний університет

СИСТЕМА НАДІЙНОГО ЗБЕРІГАННЯ ДАНИХ НА ОСНОВІ НАДЛИШКОВОЇ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Вступ. Останнім часом все більшого поширення на світовому ринку набувають дослідження систем надійного зберігання даних. Важливою характеристикою систем зберігання даних є висока швидкодія запису та зчитування інформації з накопичувачів. Враховуючи, що система зберігання базується на коригуючих кодах, необхідно отримати підвищену швидкодію процесів кодування та декодування даних.

Розробка та впровадження методів підвищення ефективності систем надійного зберігання даних дозволить значно розширити їх область застосування і відповідно збільшить ринок таких систем. Згідно світової практики більшість організацій використовують методи розподіленого (віддаленого) зберігання та резервного копіювання а також, методи зберігання даних в режимі реального часу для ліквідації наслідків втрати інформації.

Метою роботи є дослідження та розробка методу надійного зберігання даних на основі коригуючих кодів системи залишкових класів.

1. Дослідження вимог до систем надійного зберігання даних

Для зберігання даних в режимі реального часу використовують наступні типи систем [1]: пряме сховище (DAS); мережний пристрій зберігання даних (NAS); мережа зберігання даних (SAN); хмарне сховище (Cloud storage); резервний масив незалежних дисків (RAID).

Кожна з вище перерахованих систем має свої переваги та недоліки, проте згідно з тенденціями протягом останніх років у сфері безпечного зберігання інформації значну нішу займають саме RAID технології. RAID дозволяє зберігати однакові дані надлишково (в декількох кроках) збалансованим способом, щоб поліпшити загальну продуктивність. Диски RAID часто використовуються на серверах, але, як правило, не потрібні для персональних комп'ютерів. Набором пристроїв з яких складається система зберігання керує особливий контролер масиву (RAID-контролер). Він забезпечує зв'язок між дисками, розміщення даних та дозволяє відобразити увесь масив, як логічний пристрій зберігання. За рахунок виконання операцій читання та запису на декількох дисках

одночасно, масив забезпечує вищу швидкість обміну у порівнянні з одним великим диском.

Враховуючи вище викладене, можна окреслити наступні проблеми при розробці методів для підвищення ефективності систем зберігання даних: вибір коригуючих кодів на основі досконалої та модифікованої форм системи залишкових класів з мінімальною обчислювальною складністю алгоритмів декодування та можливістю адаптивної зміни коригуючої здатності коду без зміни алгоритму кодування; розробка алгоритмів зберігання розподілених даних поданих в системі залишкових класів.

2. Розробка системи надійного зберігання даних на основі НСЗК

Ідея роботи полягає у тому, що підвищення надійності системи зберігання даних можна досягти шляхом використання надлишкової системи залишкових класів (НСЗК).

Система залишкових чисел (СЗК) визначається набором k цілих чисел (модулів) $p_i (i=1, 2, \ldots, k)$.

Ціле число X у діапазоні $[0, P_k)$ може бути відновлено з k залишків $(x_1, x_2, \ldots, x_k)$ використовуючи китайську теорему про залишки [2].

Надлишкову СЗК отримуємо додаванням $r=n-k$ додаткових модулів $(p_{k+1}, p_{k+2}, \ldots, p_n)$, до раніше вибраної системи модулів. В результаті формується НСЗК - код з n додатних попарно взаємно простих модулів.

Тепер ціле число X в діапазоні $[0, P_k)$ подається послідовністю n залишків по модулях $p_1, p_2, \ldots, p_n$:

$$X=(x_1, x_2, \ldots, x_k, \ldots, x_n).$$

Відповідно, інтервал $[0, P_k)$ називається інформаційним (робочим), а інтервал $[P_k, P_n)$ сформований із додаткових модулів r називається перевірочним діапазоном.

Суть запропонованого методу полягає в наступному: отримані дані, розділяється на фрагменти (блоки) X_j з яких обчислюються залишки x_i за системою взаємно простих модулів p_i:

$$x_i=X_j (\mathrm{mod}\ p_i).$$

Отримані залишки розподілені на окремі носії (диски).

Враховуючи, що при кодуванні використовується розширена

система модулів, для відновлення даних нам необхідна тільки частина залишків (рисунок 1).

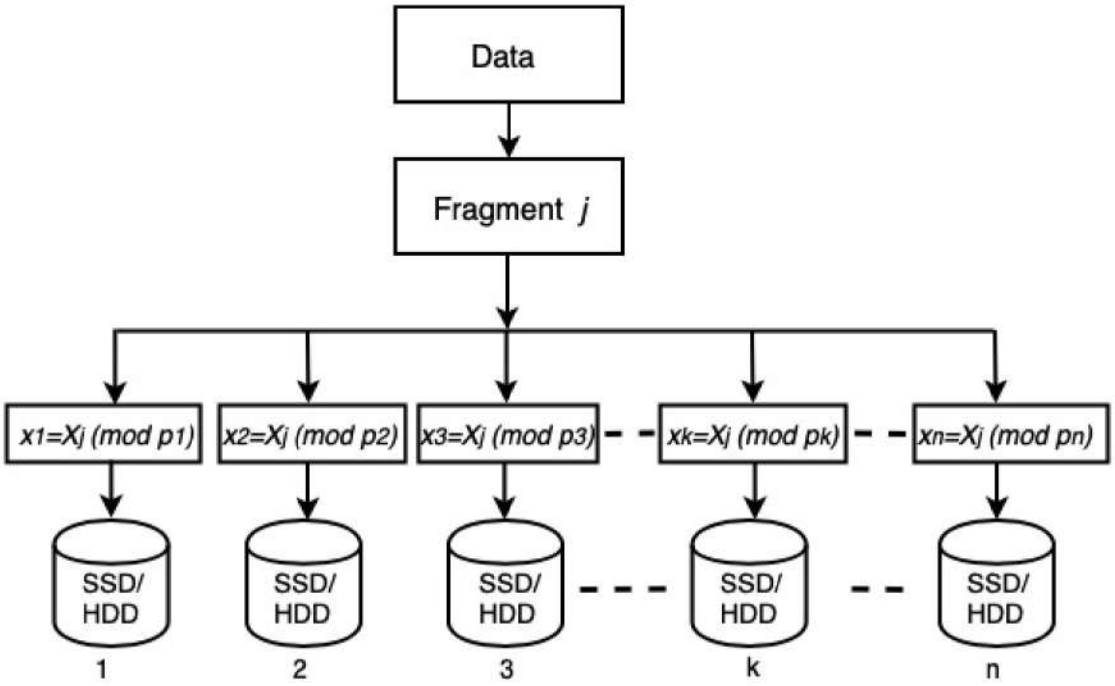


Рисунок 1 - Система надійного зберігання даних на основі НСЗК

Коригуюча здатність надлишкової СЗК визначається кількістю введених додаткових модулів. При додаванні r додаткових модулів, надлишкова СЗК здатна виявляти r та виправляти помилки в $r/2$ залишках.

Основною перевагою НСЗК є рівноцінність (взаємозамінність) інформаційних та перевірочних символів, що дозволяє відновлювати фрагменти даних при спотворенні чи виході з ладу цілого блоку залишків за одним з модулів.

Проведений аналіз використання систем модулів для кодування та декодування інформаційних фрагментів кратних 8 біт показав, що використання таких модулів дозволяє мінімізувати надлишкову інформацію [4]. На основі проведених досліджень можна сказати, що збільшення кількості модулів зменшує надлишковість інформації, яка зберігається на носіях даних. Для виявлення однієї помилки у кодах НСЗК достатньо одного модуля, проте для її виправлення необхідно два перевірочних модулі. При збільшенні кількості модулів надлишковість інформації зменшується завдяки зростанню фрагмента інформації, який опрацьовується за один цикл роботи.

При роботі з системами надійного зберігання даних у випадку втрати зв'язку чи виході з ладу одного із дисків нам відомо, який саме з них не працює. Це дає змогу зменшити необхідну кількість перевірочних модулів для виправлення фрагмента даних.

Одним з значних недоліків використання системи модулів з більшою кількістю k, є збільшення необхідної кількості носіїв для зберігання даних, проте завдяки цьому зменшується надлишковість та час опрацювання даних.

Розроблена система забезпечує високу надійність під час зберіганні даних завдяки можливості відновити фрагмент даних при виході з ладу одного з дисків, а також захищеність інформації при розподіленому зберіганні на віддалених носіях. Це відбувається завдяки тому, що для відновлення будь-якого фрагменту даних необхідно отримати фізичний або віртуальних доступ до більшості дисків.

Перевагою пропонованого методу є значно менша надлишковість для відновлення даних, у порівнянні з технологіями RAID та системами на основі інших коригуючих кодів.

Висновки.

На основі проведених досліджень було запропоновано метод використання надлишкової системи залишкових класів для підвищення надійності роботи систем зберігання даних. У системах зберігання даних, на відміну від передачі даних, визначити неробочий носій можна застосовуючи інші методи та засоби діагностики.

Розроблена система забезпечує високу надійність зберігання даних за рахунок можливості відновлення даних при виході з ладу частини дисків, а також високу захищеність даних при їх розподіленому зберіганні.

Перелік джерел.

1. Garth A. Network attached storage architecture / Garth A. Gibson and Rodney Van Meter // Communications of the ACM. – New York, 2000. Vol. 43 (№11). P. 37-45.

2. Акушский И. Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.: Сов. радио. 1968. С. 460.

3. Кулина С.В. Виявлення помилок на основі коригуючих кодів системи залишкових класів / Кулина С.В. // Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах: Матеріали VII Міжнародної науково-практичної конференції. – Чернівці: «Місто». 2018. С.126-127.

УДК 004.75

Т.Г. Цаволик, В.С. Ващук

Тернопільський національний економічний університет

АНАЛІЗ ПІДХОДІВ ТА МЕТОДИК ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ВЕБ – ДОДАТКІВ

Вступ. Поняття вразливості веб-додатків описане в таких стандартах як як ISO/IEC 29147:2014 Information technology. Security techniques. Vulnerability disclosure (в Україні діє стандарт ДСТУ ISO/IEC 29147:2016 Інформаційні технології. Методи захисту. Розкриття вразливостей та ISO/IEC 27000:2016). В стандарті ISO/IEC 29147 сказано, що вразливість – це слабке місце в програмному, апаратному забезпеченні, або ж в онлайн сервісі. Слабке місце в системі може бути викликано недоліками в процесі проектування або керуванні процесами тощо [1].

В стандарті ISO/IEC 27000:2016 вразливість визначається як слабке місце засобу управління та контролю, яку може бути використане однією або кількома загрозами [2]. В документі НД ТЗІ 1.1 – 003 – 99 сказано, що вразливість системи – нездатність системи протистояти реалізації певної загрози або сукупності загроз [3].

Тому важливою задачею при тестуванні інтернет речей на проникнення є аналіз методик. Згідно термінології НД ТЗІ 1.1 – 003 – 99, тестування на проникання – випробування, метою яких є здійснення спроби обминути або відключити механізми захисту [4].

Отже задача щодо аналізу підходів та методик є актуальною та потребує додаткового дослідження.

Метою роботи є аналіз існуючих та найбільш популярних методик тестування на проникнення веб –додатків.

1. Аналіз існуючих методик тестування на проникнення веб – додатків

Зазвичай, сценарій тестування на проникнення виглядає наступним чином:

- збір інформації про цільові системи;
- пошук вразливостей;
- проникнення в систему;
- складання звітів;
- очищення систем від наслідків тесту.

Зважаючи на це, є 3 основні підходи до проведення тестування на проникнення[5]:

- white box – тестувальник має доступ до системи та має в своєму розпорядженні всю інформацію про її будову;

- grey box – імітація дій зловмисників по зламу системи, які мають часткову інформацію про систему (діапазони IP – адрес, ідентифікатори бездротових мереж, доступ до системи з низьким рівнем привілеїв та ін.);

- black box –тестувальник імітує дії зловмисників, у яких є тільки назва компанії та зовсім відсутня інформація про систему. Практично нульові відомості про систему.

Для проведення тестування на проникнення веб – додатків існують наступні методики: OWASP Testing Guide (Інструкція тестування OWASP); PTES – Penetration Test Execution Standard (Стандарт виконання тесту на проникнення); ISSAF - Information System Security Assessment Framework.

Висновки.

У роботі приведено аналіз підходів та методик тестування на проникнення веб-додатків. Широкий вибір засобів дає змогу проводити тестування на проникнення, але їх ефективність залежить від алгоритму дій. Алгоритми дій представлені у вигляді спеціальних методик. Використання цих методик значно скоротить час на тестування та підвищить ефективність тестів.

Перелік джерел.

1. Міжнародний стандарт ISO/IEC 29147 [Електронний ресурс]. – Режим доступу: http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip#en
2. Міжнародний стандарт ISO/IEC 27000 [Електронний ресурс]. – Режим доступу: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip
3. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99 [Електронний ресурс]. – Режим доступу: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4_НД_ТЗІ_1.1-003-99.pdf
4. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99 [Електронний ресурс]. – Режим доступу: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4_НД_ТЗІ_1.1-003-99.pdf
5. Офіційний сайт компанії Агенство активного аудита [Електронний ресурс]. – Режим доступу: http://auditagency.com.ua/?r=blog&p=Pentest&lang=ru

Секція 2
БЕЗПЕКА ІНТЕРНЕТ РЕЧЕЙ

УДК 004.75

Н.В. Гавриляк[1], А.Б Бик[1], В.П. Павлюс[2]
[1)]Тернопільський національний економічний університет
[2)]Галицький коледж ім. В. Чорновола

МЕРЕЖЕВИЙ ШЛЮЗ ІНТЕРНЕТ РЕЧЕЙ НА ОСНОВІ ОДНОПЛАТНОГО КОМП'ЮТЕРА

Вступ. У зв'язку з широким впровадженням інформаційних систем у різні галузі економіки захист інформації, яка передається та обробляється у даних системах є актуальним та важливим завданням. Враховуючи той факт, що офіси багатьох компаній є географічно розподілені, захищена передача даним має надзвичайно важливе значення. Для вирішення вказаного завдання використовують технологію VPN (Virtual Private Network – віртуальна приватна мережа). VPN розширює приватну мережу через загальнодоступну мережу та дає можливість користувачам надсилати та отримувати дані через загальнодоступні мережі, так якби їхні обчислювальні пристрої були безпосередньо підключені до приватної мережі.

Завдяки VPN, підключеному до маршрутизатора, можна створити захищене зашифроване з'єднання з будь-якої точки світу до своєї домашньої мережі. Це має ряд переваг, таких як можливість доступу до файлів у своєму NAS без будь-якої чіткої конфігурації, або коли з'єднання зашифровано, можливість використовувати свій ноутбук на загальнодоступній точці Wi-Fi, не переймаючись тим, хто перехопить дані, які передаються. Найкраще, контролювати все, і можна бути впевненим, що наші дані повністю безпечні і що ми не покладаємось ні на які інші послуги [1].

З розвитком технології Інтернет – речей (IoT - Internet of Things) виникає гостра проблема безпечного підключення десятків пристроїв IoT до мережі Інтернет. Враховуючи, що IoT використовують різні інтерфейси та протоколи передачі даних, доцільно для їх підключення до Інтернету використовувати спеціалізовані IoT - шлюзи. Великі компанії та корпорації пропонують широкий асортимент захищених мережевих шлюзів Інтернет речей, проте ціни на них стартують від 1000$. Таким чином, розробка захищеного мережевого шлюзу на основі одноплатного

комп'ютера є актуальним завданням, яке дозволить значно здешевити його вартість [2].

Метою роботи є розробка захищеного мережевого шлюзу Інтернет речей на основі одноплатного комп'ютера.

1. Структура шлюзу Інтернет речей

Порівнявши характеристики найбільш популярних моделей мережевих IoT шлюзів можна зробити наступний висновок. Для того щоб мережевий шлюз Інтернет речей був здатен швидко виконати поставлене завдання він повинен бути обладнаний швидкісним процесором. Обчислювальні вузли доповнює оперативна пам'ять, яка може бути представлена у вигляді модуля на 2 чи 4 ГБ. Передача даних здійснюється за допомогою модулів введення / виведення. Система має підтримувати різні мережні стандарти, тому потрібні інтерфейси: порт RJ45 і роз'єм USB, I2C, UART та інші. Згідно з поставленим завданням, для реалізації захищеного мережевого шлюзу Інтернет речей вибрано одноплатний комп'ютер Raspberry Pi 3 model B від компанії Raspberry Pi Foundation [3].

Структура захищеного IoT шлюзу приведена на рисунку 1. Для забезпечення безперебійного живлення використаємо резевний акумулятор з інвертором напруги.

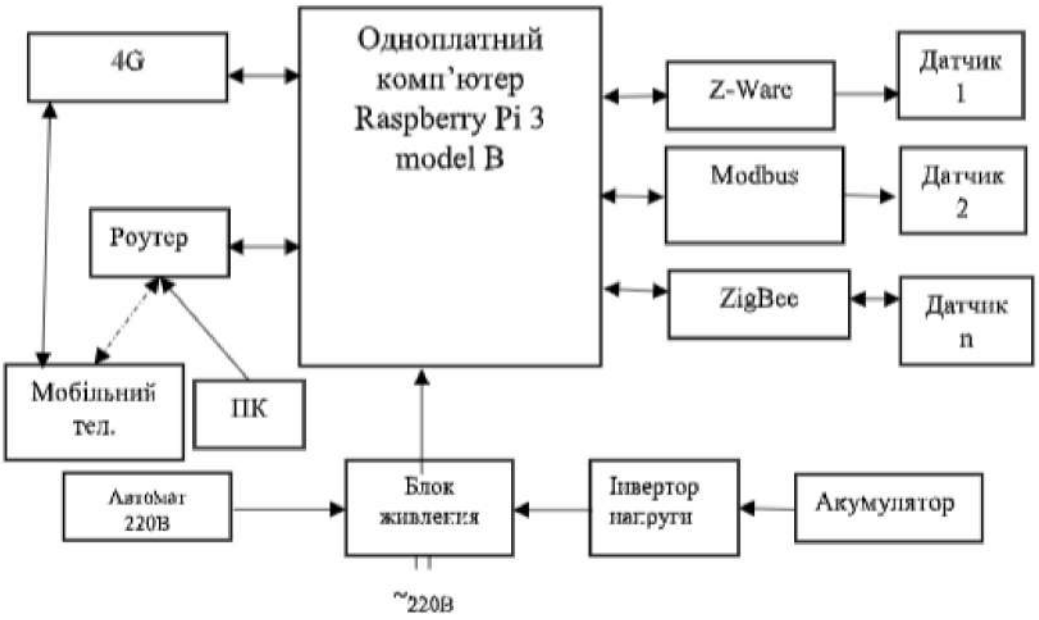


Рисунок 1 – Структура захищеного IoT - шлюзу

В якості програмного забезпечення з відкритим вихідним кодом використаємо OpenVPN. Для цього вводимо: sudo apt-get install openvpn. Підвищуємо свої привілеї до root: sudo -i. OpenVPN поставляється з Easy_RSA, легким і простим пакетом для використання методу

шифрування RSA. З Easy_RSA, запускаємо алгоритм, який поставляється разом з програмним забезпеченням для створення нового унікального ключа. Вводимо: cp –r /usr/share/doc/openvpn/examples/easy-rsa/2.0 /etc/openvpn/easy-rsa. Редактор nano є вбудованим інструментом для редагування на Raspbian - nano vars. Міняємо змінну EASY_RSA на: export EASY_RSA="/etc/openvpn/easy-rsa". Створюємо сертифікати CA Certificate і Root CA

Наступним кроком завантажуємо файл конфігурації та встановлюємо OpenVPN: cd /tmp && wget https://files.ovpn.com/raspbian/ovpn-se-gothenburg.zip && unzip ovpn-se-gothenburg.zip && mkdir -p /etc/openvpn && mv config/* /etc/openvpn && chmod +x /etc/openvpn/update-resolv-conf && rm -rf config && rm -f ovpn-se-gothenburg.zip Вводимо дані для входу: echo "CHANGE TO YOUR USERNAME" >> /etc/openvpn/credentials, echo "CHANGE TO YOUR PASSWORD" >> /etc/openvpn/credentials. Запукаємо OpenVPN і дивимось чи все працює: sudo openvpn --config /etc/openvpn/ovpn.conf –daemon. Перевіряємо чи з'єднання було успішним, чекаємо приблизно хвилину після запуску останньої команди і набираємо: curl https://www.ovpn.com/v2/api/client/ptr | python -m json.tool.

В результаті отримуємо:
"status":true,"ip":"172.20.32.41","ptr":"cliXXX.ovpn.com"}.

Розроблений IoT шлюз з можливістю організації захищеного з'єднання на основі OpenVPN може знайти ефективне застосування при проектуванні розумних будинків.

Висновки.

В роботі розроблено структуру мережевого шлюзу Інтернет речей на базі одноплатного комп'ютера, який забезпечує під'єднання до мережі Інтернет пристроїв з різними інтерфейсами, протоколами та каналами зв'язку.

Перелік джерел.

1. Сэмюэл Грингард. Интернет вещей: Будущее уже здесь. Издательство: Альпина Паблишер, 2011. –180 с.

2. Зараменских Е., Артемьев И. Интернет вещей. Исследования и область применения. – М: Инфра-М, 2016. — 188 с

3. Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 2. Modelling and Development /V.S. Kharchenko (ed.) - Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 547 p.

УДК 004.75

Т.Г. Цаволик, М.Б. Бондарчук

Тернопільський національний економічний університет

МЕТОД ВИЯВЛЕННЯ БОТ МЕРЕЖ НА ОСНОВІ DNS

Вступ. Низка методів та засобів дозволяють виявляти роботу бот-мережі. Чимало науковців виділяють метод аналізу трафіку на основі DNS, який дозволяє ініціювати бот-мережу через одночасні DNS-запити на сервер.

Тому, варто розглянути особливості методу на основі DNS.

Метою роботи є проаналізувати та визначити недоліки методу виявлення бот-мереж на основі DNS в середовищі IoT.

1. Особливості методу виявлення бо-мереж на основі DNS

DNS – це складна розподілена база даних, на яку спирається більшість Інтернет-сервісів. Його моніторинг є критично важливим, і необхідно постійно контролювати трафік DNS для виявлення аномалій, вимірювати продуктивність та генерувати статистики використання.

Сучасні бот-мережі зазвичай використовують техніку, яку називають потоком домену, або алгоритмом генерації домену, щоб генерувати велику кількість псевдовипадкових доменних імен PDN, щоб динамічно управляти операторами бот-мереж керувати їх ботами.

Такі бот-мережі стають однією з найсерйозніших загроз безпеці Інтернету в глобальному масштабі. Науковці зосереджують свою увагу на виявленні бот-мереж аналізуючи потік даних в мережі на основі функцій DNS-трафіку системи доменних імен [1].

Цей метод пасивно фіксує весь DNS-трафік із шлюзу відстежуваної мережі, а потім витягує ключові функції для ідентифікації PDN. Відомо, що в правилах побудови доменних імен є чітке зміщення.

Розроблені технології дозволяють аналізувати DNS-трафік для отримання довжини та очікуваного значення, за допомогою яких можна розрізнити доменне ім'я, сформоване людьми або ботами.

Загалом, методи виявлення бот-мереж базуються на основі даних фільтрації переданих пакетів, аналіз трафіка в мережі та портів.

При цьому, зловмисники намагаються модифікувати програми за допомогою динамічної зміни коду в системі з використанням портів.

Переважна більшість бот-мереж для керування інфікованими хостами використовує DNS [1,2]. Методи виявлення бот-мереж на основі DNS не вимагають значних обсягів обчислювальних ресурсів та здатні виявляти ще невідомі боти.

Для багатьох видів бот-мереж властиві певні особливості поведінки ботів, які простежуються в DNS-трафіку та є нетиповими для DNS-запитів звичайних користувачів. Зазвичай не інфіковані хости в локальній мережі використовують локальні DNS-сервери для здійснення DNS-запитів [3]. Боти в локальній мережі можуть використовувати або локальні, або власні DNS-сервери чи безкоштовні сервіси DNS (OpenDNS, FreeDNS). Для багатьох видів бот-мереж характерним є ігнорування ботами TTL-періоду, який містився у відповіді від авторитативного DNS-сервера на DNS-запит [4]. Це означає, що бот виконує очищення локального кеша DNS та здійснює повторний DNS-запит щодо доменного імені до завершення TTL-періоду, що надає можливість підвищити гнучкість та надійність керування бот-мережею.

Висновки.

Поширення зловмисних систем стрімко зростає. Методи виявлення бот-мережі, на основі аналізу DNS трафіку - ефективні та потребують подальшого розвитку. Аналіз трафіку DNS має значне застосування в галузі інформаційної безпеки та комп'ютерної криміналістики, в першу чергу при виявленні інсайдерських загроз, зловмисного програмного забезпечення, кіберозброєнь та розширених постійних загроз в комп'ютерних мережах

Перелік джерел.

1. Боровнікова К. Ю. Методи та програмне забезпечення інформаційної технології виявлення бот-мереж на основі аналізу DNS-трафіка. 2016. автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.06 - інформаційні технології / Кіра Юліївна Бобровнікова. – Тернопіль : ТНТУ, 2017. – 23 с.

2. Kwon J. PsyBoG: A scalable botnet detection method for large-scale DNS traffic, Computer Networks, 2016, pp. - 48-73.

3. Coubro. DNS Traffic Analysis [Electronic resource]: Access mode - https://www.cubro.com/en/blog/dns-traffic-analysis-make-networks-more-secure/

4. On Botnets that use DNS for Command and Control. Dietrich, C.J., Rossow, C., Freiling, F. C., Bos, H., van Steen, M., Pohlmann, N.: In: Proceedings of European Conference on Computer Network Defense, 2011. - pp. 9-16.

УДК 004.75

В.В.Бойчук, В.В. Блажко, Ю.О.Верцімага

Тернопільський національний економічний університет

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СФЕРІ ЛОГІСТИКИ

Вступ. Технологія блокчейн розроблена в 2008 році, а в 2009 році добуті перших 50 біткоїнів, які в даний час отримали широке використання у всьому світі. З 2012 року значно зріс інтерес до криптовалют, почалося активне обговорення можливості, що надає біткоїн та блокчейн. Пік активності та зацікавленості інвесторів у блокчейні припав на 2016 рік, високу популярність отримали криптовалюти. Проте блокчейн має багато специфічних особливостей, які дають можливості використання його у інших сферах, зокрема у логістиці.

Метою роботи є дослідження особливостей застосування технології блокчейн у сфері логістики.

1. Технологія блокчейн та особливості її застосування у сфері логістики

Блокчейн це децентралізована система зберігання даних або цифровий реєстр транзакцій, угод, контрактів. Основна перевага – те, що цей реєстр не зберігається в одному місці. Він розподілений між великою кількістю комп'ютерів. Будь-який користувач цієї мережі може мати доступ до актуальної версії реєстру, що робить його доступним абсолютно для всіх учасників [2].

На прикладі логістичних компаній можна побачити необхідність більшості підприємств підвищення якості контролю процесів діяльності. З кожним днем стає необхіднішою потреба в підвищенні прозорості перевезень та оптимізації їх контролю. Одним із способів вирішення проблем, шляхом вилучення людського фактору є використання блокчейну, яке підвищить рівень довіри клієнта та унеможливить несанкціоновані маніпуляції з даними.

Розглянемо середньостатистичну схему потоку продукту від виробника до клієнта та розділимо її на дві частини. Перша частина охоплює потік продукту А, від завантаження у постачальника А до прибуття його на центральний склад. В першій частині було виконано три замовлення, які складалися із чотирьох піддонів. Друга частина стосується

подорожі піддону з різними товарами, який також містить продукт А серед інших товарів, від завантаження на центральному складі до його прибуття та отримання в магазині клієнта. Причиною поділу потоку на дві частини було те, що центральний склад зберігає продукт А кілька тижнів, перш ніж його знову поставлять. Отже, потік одних і тих же ідентифікаторів продукту А не можна було б послідовно отримувати без значного збільшення часу на дослідження. Моделювання виконано з реальною інформацією, наданою різними учасниками ланцюга. Загальні покриті трансферти можна побачити на рисунку 1.

Всі учасники ланцюга поставок підтверджують свої дії через систему, яка використовує блокчейн. Після прибуття до постачальника А, водій вантажівки А отримав вантажні документи та перевірив, щоб замовлення були непошкоджені та кількість товарів була правильною. Коли водій вантажівки А завантажив чотири піддони, водій та постачальник переконалися, що штрих-код номера SSCC на кожному піддоні був відсканований. Використовуючи систему, постачальник А підтвердив передачу замовлень. Ця процедура виконується для кожного замовлення, яке було завантажено на вантажівку. Після підтвердження відправником перша передача замовлення була завершена, а цифровий підпис створено та збережено в блокчейні.

На шляху водій вантажівки А здійснюватиме розвантаження безпосередньо до вантажівки, яка здійснюватиме транспортування до центрального складу. Водій вантажівки В ініціалізував передачу, сканувавши штрих-код SSCC на одному з піддонів, і перевантажив замовлення у водія вантажівки А, учасники підтвердили дії таким же чином, як і в попередній передачі.

Коли три замовлення, що містили продукт А, надійшли на центральний склад, перша частина тесту була закінчена. Ця частина була виконана точно так само, як і попередні процедури передачі. Друга, змодельована частина починається, коли водій вантажівки С завантажує замовлення на центральному складі. Передбачено перевезення одного піддону з різнити товарами, що містив продукт А серед інших продуктів. Оскільки водій вантажівки С сканував штрих-код піддонів, інформація про замовлення була доступна йому, підтвердження передачі товару відбулося таким чином, як попередні завантаження, де учасники можуть прийняти або відхилити її.

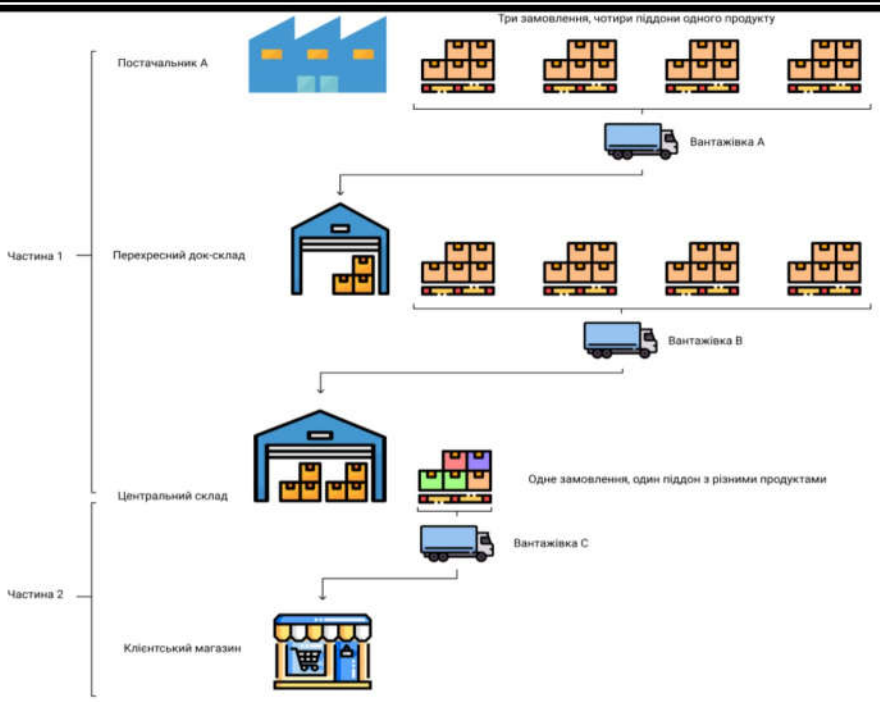


Рисунок 1 - Загальні трансфери

Остання частина тесту, після прибуття до магазину, водій вантажівки С підтвердили передачу товару. Як тільки водій вантажівки С підтвердив передачу, весь потік від постачальника А до магазину був покритий.

Менеджер під час транспортування може увійти та подивитися, де саме відбулося останнє перевезення, в який час та ким.

Висновки.

Блокчейн робить передачу даних швидше, безпечніше та дешевше, оскільки виключає участь посередників. З допомогою системи створюється унікальна довіра, тому що дані, що зберігаються в системі, неможливо змінити, це сприяє прозорості вантажних перевезень. В кінцевому результаті реалізована система дозволяє логістичним компаніям зміцнювати зв'язки зі своїми поточними клієнтами та залучати нових.

Перелік джерел

1. Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Int. Things J. 2018, *5*, pp.1184–1195.

2. What is Blockchain Technology? A StepbyStep Guide For Beginners [Електронний ресурс]. — Режим доступу: https://blockgeeks.com/guides/whatis blockchaintechnology/

3. Яцків Н.Г., Яцків С.В. Перспективи використання технології блокчейн в мережі Інтернет речей. Науковий вісник НЛТУ України. - 2016. - Вип. 26.8. – С. 381-387.

УДК 004.75

М.Ф. Драчук, Ю.В. Тимощук

Тернопільський національний економічний університет

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Вступ. В Інтернеті існує багато видів небезпек, в тому числі шкідливі програми і DDOS-атаки. Мережа може бути захищена від таких атак за допомогою системи виявлення вторгнень (Intrusion Detection System, IDS). IDS виявляє вторгнення і генерує попередження при виявленні вторгнення. Система виявлення вторгнень в мережі аналізує весь трафік. Для великих центрів обробки даних це складне завдання, так як є велика кількість даних, що проходять через мережу центру обробки даних [1].

З огляду на це, стає все більш важливим мати можливість виявляти і запобігати атакам на мережеві системи. Система виявлення вторгнень може попереджати адміністраторів про зловмисні дії. Щоб мати гарну продуктивність, більшості систем виявлення вторгнень потрібно багато ручного обслуговування. Ця теза намагається з'ясувати, чи може система виявлення вторгнень працювати "з коробки" з прийнятною продуктивністю. Це робиться за допомогою алгоритмів машинного навчання, які можуть вчитися і знаходити шаблони при введенні. Алгоритми машинного навчання мають хорошу перспективу вирішення проблеми автоматичного виявлення вторгнень. Тому в цій роботі робиться спроба побачити, що готова система виявлення вторгнень може мати хорошу продуктивність. Це робиться за допомогою алгоритмів машинного навчання, які можуть робити висновки з даних і шаблонів. Це здається цілком прийнятним до проблеми виявлення вторгнень [2, 3].

Метою роботи є дослідження систем виявлення вторгнень на основі машинного навчання.

1. Дослідження вимог до систем виявлення вторгнень

Системи виявлення вторгнень були ретельно досліджені, але більшість змін відбуваються в наборі даних, який містить багато зразків методів вторгнення, таких як груба сила, відмова в обслуговуванні або навіть проникнення зсередини мережі [4].

У міру зміни поведінки і моделей мережі, а також розвитку вторгнень, виникла необхідність переходу від статичних і одноразових

наборів даних до більш динамічно створюваним наборам даних, які не тільки відображають склад трафіку і вторгнення в реальному часі, але також є розширюваними і відтвореними.

Завдяки застосуванню алгоритмів машинного навчання в системі, виявлення на основі аномалій є більш ефективним серед систем виявлення вторгнень, оскільки йому не потрібно шукати певний конкретний шаблон аномалії, а скоріше вони просто обробляють все, що не відповідає профілю як «аномальний».

2. Розробка структури систем виявлення вторгнень на основі машинного навчання

Для побудови моделі алгоритму навчання використано техніку навчання з навчанням на попередньо навченій моделі VGG-19 Keras, структура якої зображення на рисунку 1.

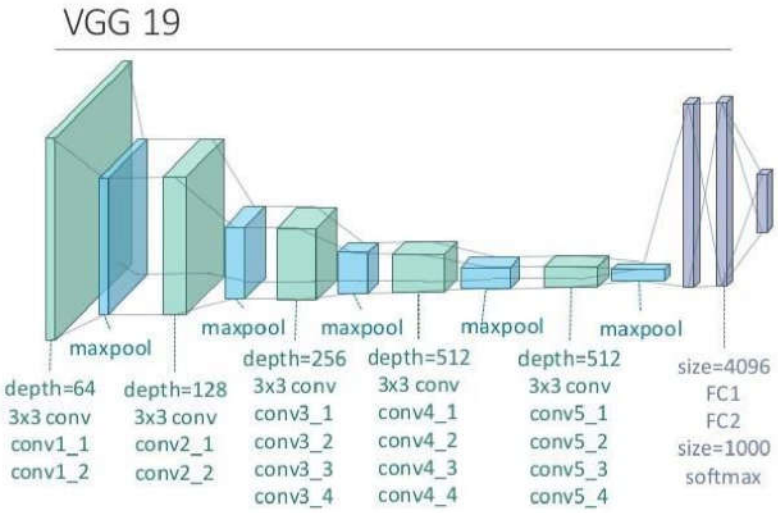


Рисунок 1 – Структура алгоритму машинного навчання VGG-19 Keras

Використано традиційний метод виявлення аномалій, який включає в себе дві фази:

- етап навчання. Етап, на якому створюється профіль звичайних корисних навантажень. Зазвичай будь-які дані про аномалії не потрібні для навчання, так як IDS миттєво відкидає будь-які дані з найменшим відхиленням від даних в профілі на наступному етап;

- етап тестування. Етап, на якому вхідні корисні дані порівнюються з даними, що зберігаються в профілі.

При цьому модель навчена на значеннях даних, теги яких були позначені як «Нормальні», і, в свою чергу, вона досягла 100% точності в

найпершу епоху. Однак з введенням значень даних про аномалії модель досягла точності 100%, що дозволило зробити висновок, що модель правильно визначила нормальні дані, проте в разі аномалій вона просто обійшла їх без класифікації.

Таким чином, використовувались, як данні про аномалії, так і нормальні дані в навчальних даних. На етапі тестування досягнуто задовільних результатів: модель змогла ідентифікувати нормальні дані з точністю 100% і аномальні дані з точністю 85%. З огляду на набір даних, отримані результати були задовільними. На рисунку 2 зображено графік точності моделі в двох епохах.

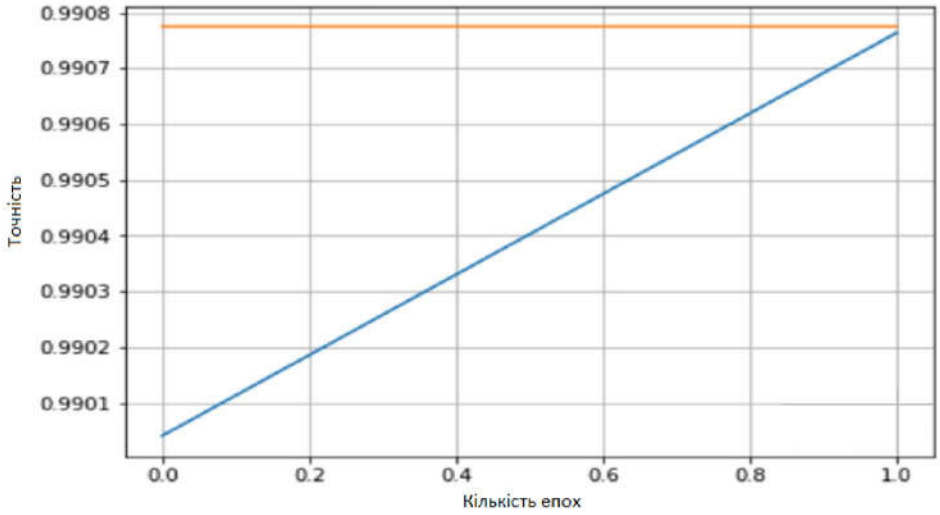


Рисунок 2 – Графік точності моделі

Висновки.

Робоблена модель виявлення вторгнень на основі машиного навчання може бути використана в якості внутрішнього механізму для додатку системи виявлення вторгнень, яку можна встановити для будь-якої комп'ютерної мережі.

Перелік джерел.

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський – К.: Видавнича група BHV, 2009 – 608с.

2. Завада А. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А. Завада, О. Самчишин, В. Охрімчук. – Житомир: Збірник наукових праць ЖВІ НАУ, 2012. – 106.

3. Климов, С. М. Противодействие компьютерным атакам. Методические основы / С. М. Климов, М. П. Сычёв, А. В. Астрахов. – М. : МГТУ им. Н. Э. Баумана, 2013. – 108 с.

4. Кузнецов А. The statistical analysis of a network traffic for the intrusion detection and prevention systems/ А. Кузнецов, Л. Г.Зайончик, О. С. Игнатенко, П. Р. Левковець. – Харків: Телекомунікації та радіотехніка, 2005. – 176 с.

УДК. 004.75

Д.Ю. Кузик

Тернопільський національний економічний університет

ДОСЛІДЖЕННЯ АЛГОРИТМІВ ЗАХИЩЕНОГО РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ВЕЛИКИХ ОБСЯГІВ ІНФОРМАЦІЇ

Вступ. На сьогоднішній день Big Data являється однією з найбільш актуальних тем, обсяг даних і їх збільшення зростає з кожною секундою і необхідно мати відповідні інструменти, щоб структурувати та захистити дані для подальшого використаннях[1].

Завдяки її широкому використанню практично у всіх сучасних галузях значно полегшується рішення багатьох практичних завдань. Дані із всіх пристроїв - комп'ютерів, планшетів та смартфонів - постійно збираються та передаються в мережу, та насправді це лише початок процесу.

Незабаром вся інформація буде потрапляти онлайн навіть з таких пристроїв, як годинники, телевізори, датчики в розумних будинках, авто, обладнання на виробництві та з безлічі інших девайсів. Крім того, можна самостійно продукувати гігабайти інформації[2].

Якщо підсумувати, то це інформація, що не піддається обробці класичними способами через її величезний об'єм[3].

Метою роботи є дослідження, застосування на практиці алгоритмів захищеного та розподіленого зберігання великих обсягів інформації та тестування системи з подальшим аналізом результатів.

1. Дослідження вимог до систем захисту та розподіленого зберігання великих обсягів інформації.

Питання збереження, обробки та захисту великих даних з кожним роком набуває все більшої актуальності, тому що такі дані настільки великі та складні, що жоден із традиційних засобів управління даними не в змозі їх зберігати чи обробляти ефективно.

Також великі дані відіграють велику роль через те, що на даний момент використовуються практично всюди, вони стали сировинним матеріалом бізнесу, життєво важливим економічним внеском, використовуваним для створення нової економічної вигоди [4].

Одним із прикладів використання великих даних є соціальні мережі, такі як Facebook, Instagram та інші.

Оскільки щодня одними лише соціальними мережами генерується сотні терабайт даних, система зберігання та обробки даних повинна бути толерантною до помилок або несправностей в окремих комп'ютерах.

Ще однією вимогою до системи є те, що вона повинна бути розподіленою, тобто паралельно вирішувати велику кількість задач.

З іншої сторони, кожен комп'ютер може мати свого власного користувача зі своїми індивідуальними потребами, і метою розподіленої системи є координація використання загальних ресурсів або надання послуг зв'язку для користувачів. Остатньою з вимог є надійність системи та захист інформації, яку вона зберігає[5].

Всі ці можливості надає вільна програмна платформа Hadoop.

2. Дослідження технології Hadoop для розробки систем розподіленого зберігання

Принцип реалізації системи захищеного розподіленого зберігання великих даних оснований на Hadoop. Hadoop – це фреймворк, який складається з набору утиліт для розробки і виконання програм розподілених обчислень.

Основними утилітами Hadoop є:

- HBase - NoSQL СУБД, ефективно підтримує читання і запис;
- Pig - мова обробки даних і середовище виконання;
- SPARK - набір інструментів для реалізації розподілених обчислень;
- Hive - сховище даних з інтерфейсом SQL;
- ZooKeeper - сховище конфігураційної інформації.

При правильній архітектурі системи, інформація про те, на яких машинах розташовані блоки даних, дозволяє запустити на них же обчислювальні процеси і виконати більшу частину обчислень локально, тобто без передачі даних по мережі. Саме ця ідея лежить в основі парадигми MapReduce і її конкретної реалізації в Hadoop.

Класична конфігурація кластера Hadoop складається з одного сервера імен, одного майстра MapReduce і набору робочих машин, на кожній з яких одночасно крутиться сервер даних (DataNode) і Воркер (TaskTracker).

Кожна MapReduce робота складається з двох фаз:

- map - виконується паралельно і (по можливості) локально над

кожним блоком даних. Замість того, щоб доставляти терабайти даних до програми, певна програма копіюється на сервера з даними і робить з ними все, що не вимагає перемішування і переміщення даних (shuffle).

- reduce - доповнює map агрегуються операціями. Насправді між цими фазами є ще фаза combine, яка робить те ж саме, що і reduce, але над локальними блоками даних.

Далі за допомогою combine можна відфільтрувати рядки з повідомленням про помилку на рівні одного сервера, а потім за допомогою reduce зробити те ж саме на рівні всіх даних.

Все, що можна було розпаралелити (розподілити) було розподілене, і крім того була мінімізована передача даних між серверами. І навіть якщо якась задача з якоїсь причини впаде, Hadoop автоматично перезапустить її, піднявши з диска проміжні результати.

Висновки.

Досліджений фреймворк (Hadoop) було обрано для реалізації системи. Враховуючи предмет дослідження та специфіку даного завдання, було сформульовано постановку задачі, де описано основні проблеми, які треба вирішити для створення програмного продукту за допомогою якого можна дослідити ефективність застосування системи розподілених обчислень Hadoop.

Список джерел.

1. Hadoop: що, де та навіщо? - Електронний ресурс. Режим доступу: https://habr.com/ru/post/240405/

2. What is BIG DATA? - Електронний ресурс. Режим доступу: https://intellipaat.com/blog/tutorial/hadoop-tutorial/big-data-overview/

3. M. Kasianchuk. Theoretical Foundations of the Modified Perfect form of Residue Number System / M. Kasianchuk, Ya. M. Nykolaychuk, , I. Z. Yakymenko // Cybernetics and Systems Analysis. – March, 2016. -Volume 52, Issue 2. – pp.219-223.

4. Karpinski M. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes / M. Karpiński, S. Ivasiev, I. Yakymenko, M. Kasianchuk ,T. Gancarczyk// Proc. of 16th International Conference on Control, Automation and Systems (ICCAS–2016) – Gyeongju, Korea. – V.1. – October, 2016. – P.1484–1486.

5. Николайчук Я.М. Метод збереження простих великорозрядних чисел у базисі Радемахера / Я.М. Николайчук, І.З. Якименко, М.М. Касянчук, С.В. Івасьєв // Праці міжнародної молодіжної математичної школи —Питання оптимізації обчислень (ПОО-XXXVII)‖. Київ: Інститут кібернетики імені В.М. Глушкова НАН України. - 2015. –С. 159-161.

УДК 004.75

Н.І.Садовий, В.С.Шаршин

Тернопільський національний економічний університет

АЛГОРИТМ ВІДНОВЛЕННЯ ФАЙЛІВ В СИСТЕМІ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ДАНИХ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Вступ. Роль і важливість системи надійного зберігання даних визначається постійно зростаючою цінністю інформації в сучасному суспільстві, можливість доступу до даних і управління ними є необхідною умовою для ефективного виконання бізнес-процесів. Безповоротна втрата даних піддає бізнес організації серйозній небезпеці. Втрачені обчислювальні ресурси можна відновити, а втрачені дані, за відсутності грамотно спроектованої і впровадженої системи резервування, вже не підлягають відновленню [1].

На сьогодні можна знайти багато рішень цього питання, наприклад, створення RAID-масиву чи просте копіювання на флеш-носій чи оптичний диск, копіювання на віддалений FTP-сервер чи окремий жорсткий диск, а можливо й віддалене зберігання інформації за допомогою «хмарного» сервісу [2].

Метою роботи є розробка системи надійного зберігання даних з використання перетворення системи залишкових класів та розподіленого зберігання частин файлу.

1. Дослідження вимог до системи надійного зберігання даних

Основною вимогою системи зберігання даних є надійність, яка досягається завдяки особливості системи залишкових класів. Для перетворення числа з десяткової системи числення в систему залишкових класів використовуються деякі прості числа (модулі), які використовуються для отримання залишків від числа. Кількість модулів прямо пропорційне кількості отриманих залишків і відповідно частин файлу. Згідно з алгоритмом перетворення, з системи залишкових класів в десяткову систему числення, для отримання початкового числа необхідно лише три будь-які залишки або n-1 залишок, де n – кількість модулів.

В даному випадку, система перетворюватиме файл в чотири файли, які залишки і для відновлення початкового файлу, системі необхідно буде лише три з них. Для збільшення надійності, файли залишки будуть

завантажуватися на хмарні сховища зберігання даних. Для перевірки незмінності файлу залишку обчислюємо хеш функцію SHA-1.

2. Алгоритм роботи системи надійного зберігання даних

Алгоритм перетворення файлу в систему залишкових класів і завантаження на хмарні сховища зображено на рисунку 1.

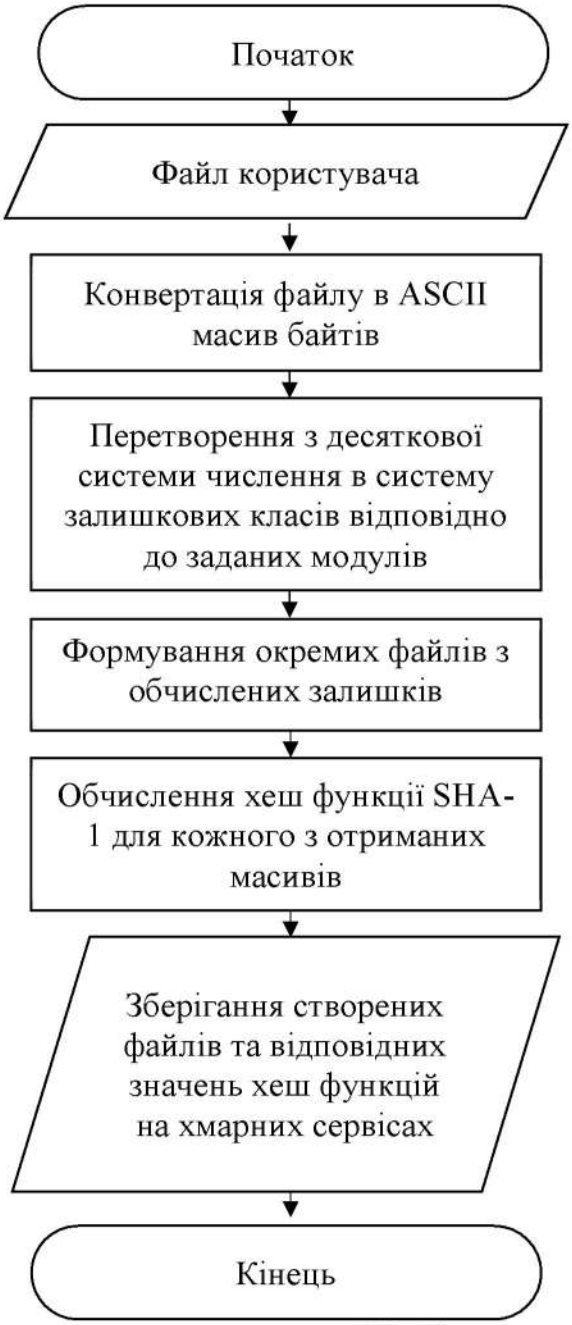


Рисунок 1 – Алгоритм перетворення в СЗК і завантаження на хмарні сховища

Алгоритм завантаження файлів залишків з хмарних сховищ і перетворення в початковий файл зображено на рисунку 2.

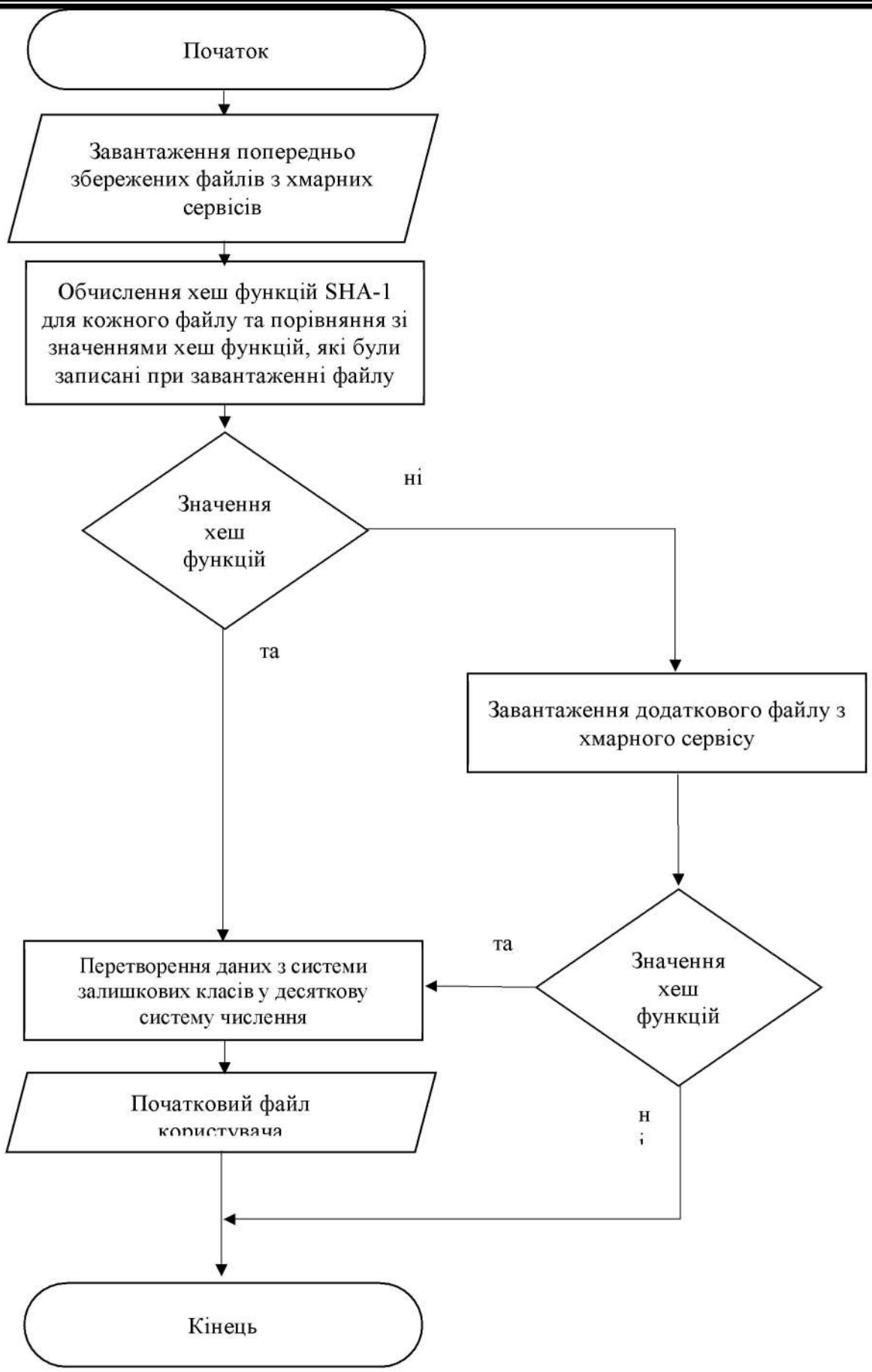


Рисунок 2 – Алгоритм відновлення файлів із залишків збережених на хмарних сховищах

Завантажений файл користувача перетворюється в масив байтів. Після цього, кожен елемент масиву перетворюється з десяткової системи в систему залишкових класів. Кожен залишок записується в окремий масив. Після обробки всіх елементів масиву з отриманих масивів залишків розраховуються хеш функції SHA-1, які записуються в базу даних.

Кожен масив, що містить залишки, записується в файл, який звантажується на хмарний сервіс зберігання даних. Спершу завантажуються файли залишки з хмарних сховищ і перетворюються в масиви байтів. З кожного масиву розраховуються SHA-1 хеші, які порівнюються з значеннями хеш функцій з бази даних, які були записані при завантаженні файлу.

Якщо значення хеш функцій рівні, система продовжує роботу - відновлює інформацію з файлів, перетворює дані з системи залишкових класів у десяткову систему числення.

Якщо одне із обчислених значень хеш функцій не співпадає зі збереженим в базі значенням, то для відновлення файлу необхідно завантажити додатковий файл з хмарного сервісу.

Якщо не співпадають два або більше обчислених значення хеш функцій зі збереженими, то відновлення початкового файлу не можливе.

Висновки.

Запропонований алгоритм зберігання даних, з використанням системи залишкових класів, забезпечує надійне зберігання інформації шляхом зберігання файлів залишків на хмарних сховищах і можливості відновлення початкової інформації з трьох файлів залишків при використанні чотирьох модулів.

Перелік джерел.

1. Ковалев В. Безопасность в системах хранения данных // LAN Magaine. 2005. № 6. С.56-62;

2. Randy H. Katz, RAID: A Personal Recollection of How Storage Became a System, IEEE Annals of the History of Computing, Volume 32, Number 4, October-December 2010, pp. 82-86 (Article);

3. Omondi, A. R., & Premkumar, B. (2007). Residue number systems: theory and implementation (Vol. 2). World Scientific.

УДК 681.3

В.І. Воляк [1], М.В. Філіпович [1], В.В. Лукіянчук[2], М.Й. Джугла[2]

[1]Тернопільський національний економічний університет

[2]Опорний заклад Теребовлянська загальноосвітня школа І-ІІІ ступенів №1 Теребовлянської міської ради

АЛГОРИТМ СИМВОЛЬНОГО РОЗЧЕПЛЕННЯ ПО ВЕКТОРНІЙ БАЗІ

Вступ. У США К. Шеннон в 1944 р створив основи теорії секретного зв'язку. У його роботах викладається теорія так званих секретних систем, службовців, фактично, математичною моделлю шифрів [39, 55]. З тих пір при розробці нових класів шифрів широко використовується принципи розсіювання і перемішування К. Шеннона.

У роботі для захисту текстової інформації пропонується скористатися певним узагальненням відомої арифметичної операції ділення із залишком. Це узагальнення дозволяє скористатися аналогією з відповідними роботами К. Шеннона про стійкість систем захисту. В якості такого узагальнення запропоновано так зване розщеплення к-го рівня по векторній базі, що дозволяє користувачеві вибирати рівень захисту в залежності від різних вимог, що пред'являються до якості захисту.

Тому дослідження властивостей пропонованого нового методу захисту текстової інформації, чому присвячена робота, є актуальним завданням, що виникає як у зв'язку з передачею по мережах зв'язку, так і з появою таких нових способів зберігання інформації, як хмарна технологія.

Метою роботи є дослідження алгоритмів символьного розчеплення по векторній базі.

1. Алгоритм розщеплення по векторній базі

Розщеплення по векторної базі - це узагальнене розщеплення рівня k по векторній базі $\vec{r} = (r_1, r_2, \dots, r_l)$, коли черговий ($i$-й) крок процесу цілочисельного розщеплення виконується при новому значенні бази розщеплення.

Таке розщеплення виявляється найбільш корисним в додатках, пов'язаних із захистом інформації, що передається.

Передбачається, що канал зв'язку безшумний, тобто перешкоди в каналі зв'язку відсутні. Однак наявність перешкод можна грубо оцінити

теоретично при передачі замість символу його розщеплення.

Нехай ε - ймовірність помилки при передачі одного числа. Тоді ймовірність безпомилкової передачі одного числа дорівнює (1- ε). Імовірність безпомилкової передачі всіх k чисел дорівнює $(1-\varepsilon)^k$. Тому при наявності перешкод збільшення k не вигідно. І може знадобитися застосування теоретико-інформаціоного кодування. Однак в цій роботі буде всюди передбачатися, що канал зв'язку є безшумним, як у випадку передачі даних між двома комп'ютерами по виділеній лінії.

Узагальненим цілочисельним розщепленням числа a по векторній базі $\vec{r} = (r_1, r_2, \dots, r_l)$ називається уявлення a у вигляді послідовності чисел $a_1, a_2, a_3, \dots, a_{k-1}, a_k$, в якій:

$$a_1 = \delta^{(2)}, \text{ де } \delta^{(2)} = r_1 mod\ a, r_1 > a,$$

$$a_2 = \delta^{(3)}, \text{ де } \delta^{(3)} = r_2 \bmod q^{(2)}, q^{(2)} = \left\lfloor \frac{r_1}{a} \right\rfloor, r_2 > q^{(2)},$$

$$a_3 = \delta^{(4)}, \text{ де } \delta^{(4)} = r_3 mod\ q^{(3)}, q^{(3)} = \left\lfloor \frac{r_2}{q^{(2)}} \right\rfloor, r_3 > q^{(3)} \dots$$

$$a_{k-1} = \delta^{(k)}, \text{ де } \delta^{(k)} = r_{k-1}\ mod\ q^{(k-1)}, q^{(k-1)} = \left\lfloor \frac{r_{k-2}}{q^{(k-2)}} \right\rfloor, r_{k-1} > q^{(k-1)},$$

$$a_k = q^{(k)}, \text{ де } q^{(k)} = \left\lfloor \frac{r_{k-1}}{q^{(k-1)}} \right\rfloor,$$

де δ - залишок при цілочисельному розподілі r_i/a,

символ $\lfloor\ \rfloor$ означає округлення до найближчого цілого в меншу сторону,

k – рівень розщеплення.

Отже, цей математичний апарат є узагальненням схеми математичного цілочисельного розщеплення.

Висновки.

Розглянутий у статті алгоритм цілочисельного розчеплення чисел по векторній базі дозволяє ефективно застосовувати його в симетричних системах захисту інформації і поряд з цим, забезпечувати необхідний рівень захисту.

Перелік джерел.

1. Алферов А.П. Основы криптографии// А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин /Москва: Гелиос АРВ. – 2005. - 480 с.

2. Шеннон К. Работы по теории информации и кибернетике // Издательство иностранной литературы, Москва. - 1963. - 829 с.

УДК 004.75

Т.Г. Цаволик, О.В. Небесний

Тернопільський національний економічний університет

СИМЕТРИЧНИЙ АЛГОРИТМ ШИФРУВАННЯ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Вступ. Однією з важливих для сучасних автоматизованих систем є проблема забезпечення конфіденційності інформації [1 − 3], для вирішення якої застосовуються ті чи інші методи, методики чи алгоритми. Для забезпечення конфіденційності інформації в багатьох випадках криптографічне перетворення є чи не єдиним шляхом забезпечення її конфіденційності. На цей час теорія криптографічних перетворень розвинута досить широко й для забезпечення конфіденційності інформаційних об'єктів можна застосувати ті чи інші алгоритми криптографічного перетворення. Для шифрування інформації серед інших можуть використовуватися і аналітичні перетворення [4, 5].

Метою роботи є дослідження симетричного алгоритму системи залишкових класів.

1. Особливості симетричного алгоритму

Симетричні алгоритми, які іноді називають умовними алгоритмами, це ті, в яких ключ зашифрування може бути розрахований з ключа розшифрування, і навпаки. У більшості симетричних алгоритмів ключі зашифрування і розшифрування ті самі. Ці алгоритми, також звані алгоритмами з секретним ключем або алгоритмами з єдиним ключем, вимагають, щоб відправник і одержувач погодили використовуваний ключ перед початком передачі секретних повідомлень. При передачі саме повідомлення, яке передається, повинно залишатися таємними, а ключ повинен зберігатися в секреті.

Симетричні алгоритми шифрування засновані на тім, що відправник і одержувач інформації використовують той самий ключ. Цей ключ повинний зберігатися в таємниці і передаватися способом, що виключає його перехоплення. Обмін інформацією здійснюється в 3 етапи:

– відправник передає одержувачу ключ (у випадку мережі з декількома абонентами в кожної пари абонентів повинний бути свій ключ, відмінний від ключів інших пар);

– відправник, використовуючи ключ, зашифровує повідомлення, що пересилається одержувачу;

– одержувач одержує повідомлення і розшифровує його.

На рисунку 1 представлена загальна схема шифрування та дешифрування.

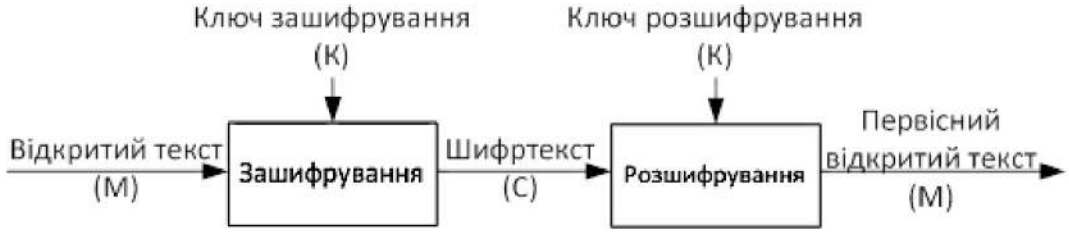


Рисунок 1 – Операції шифрування та дешифрування в симетричних алгоритмах

Якщо кожного разу міняти ключ для дешифровки повідомлення, то це підвищить надійність передачі даних.

Висновки.

Таким чином, аналіз криптографічної стійкості механізмів блокових матричних перетворень дає можливість стверджувати, що способи криптоаналізу шляхом "статистичного" аналізу з використанням фрагментів відкритого та зашифрованого тексту, спроби обрахування прямих чи зворотних матриць, при дотриманні викладених у відповідних розділах рекомендацій, є не результативними, а кількість варіантів ключових наборів є не меншою ніж для інших відомих механізмів формування контрольних ознак.

Перелік джерел.

1. Алфьоров А. П., Зубов А Ю., Кузьмін А. С., Черьомушкін А.В. Основи криптографії: Навчальний посібник. 3-тє вид., Випр. і доп. - М.: 2005. - 480с.

2. Введення в криптографію / За заг. ред. В. В. Ященко. - 3-е вид., Доп. - М.: 2000.- 288с.

3. Нечаєв В. І. Елементи криптографії (Основи теорії захисту інформації): Учеб. Посібник для ун-тів і пед. вузів. / За ред. В. А. Садовнича - М.: Вищ. шк., 1999 - 109с. Василенко В. С.

4. Варіант завадостійкого криптографічного перетворення // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні, вип. 8, 2004 р. –с. 101 – 108. Василенко В. С.

5. Блокові криптографічні перетворення з використанням лишкових класів // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні, вип. 8, 2004 р. – с. 101

УДК 681.3

С.М. Павловський[1], С.А. Шандалюк[1], М.І. Безух[2], Г.Є. Козбур[3]

[1]Тернопільський національний економічний університет,

[2]Тернопільська загальноосвітня школа №23,

[3] Тернопільський технічний ліцей

СУЧАСНІ МЕТОДИ ТА ПІДХОДИ В РЕАЛІЗАЦІЇ СИСТЕМ КВАНТОВОЇ КРИПТОГРАФІЇ

Вступ. Серед областей науки і технологій, в яких за останні роки досягнуто помітного прогресу, по праву своє місце зайняла квантова криптографія. Народившись близько 30 років тому на стику квантової механіки і традиційної криптографії, квантова криптографія досягла найбільших результатів в сфері практичних програмних рішень, що мають безпосереднє відношення до питань забезпечення інформаційної безпеки.

В даний час можна спостерігати бурхливий розвиток телекомунікацій а також автоматизованих засобів збору, зберігання і обробки інформації. В свою чергу це вимагає розробки нових криптографічних методів, що забезпечують захист при передачі і зберіганні даних.

Метою роботи є дослідження сучасних методів та підходів у реалізації систем квантової криптографії.

1. Квантові схеми

Для того, щоб описати квантовий алгоритм часто використовують різного типу квантові схеми, які в свою чергу можуть складатись з безлічі квантових вентилів, що застосовуються до квантового реєстру в визначеній та чіткій послідовності. Наприклад, такі алгоритми як квантове перетворення Фур'є або алгоритм Шора можуть бути графічно представлені у вигляді схеми, що складається з серії простих квантових вентилів - операторів Адамара, операторів фазового зсуву і т.д. Іншими словами, математично це квантова схема, комплексне унітарне перетворення, матриця якого є добутком матриць окремих квантових вентилів.

На даний момент ведеться мова про створення інтерфейсу між носіями квантової інформації (світловими квантовими станами) і квантової пам'яттю і квантовими процесорами (атомами, іонами, твердими тілами), які є інтегруючою частиною повномасштабних квантових ІС. Поки час зберігання інформації в квантової пам'яті становить близько 4 мс, що

дозволяє передавати квантову інформацію на відстань до 1000 км.

Сьогодні здійснюється кілька проектів зі створення квантових інтерфейсів, ретрансляторів, квантової пам'яті і навіть квантових ідентифікаційних карт.

Важливим напрямком є створення квантових генераторів випадкових чисел, заснованих на елементарному оптичному процесі. Фотони світла від джерела один за одним направляються на напівпрозоре дзеркало і детектируются двома приймачами, спрацьовування одного з яких асоціюється з одиницею, а іншого - з нулем. Побудовані за цим принципом КГСЧ з вбудованим моніторингом можливих збоїв серійно випускаються в ряді країн і мають швидкість генерації до 16 Мбіт / с. Один з КГСЧ був сертифікований однією з всесвітньо відомих компаній, що тестують гри для онлайнових ігрових додатків.

Послідовність операцій над q-бітами зручно представляти у вигляді квантових схем. На рисунку нижче (рисунок 1) зображений приклад схеми, яка створює синглетний стан:

$$\mathrm{CNOT}_{12}\ \mathrm{H}^{(1)}\ \ \sigma_x^{(1)}\ \ \sigma_x^{(2)}\ \ |00\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

де CNOT_12 - це операція контрольоване НЕ, яка «перевертає» контрольований q-біт 2 в залежності від стану контролюючого q-біта 1 а верхні індекси позначають q-біт, на який діє оператор.

На самому початку схеми зображуються q-біти в їх початковому стані $|0\rangle$.

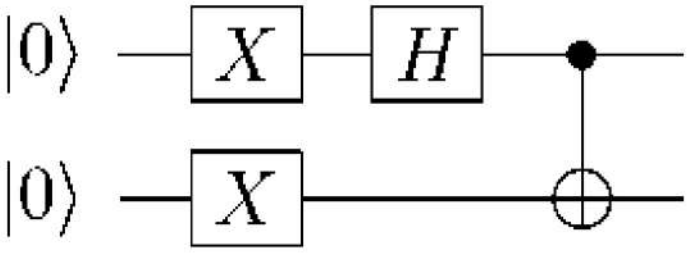


Рисунок 1 – Приклад схеми, яка створює синглетний сигнал

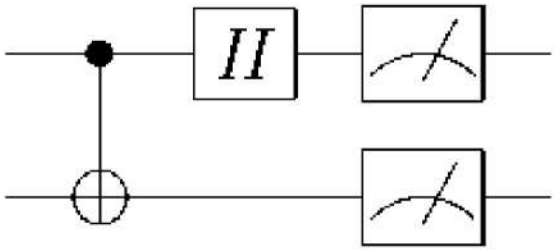
Прямокутники, які називаються квантовими вентилями (quantum gates), позначають унітарні операції над q-бітами. Процес вимірювання позначається як ψ. Зазвичай під таким знаком вимірюванням розуміється вимірювання в обчислювальному базисі $\{|0\rangle, |1\rangle\}$, і це є проектування на власні стани матриці Паулі σ_z.

Можна показати, що вимірювання в будь-якому бажаному базисі можна звести до вимірювання в обчислювальному базисі. Розглянемо базис Бела, який є ортонормованим базисом в просторі двох q-бітів

$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\psi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\psi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Ці вектори можна отримати з станів |00⟩, |01⟩, |10⟩, |11⟩ послідовним застосуванням операторів H^((1))і CNOT_12. Застосування цих операторів в зворотному порядку з наступним виміром в результаті дасть вимірювання в базисі Белла. Такому виміру відповідає наступна квантова схема:



Дійсно, нехай система з двох q-бітів знаходиться в стані $|\phi\rangle$. Тоді схема діє на цей стан наступним чином:

$$M_k H^{(1)} CNOT_{12} |\phi\rangle,$$

де M_1 = |00⟩ ⟨00|,
M_2 = |01⟩ ⟨01|,
M_3 = |10⟩ ⟨10|,
M_4 = |11⟩ ⟨11|.

Перемножимо оператори зліва:

$$|00\rangle\langle 00| H^{(1)} CNOT_{12} = \frac{1}{\sqrt{2}} |00\rangle(\langle 00| + \langle 11|) = B_1,$$

$$|01\rangle\langle 01| H^{(1)} CNOT_{12} = \frac{1}{\sqrt{2}} |01\rangle(\langle 01| + \langle 10|) = B_2,$$

$$|10\rangle\langle 10| H^{(1)} CNOT_{12} = \frac{1}{\sqrt{2}} |10\rangle(\langle 00| - \langle 11|) = B_3,$$

$$|11\rangle\langle 11| H^{(1)} CNOT_{12} = \frac{1}{\sqrt{2}} |11\rangle(\langle 01| - \langle 10|) = B_4.$$

Таким чином, оператори B_k проводять вимірювання в базисі Белла (7), а оператори:

$$B_1^* B_1 = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|),$$

$$B_2^* B_2 = \frac{1}{2}(|01\rangle + |10\rangle)(\langle 01| + \langle 10|),$$

$$B_3^* B_3 = \frac{1}{2}(|00\rangle - |11\rangle)(\langle 11| - \langle 11|),$$

$$B_4^* B_4 = \frac{1}{2}(|01\rangle - |10\rangle)(\langle 01| - \langle 10|)$$

Аналіз показав, що в останні роки одними з найбільш обговорюваних проблем стали проблеми теорії складності квантових обчислень, розширення класу ефективних квантових алгоритмів і забезпечення стійкості квантових обчислень стосовно до різних моделей КВ, зокрема за рахунок використання методів квантової корекції помилок.

Роботи по конструюванню елементної бази квантових комп'ютерів, які перебували більше 10 років в стадії експериментальних досліджень вже зараз почали виходити на рівень проектування прототипів обчислювачів, що виконують квантові алгоритми.

2. Квантові пристрої IBM

IBM Quantum Experience – це хмарна платформа, яка представляє можливість роботи на квантовому комп'ютері. Пристрої побудовані на надпровідних q-бітах, робота яких заснована на ефекті Джозефсона [4]: між зверхпровідниками, розділеними тонким шаром діелектрика, тече струм. В даний момент IBM надає доступ до одного W-q-бітного пристрою ibmqx5 і двом 5- q -бітними ibmqx2 і ibmqx4.

У квантових пристроях IBM все q-біти мають різні частоти роботи. Для застосування двох- q-бітних вентилів потрібно встановити взаємодію між потрібними квантовими бітами і мінімізувати з іншими. Для цього використовується межрезонансний ефект (cross-resonance effect) [5], в якому контролюючий q-біт опромінюється мікрохвильовим імпульсом, частота якого дорівнює частоті роботи контрольованого q-біта.

Процес вимірювання виконується в такий спосіб. Кожен q-біт слабо зв'язується з мікрохвильовим резонатором, резонансні характеристики якого залежать від стану q-біта.

Потім в резонатор надсилається високочастотний імпульс, після чого аналізується прийшов з резонатора сигнал. Амплітуда і фаза цього сигналу будуть відрізнятися від вихідних в залежності від стану q-біта.

Також IBM надає інформацію про деякі властивості своїх квантових комп'ютерів (рисунок 1): часи T1 і T2, що характеризують когерентність станів, помилки читання (readout errors) і помилки застосування одно-q-бітних (gate error) і двох-q-бітних (MultiQubit gate error) вентилів.

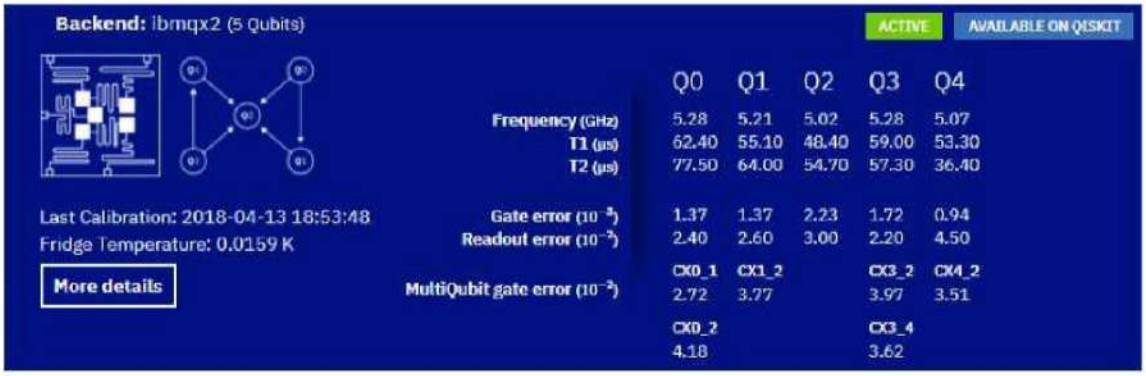


Рисунок 1 – Інформація про квантовий пристрій ibmqx2

Помилка застосування вентилів показує, наскільки точно виконуються ті чи інші операції над q-бітами. Для того, щоб обчислити значення помилки, проводиться наступна процедура. До q-бітів, приготованим в початковому стані $|\psi o\rangle$, застосовується випадкова послідовність вентилів, але таким чином, щоб кінцевий стан було таким же, як і початковий. Після застосування операцій квантові біти знаходяться в стані, описуваному матрицею щільності ρ. Потім обчислюється величина:

$$F = \langle\psi_0|\rho|\psi_0\rangle,$$

яка показує ступінь збігу початкового стану з кінцевим.

Тоді помилкою застосування вентилів буде величина (1 - F). Іноді при вимірюванні q-біта, який знаходиться в стані $|0\rangle$ або $|1\rangle$, можна отримати неправильні результати -1 і 1 відповідно.

Відомо, що будь-який унітарний оператор і, діючий в про-просторі q-біта, можна представити у вигляді Z-Y-розкладання:

$$U = \mathrm{R_z}(\varphi)\mathrm{R_y}(\theta)\mathrm{R_z}(\lambda) = \begin{bmatrix} e^{-i(\varphi+\lambda)/2}\cos(\theta/2) & -e^{-i(\varphi-\lambda)/2}\sin(\theta/2) \\ e^{i(\varphi-\lambda)/2}\sin(\theta/2) & e^{i(\varphi+\lambda)/2}\cos(\theta/2) \end{bmatrix},$$

де $\mathrm{R_y}(\theta)$, $\mathrm{R_z}(\theta)$ - оператори обертання навколо осей y і z на кут θ. Таким чином, будь-який одно-q-біт вентиль може бути заданий через параметр трьома числами φ, θ та λ.

Помилка читання визначається як відношення числа таких помилкових вимірювань до загальної кількості вимірювань. Калібрування пристроїв і вимірювань значень згаданих вище значень проводяться два рази на добу.

Крім квантових пристроїв, IBM надають доступ до двох симуляторам квантових обчислень. Перший з них може симулювати роботу до 20-ти q-бітів і дозволяє застосовувати деякі зумовлені умовні операції (застосування певного вентиля в залежності від стану одного або двох q-бітів), в той час як другий симулює обчислення на 32-х q-біти без можливості застосувань умовних операцій.

Висновки.

Таким чином, комерційні варіанти та рішення в галузі квантової технології захисту інформації можливі та існують лише в такому методі, як квантовий розподіл ключів. Ці дані потім використовуються для класичного симетричного шифрування. Дуже активною галуззю на даний час залишаються аспекти безпеки та захисту квантової криптографії, що на даний час постійно розвиваються. Перешкодами для цього можна вважати лише технологічні складності, проте і вони на мою думку будуть вирішені в найближчому майбутньому.

Пост-квантові криптографічні системи у своєму розвитку показують набагато нижчі результати і в цілому розвиваються повільніше. До однієї з можливих причин можна віднести те, що існують різні протиріччя теоретичної і практичної крипостійкості між системами асиметричного шифрування, які основані на задачах теорії граток. Проте це відкриває перспективний напрямок прикладних математичних досліджень в даній галузі пост-квантової криптографії.

Перелік джерел.

1. Daniel Gottesman and Isaac Chuang. Quantum digital signatures. Technical Report arXiv:quant-ph/0105032, Cornell University. Library, Nov 2001.

2. Гриб А.А Неравенства Белла и экспериментальная проверка корреляций на макроскопических расстояниях // Успехи физ. наук. 1984. Vol. 4. P. 619 - 634.

Science, 378(1):101- 116, Jun 2007.

3. Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum Engerprinting. Phys. Rev. Lett, 87(16): 167902, Sep 2001.

4. Килин С.Я., Хорошко Д.Б., Низовцев А.П. Квантовая криптография: идеи и практика. Минск: Беларуская наука, 2007.

5. Chow J. M., Corcoles A. D., Gambetta J. M. et al. Simple All-Microwave Entangling Gate for Fixed-Frequency Superconducting Qubits // Phys. Rev. Lett. 2011. Vol. 107. P. 080502.

УДК 004.75

Т.Г. Цаволик, О.В. Небесний

Тернопільський національний економічний університет

АЛГОРИТМИ ШИФРУВАННЯ ІНФОРМАЦІЇ В СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Вступ. Шифрування – це оборотне перетворення даних, з метою приховування інформації. Шифрування відбувається із застосуванням криптографічного ключа. Ключ – це певна кількість символів, сформованих вільним чином з символів, що доступні у системі шифрування [1].

Те, що в 60-і роки називалося комп'ютерною безпекою, а в 70-і - безпекою даних, зараз більш правильно іменується інформаційною безпекою. Інформаційна безпека підкреслює важливість інформації в сучасному суспільстві - розуміння того, що інформація – це коштовний ресурс, щось більше, ніж окремі елементи даних.

Загалом виділяють два методи шифрування:

- симетричне;
- асиметричне.

У симетричному шифруванні – один ключ, який зберігається в секреті, служить і для шифрування, і для дешифрування, а в асиметричному алгоритмі шифрування для зашифровування інформації використовується один відкритий ключ, но для дешифрування – використовується закритий ключ [2].

Оскільки в асиметричному алгоритмі шифрування ключі є різні і отримати їх один з одного не можливо.

Головне досягнення асиметричного шифрування в тому, що воно дозволяє людям, що не мають наперед наявної домовленості про безпеку, обмінюватися секретними повідомленнями [2].

Метою роботи є дослідження алгоритмів шифрування даних в системі залишкових класів.

1. Дослідження шифрування даних

Більшість засобів захисту інформації базується на використанні криптографічних шифрів і процедур шифрування – дешифрування. Основною характеристикою шифру є криптостійкість, яка визначає його стійкість до розкриття методами криптоаналізу.

Зазвичай ця характеристика визначається інтервалом часу, необхідним для розкриття шифру.

До шифрів, що використовуються для криптографічного захисту інформації, пред'являється ряд вимог:

– висока криптостійкість; –

– простота процедур шифрування і дешифрування; –

– незначна надлишковість інформації за рахунок шифрування;

– нечутливість до невеликих помилок шифрування та ін.

До таких вимог належать такі шифри:

– шифрування перестановкою полягає в тому, що символи шифрованого тексту переставляються за певним правилом в межах деякого блоку цього тексту;

– шифрування заміною (підстановкою) полягає в тому, що символи шифрованого тексту замінюються символами того ж або іншого алфавіту відповідно до заздалегідь обумовленої схемою заміни;

– шифрування аналітичним перетворенням полягає в тому, що шифрований текст перетворюється за певним аналітичним правилом (тобто за формулою).

Процеси шифрування і дешифрування здійснюються в рамках деякої криптосистеми.

Характерною особливістю симетричною криптосистеми є застосування одного і того ж секретного ключа як при шифруванні, так і при розшифрування повідомлень.

Висновки.

Алгоритми шифрування використовуються майже у всіх програмах для передачі важливих даних, а також в банківських і державних установах, системах безпеки. Головним чином, шифрування служить завданням дотримання конфіденційності інформації, що передається. Важливою особливістю будь-якого алгоритму шифрування є використання ключа є його надійність.

Перелік джерел.

1. Handbook of Applied Cryptography. Alfred J. Menezes; Paul C. van Oorschot; Scott A. Vanstone (August 2001).

2. [Електронний ресурс]. Режим досутпу: https://en.wikipedia.org/wiki/Public-key_cryptography.

УДК 681.32

О.О. Чубей[1], А.З. Шумський[2], С.В. Івасьєв[2]

[1]Галицький коледж ім. В. Чорновола

[2]Тернопільський національний економічний університет

ВИЗНАЧЕННЯ ІНТЕРВАЛЬНОГО РІШЕННЯ ЗАДАЧІ ФАКТОРИЗАЦІЇ ДЛЯ КРИПТОГРАФІЧНИХ СИСТЕМ

Вступ. Важливим напрямком розвитку досліджень у галузі методів та програмно-апаратних засобів опрацювання цифрових даних є вдосконалення алгоритмів, які використовуються в сучасних комп'ютерних системах, та розвиток математичних основ теорії чисел на базі кодових систем різних теоретико-числових базисів, до яких належать: унітарний, Хаара, Радемахера, Крестенсона, Уолша, Галуа тощо[1,2]. До таких задач відноситься задача факторизації багаторозрядних чисел, оскільки на основі її високої обчислювальної складності базуються сучасні криптосистеми RSA, Рабіна.

Метою роботи є дослідження визначення інтервального рішення задачі факторизації для криптографічних систем.

1. Метод визначення околу рішення задачі факторизації

Метод Ферма ґрунтується на розв'язанні діофантового рівняння виду:

$$F_k - P_0 = \overset{\bullet}{\Delta}^2 \qquad (1)$$

де P_0 – відоме число, яке рівне добутку двох багаторозрядних простих чисел, Fk - повний квадрат:

$$P_0=P_1\times P_2 \qquad (2)$$

Метод пошуку P_1 і P_2 є складним, оскільки потрібно здійснювати операцію ділення над БРЧ, що призводить до експоненційного зростання складності:

$$\frac{P_0}{\breve{P}_1} = P_2 \ , \ P_1<P_2 \qquad (3)$$

При розрядності 100 – 1000 біт P_0 і відповідно 50 – 500 біт P_1 та P_2 приводить до пошуку тільки одного розв'язку у цілих числах у діапазоні $2^{50} - 2^{500}$ [3].

Дослідження операції множення багаторозрядних двійкових чисел (768 біт) на основі матриць (рисунок 1) кодового

представлення $P_1 \times P_2$ показують розподіл наскрізних переносів, що, в свою чергу, вказує кількість одиниць або нулів в добутку.

Згідно методу Ферма, для факторизації числа P_0 виконуються наступні операції: обчислюється $\sqrt{P_0}$, яке округлюється до більшого цілого P_c^*. Підноситься P_c^* до квадрату $F_1 = P_c^{*2}$, після чого формується послідовність квадратів згідно співвідношень $F_1 = (P_c^*+1)^2$, $F_2 = (P_c^*+2)^2$,…, $F_k = (P_c^*+k)^2$[4].

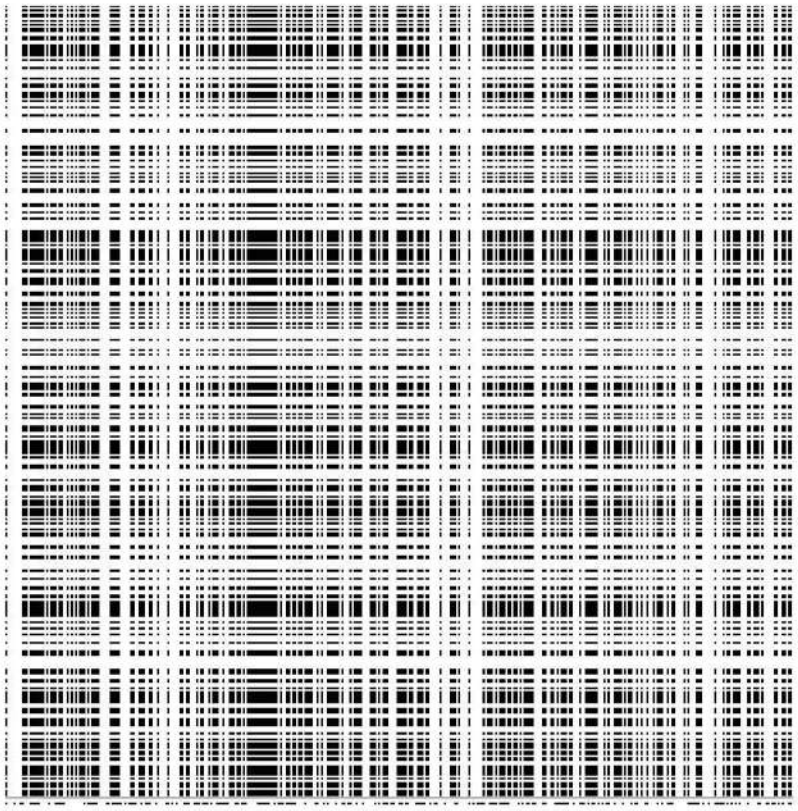


Рисунок 1 – Матриця кодового представлення множення багаторозрядних двійкових чисел (768 біт)

Перевіряється, чи добувається цілочисельний корінь з різниці $\dot{\Delta} = \sqrt{F_k - P_0}$. Якщо добувається, то числа P_1 і P_2 знаходяться згідно виразу:

$$P_1 = \dot{\Delta} - P * c + k + \dot{\Delta} = P_2 \qquad (4)$$

Обчислювальна складність методу Ферма для багаторозрядних чисел експоненційна. Із збільшенням розрядності вона відповідно зростає, оскільки число процесів k може складати 2^{300} - 2^{400} і тільки на єдино правильному кроці можливе однозначне рішення задачі факторизації[5]. Слід зазначити, що при використанні даного методу необхідно підносити до квадрату числа P_c+k з розрядністю 300-500 біт, що приводить до необхідності кожного разу знаходити різницю $F_к$-P_0 та добувати корені

квадратні з цієї різниці. Графічно модель факторизації такого методу представлено на рисунку 2.

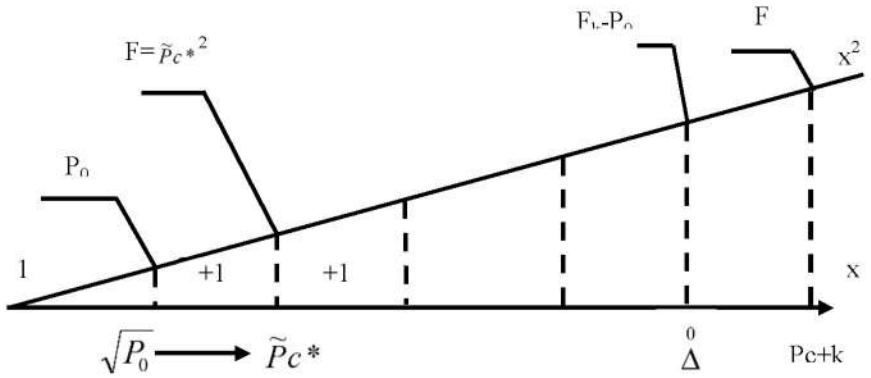


Рисунок 2 - Граф – модель спрощеного алгоритму факторизації на основі теореми Ферма

Отже, з врахуванням недоліків методу Ферма, доцільно розробити алгоритм, в основі якого лежать наступні операції: добувається $\sqrt{P_0}$ і округлюється до більшого цілого $\left|\sqrt{P_0}\right| = \widetilde{P}_c$. Піднімається $\widetilde{P}_c$ один раз до квадрату і обчислюються значення S_k згідно співвідношення:

$$S_k = k(2\widetilde{P}_c + k) + \Delta_0. \qquad (5)$$

Значення $\sqrt{S_k} = \overset{0}{\Delta}$ перевіряється на існування цілого кореня і для єдиного знайденого k з рівняння (5) визначаються шукані P_1 і P_2.

Оскільки k – багаторозрядне число, то метод, в якому відсутні операції піднесення $\widetilde{P}c + k$ до квадрату, буде мати меншу обчислювальну складність. Числа, що використовуються в методі, мають значно меншу розрядність, ніж в алгоритмі Ферма, як зображено на рисунку 3.3 граф–моделі вдосконаленого методу відображення кроків S_k.

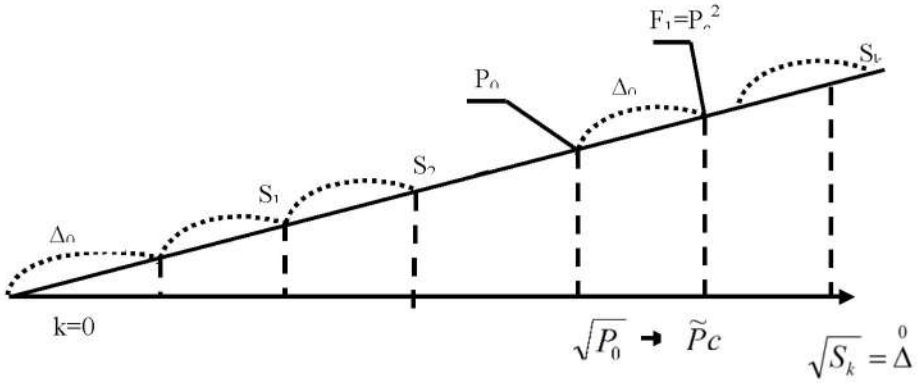


Рисунок 3 – Граф–модель спрощеного алгоритму факторизації на основі теореми Ферма

Таблиця 1 – Приклад факторизації класичним та запропонованим алгоритмом

k	n	$(\Delta_n)^2$, класичний метод	$(\Delta_n)^2$, вдосконалений метод
1	62	62^2-3811=33	62^2-3811=33
2	63	63^2-3811=158	33+125=158
3	64	64^2-3811=285	158+127=285
4	65	65^2-3811=414	285+129=414
5	66	66^2-3811=545	414+131=545
6	67	67^2-3811=678	545+133=678
7	68	68^2-3811=813	678+135=813
8	69	69^2-3811=950	813+137=950
9	70	70^2-3811=1089=33^2	950+139=1089=33^2

Таким чином, отримано розклад числа 3811 на прості множники:

$$811 = 70^2 - 33^2 = (70 + 33)(70 - 33) = 103 \cdot 37.$$

Кількість ітерацій в обох випадках буде однаковою, а найскладнішою залишається операція перевірки квадратичності лишку. Для зменшення її обчислювальної складності можна використати СЗК. Це дозволяє уникнути операцій піднесення до степеня та зменшити розрядність операндів на декілька порядків

Висновки.

В результаті досліджень видно, що у вдосконаленому методі виключається операція піднесення до квадрату. Крім того, арифметичні дії виконуються над числами, розмірність яких на декілька порядків менша, ніж у класичному методі.

Перелік джерел.

1. Buchstab, A.A. Number Theory / A.A. Buhshtab, Education, Moscow, Russia, 1966, 384 p.

2. Zadiraka, V.K. Computer technologies of cryptographic protection of information on the specific digital carriers: Textbook / V.K. Zadiraka, A.M. Kudin, V.O. Lyudvichenko, A.S. Oleksyuk, Textbooks and manuals, Kyiv - Ternopil, Ukraine, 2007, 272 p.

3. Ishmukhametov, Sh.T. Methods for factorization of integers: a tutorial / Sh.T. Ishmuhametov, Kazan University, Kazan, Russia, 2011, 190 p.

4. Zadiraka, V.K. Computer cryptology / V.K. Zadiraka, A.S. Oleksyuk, Tanha, Ternopil, Ukraine, 2002, 504 p.

5. Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko. Theoretical Foundations of the Modified Perfect form of Residue Number SystemCybernetics and Systems Analysis, 52(2), pp.219-223.

УДК 681.32

***Я.М. Николайчук*[1], *О.Б. Посвятовська*[2], *С.В. Івасьєв*[1]**

[1]*Тернопільський національний економічний університет*

[2]*Галицький коледж ім. В. Чорновола*

ПРИСТРІЙ КОМПАКТНОГО КОДУВАННЯ БАГАТОРОЗРЯДНИХ ПРОСТИХ ЧИСЕЛ

Вступ. При реалізації алгоритмів опрацювання багаторозрядних простих чисел в задачах вибору системи взаємно простих модулів для процесорів теоретико числового базису Крестенсона, пошуку найбільшого спільного дільника, виявлення квадратичного лишку, виконання арифметичних операцій модульної арифметики виникає необхідність зберігання та генерування великих масивів багаторозрядних простих чисел[1]. Генерування та зберігання багаторозрядних простих чисел, представлених повнорозрядними двійковими кодами, є неефективним у зв'язку з тим, що потребує великих об'ємів пам'яті.

Метою роботи є дослідження та розробка пристрою компактного кодування багато розрядних простих чисел.

1. Складові пристрою

На основі запропонованого у [2] методу компактного кодування [3] розроблена структурна схема пристрою зберігання та генерування БПЧ, яка показана на рисунку 1.

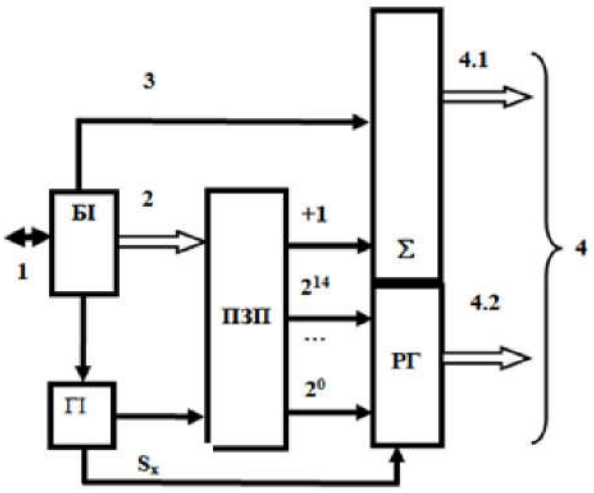


Рисунок 1 – Структурна схема пристрою компактного кодування та генерування багаторозрядного простого числа

Пристрій містить: 1- вхідна інтерфейсна шина; 2 – адресна шина; 3 – шина стартового коду старших розрядів простого числа; 4 – вихідна шина коду БПЧ; +1 – інкрементна одиниця накопичуючого суматора; 2^0-2^{14} – код БПЧ; БІ – блок ініціалізації; ГІ – генератор імпульсів; ПЗП – постійний запам'ятовуючий пристрій; РГ – регістр пам'яті; $\sum$ - багаторозрядний паралельний суматор; 2 – вихідна шина.

В основу пристрою покладено процес зберігання в ПЗП 15 молодших розрядів кодів багаторозрядних простих чисел(БПЧ) та одного розряду – біту синхронізації, на основі якого відбувається інкрементне нарощення старших бітів у суматорі $\sum$, починаючи з 16-го розряду числа у суматорі.

В структурі пристрою функціональні модулі виконують наступні операції: БІ – блок ініціалізації, оснащений інтерфейсною шиною 1, реалізує інформаційний зв'язок з зовнішнім комп'ютерним пристроєм і виконує стартові функції: записує в ПЗП стартовий код 15 біт молодших розрядів БПЧ, а в суматор - багаторозрядний стартовий код старших розрядів БПЧ і запускає генератор імпульсів ГІ.

В процесі генерування імпульсів відбувається інкрементне генерування адресів ПЗП, що забезпечує генерування кодів молодших розрядів БПЧ. У момент появи біта синхронізації на виході ПЗП відбувається інкрементне нарощення кодів суматора.

Перший вихід генератора інкрементує адресацію ПЗП, а другий вихід генератора реалізує запис інформації в регістр та запис стартового коду суматора. На вихідній шині 4 формується послідовність багаторозрядних кодів БПЧ.

В якості ПЗП використовуються кристали флеш-пам'яті з відповідною адресною розрядністю. При цьому, враховуючи, що для запису 15 молодших розрядів БПЧ і біта синхронізації необхідно 2 байти, незалежно від розрядності БПЧ, що забезпечує необхідну компактність зберігання великого об'єму кодів.

Наприклад, при об'ємі флеш-пам'яті 32 ГБ число компактно закодованих та генерованих 32-бітних простих чисел відповідно складатиме $64 \cdot 10^9$ розрядів кодів чисел.

В залежності від розрядності стартового коду розрядність генерованих БПЧ може довільно зростати.

У результаті досягається зменшення об'єму кодів для зберігання БПЧ відповідно в межах 32 розрядів у два рази, для 256 розрядів в 16 разів,

а при 1024 розряди - в 64 рази[3].

У таблиці 1 приведено характеристики та об'єми рекомендованої флеш-пам'яті.

Таблиця 1 – Рекомендовані характеристики флеш-пам'яті, необхідної при реалізації пристрою кодування

Модель пристрою	Характеристики (об'єм / швидкість)
Silicon Power Marvel M01	32 Гб; 5 Гбіт/с.
Transcend JetFlash 350	32 Гб; 5 Гбіт/с.
Kingston DataTraveler SE9 G2	64 Гб; 15 МБ/с.
Kingston DataTraveler 101 G2	128 Гб; 5 МБ/с.

На рисунках 2, 3, показані структури мікроелектронних компонентів пристрою компактного кодування та генерування БПЧ.

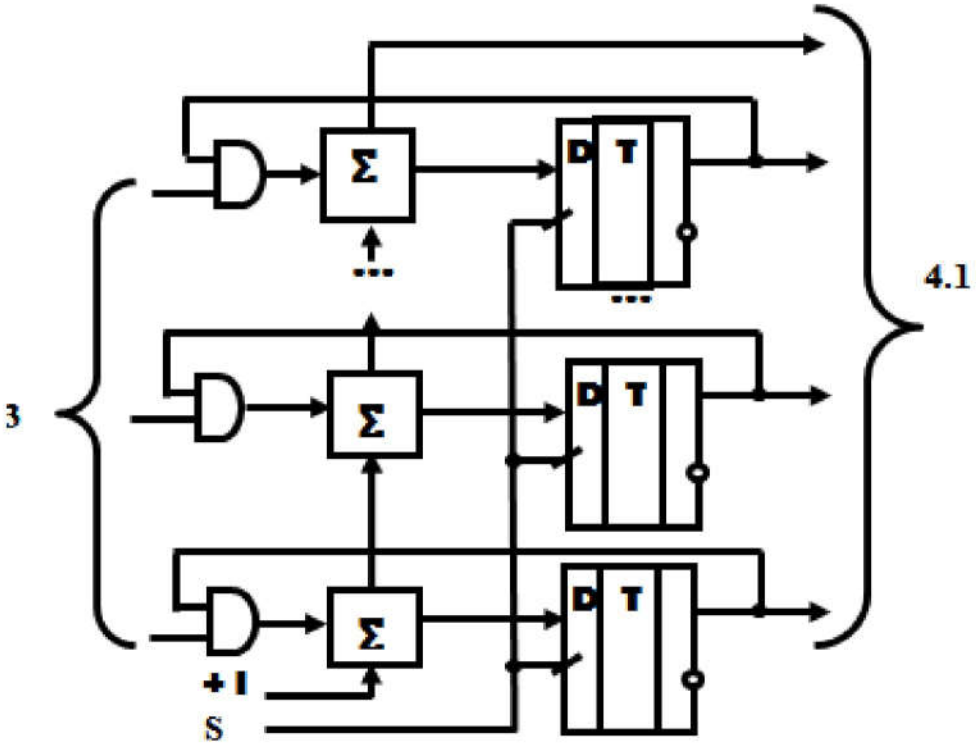


Рисунок 2 - Структурна схема накопичуючого суматора з паралельним 3 та інкрементним +1 входами - формувача старших розрядів БПЧ

Швидкодія структури неповного суматора, представленого на рисунку 4, визначається часом переключення одного логічного елемента, тобто складає 1υ.

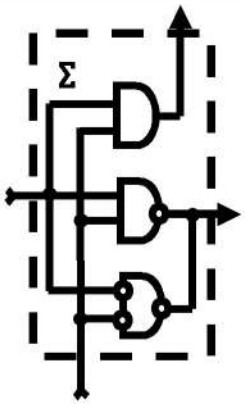


Рисунок 3 - Структура неповного суматора на логічних елементах І, І-НЕ та І-НЕ з інверсними входами

Така реалізація компонента багаторозрядного суматора забезпечує підвищення швидкодії наскрізних переносів у 3 – 5 разів у порівнянні з відомими схемами, які побудовані на логічних елементах І, АБО, НЕ, а також на елементах типу XOR, які в своїй структурі містять п'ять логічних елементів, з яких три з'єднані послідовно.

Розрахунок апаратної складності запропонованих компонентів пристрою компактного кодування та генерування БПЧ у залежності від розрядності розраховується згідно виразу:

$$A = A_{PГ} + A_{\sum}$$

$$A_{PГ} = 15 \cdot A_{\text{DT}} = 15 \cdot 2 = 30\upsilon,$$

де υ - вентилі, які реалізуються на ПЛІС.

$$A_{\sum} = ЛЕ + \text{A}_S + A_{DT},$$

де $\text{A}_S = 3ЛЕ$ - число логічних елементів однорозрядного неповного суматора, звідки

$$A_{\sum} = \text{n}(ЛЕ + 3ЛЕ + 2ЛЕ) = 6\text{n}\upsilon.$$

На рисунку показано характеристики апаратної складності базових компонентів пристрою та зменшення об'єму використовуваної пам'яті при зростанні розрядності БПЧ.

З рисунку видно, що зменшення апаратної складності порівняно з відомими структурами складає півтора-два рази, а об'єм пам'яті при зростанні розрядності БПЧ в межах 32-1024 відповідно зменшується в 2 – 64 рази.

На рисунку 4 показано характеристики часової складності пристрою, які розраховуються на основі параметрів накопичуючого суматора, який

має більше число послідовно з'єднаних елементів $\tau_{PГ} = 2\upsilon$, а $\tau_{\Sigma} = 3n$ нс.

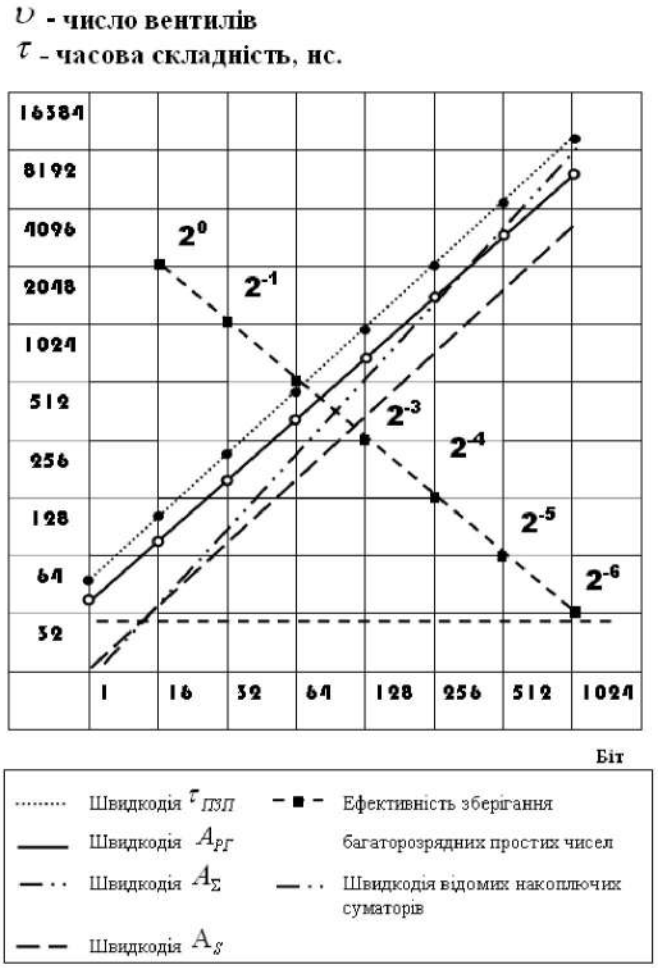


Рисунок 4 - Характеристики часової складності пристрою кодування багаторозрядних чисел та його структурних елементів

Це призводить до зменшення часової складності в більш, ніж два рази в порівнянні з відомими реалізаціями накопичуючих суматорів, часова складність яких складає $\tau_{\Sigma} = 7n$,. Тобто швидкодія розробленого схемотехнічного рішення перевищую аналоги в два рази.

Суттєве підвищення швидкодії пристрою компактного кодування та генерування БПЧ може бути досягнуте застосуванням в якості компонента накопичуючого суматора запропонованого в роботі [3] швидкодіючого багаторозрядного суматора, структура якого показана на рисунку 5.

При цьому часова складність складає $log_2 n$. В той же час, як видно з рисунку 4, його апаратна складність, практично, на порядок вища в порівнянні з розробленим, що може обмежувати доцільність практичного застосування подібного елемента в розробленому пристрої.

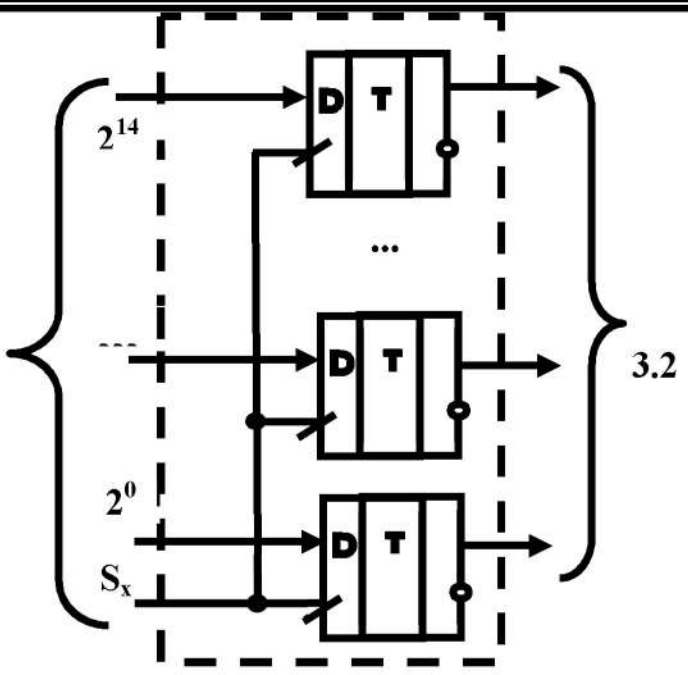


Рисунок 5 – Структура регістра пам'яті молодших розрядів БПЧ на D-тригерах

Висновки.

Обчислимо ефективність пристрою згідно суми ефективності обчислювальних елементів: $\tau = \tau_{ГІ} + \tau_{ПЗП} + \tau_{\sum}$. Кількість логічних елементів генератора імпульсів $\tau_{ГІ} = 2\upsilon$; регістр пам'яті містить $\tau_{РП} < \tau_{\sum}$; постійно запам'ятовуючий пристрій $\tau_{ПЗП} = 10\upsilon$; суматор - $\tau_{\sum} = 4\upsilon$. Таким чином, швидкодія пристрою генерування та кодування БПЧ складає $\tau = 16\upsilon$, що свідчить про високу ефективність розробленого пристрою опрацювання БПЧ.

Перелік джерел.

1. Івасьєв С.В. Метод зберігання простих великорозрядних чисел у базисі Радемахера / С.В. Івасьєв, М.М. Касянчук, І.З. Якименко // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2013. – С. 142-144.

2. Івасьєв С.В. Метод зберігання простих великорозрядних чисел у базисі Радемахера / С.В. Івасьєв, М.М. Касянчук, І.З. Якименко // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2013. – С. 142-144.

3. Івасьєв С.В. Метод організації компактної бібліотеки простих чисел великої розрядності / С.В. Івасьєв //Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління» (ICSM) – Тернопіль, 2014. – С. 86-89.

УДК 681.32

В.В. Власюк, У.Б. Сас, А І. Сегін

Тернопільський національний економічний університет

ВДОСКОНАЛЕННЯСИСТЕМИ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ВИРОБНИЦТВА КАРТОНУ

Вступ. Завдяки багатій сировинній базі та широкому попиту виробництво картону в Україні за останні роки розвивається та вдосконалюється. Використання картону має різноманітне призначення, що накладає певні умови на його структуру та якість. Крім того, існує конкуренція між виробниками, яка вимагає зниження собівартості його виробництва, підвищення продуктивності виготовлення та покращення якості. Для забезпечення конкурентоздатності підприємства картоноробної промисловості впроваджують новітнє обладнання, технології та системи автоматизованого управління, які дозволяють скоротити енергозатрати, зменшити кількість браку, підвищити продуктивність, покращити якість продукції та отримати інші конкурентні переваги.

Одним з основних способів досягнути цього є запровадження автоматизованих систем. Сучасні системи автоматизованого управління в картоноробній галузі повинні забезпечувати жорстке дотримання технологічних параметрів, здійснювати автоматичне регулювання вхідних впливів для досягнення високої якості, запобігати виникненню складних аварійних ситуацій, а в ідеальному випадку, попереджати їх появу взагалі.

Зважаючи на це, в роботі запропоновано вдосконалену систему автоматизованого управління для дотримання технологічних параметрів.

Метою роботи є дослідження та оптимізація системи автоматизованого управління технологічним процесом виробництва картону.

1. Опис технологічного процесу виробництва картону

Сировиною для виготовлення картону служать переважно напівфабрикати з грубішими волокнами, ніж для виробництва паперу: бура деревна маса, напівцелюлоза, цупка сульфатна целюлоза і макулатура. Виготовляють картон [1] із приготованої (розмеленої, інколи проклеєної, наповненої і забарвленої) маси на карторобних машинах (плоскосіткових і циліндрових) у вигляді безперервної висушеної, інколи каландрованої стрічки; на пакових машинах у вигляді окремих вологих листів. Листи пресують в

гідравлічних плиткових пресах, сушать в канальних, стрічкових та ін. сушарках, глазують і ущільнюють на каландрах, сортують і пакують.

В загальному, кортоноробну машину (КРМ) схематично можна представити у вигляді показаному на рисунку 1.

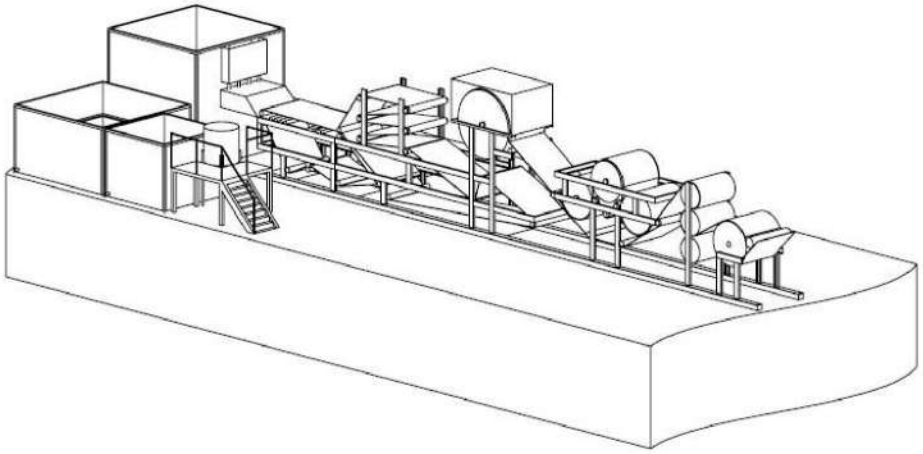


Рисунок 1 – Схематичне представлення загального вигляду картоноробної машини

Технологічний процес виробництва картону покроково представлений у вигляді блок-схеми на рис. 2 і здійснюється наступним чином [1].

Маса високої концентрації (МВК) призначена для формування першого (первинного) шару. Вона подається по трубопроводу до бака постійного напору. Звідси МВК надходить на вхід змішувального насоса. Сюди також подається обігова вода із збирача обігової воді. Розбавлена маса (маса низької концентрації –0.5 %) змішувальним насосом подається до першого напірного ящика з якого вода витікає на сітку, де формується первинний шар двошарового картону.

МВК, яка призначена для формування другого (вторинного) шару двошарового картону, по трубопроводу подається до бака постійного напору, звідки надходить – на вхід змішувального насоса. В насос також подається обігова вода із збирача обігової води. Розбавлена маса (маса низької концентрації) змішувальним насосом подається до другого напірного ящика звідки вона витікає на перший сформований шар.

Утворене таким чином мокре двошарове картонне полотно подається до пресової частини машини. У ній картонне полотно піддається пресуванню з метою видалення води механічним способом. Із пресової частини картонне полотно надходить до сушильної частини машини.

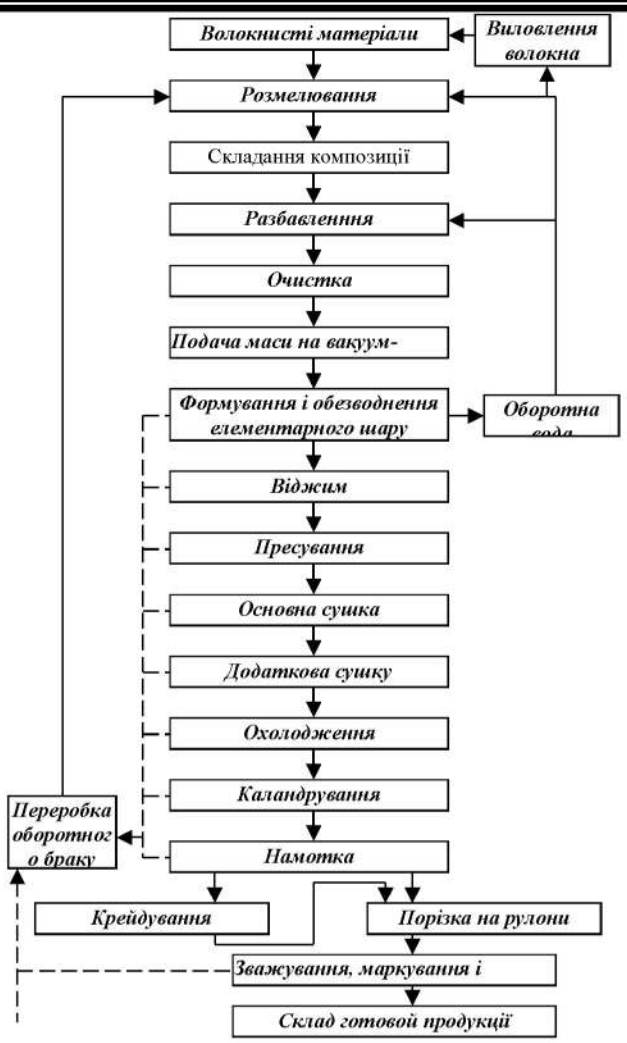


Рисунок 2 – Блок-схема процесу виготовлення картону

Сушильна частина КРМ складається із великої кількості (до 100...120 шт.) сушильних циліндрів, у які подається пара по трубопроводу. Внаслідок сушіння картонного полотна на сушильних циліндрах утворюється конденсат, який відводиться по спеціальному трубопроводу на теплоелектростанцію.

Вироблене таким чином картонне полотноза допомогою накату намотується у рулони.

2. Вимоги до САУ виробництва картону та структура

З розглянутого процесу виробництва картону видно, що ОУ для даного процесу є технологічний ланцюжок послідовних операцій, в якому відсутні зворотні технологічні зв'язки. Кожна ланка такого ланцюга пов'язана з виконанням певної технологічної задачі. Результат оцінюється за показниками, що характеризують або місцеву якісну ознаку сировини, що переробляється, або режим роботи обладнання. Ці показники повинні бути віднесені до вихідних змінних даної ланки. Вони ж є вхідними

змінними для наступної ланки, технологічного ланцюжка. Вхідними змінними такого ланки, в свою чергу, є вихідні змінні попереднього ланки і т.д.

На основі викладеного, розроблена структурна схема моделі автоматизованої системи регулювання з відповідними ланками передавальних функцій.

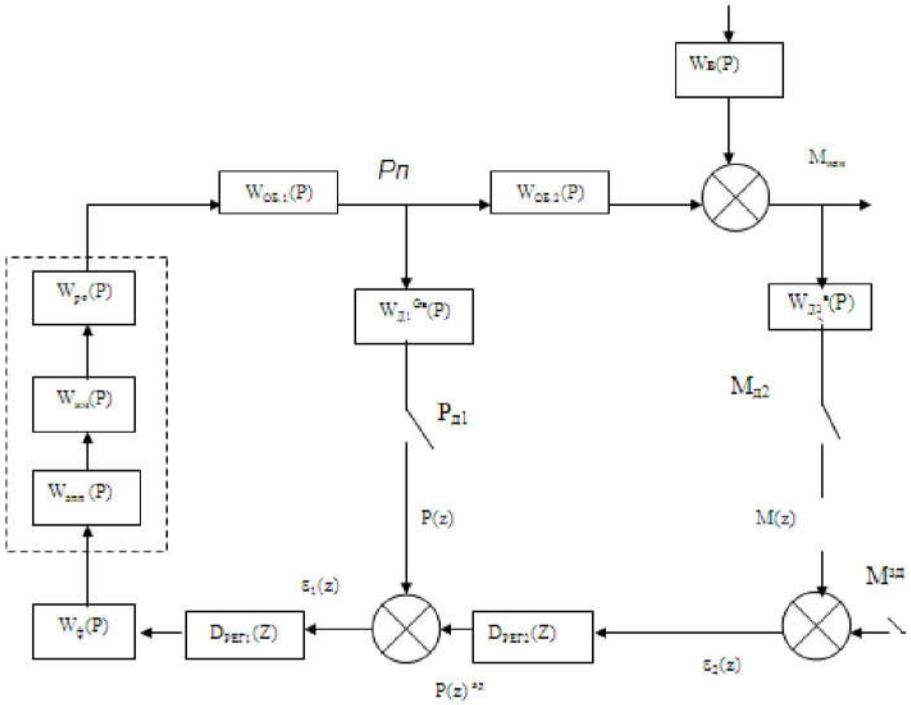


Рисунок 3 – Структурна алгоритмічна схема двохконтурной АСР вологості

На Рисунку 3 використано такі позначення:

$W_{об1}$ (Р) – передавальна функція тиску пара в ведучій сушильній групі (об'єкт регулювання 1);

$W_{об2}$ (Р) – передавальна функція підтримки вологості картонного полотна (об'єкт регулювання 2);

$W_{Д1}$ (Р) – передавальна функція давача 1 – вимірювання тиску пари;

$W_{Д2}$ (Р) – передавальна функція давача 2 – вимір вологості картонного полотна;

$W_{ф}$ (Р) – передавальна функція фіксатора;

$W_{ВМ}$ (Р) – передавальна функція виконавчого механізму;

$W_{РО}$ (Р) – передавальна функція регулюючого органу (кульового клапана) на лінії подачі пари в провідну сушильну групу;

$W_{ЕПП}$ (Р) – передавальна функція електропневматичного перетворювача

$D_{РЕГ1}$ (Z) – передавальна функція регулятора 1;

$D_{РЕГ2}$ (Z) – передавальна функція регулятора 2;

До даної САУ ставляться такі вимоги:

1. Система повинна володіти заданим запасом стійкості.

2. Динамічна помилка, величина перерегулювання і статична помилка не повинні бути більше заданих.

3. Час регулювання має бути мінімальний.

Для регулювання САУ вибираємо ПІ-закон регулювання. Це дозволить збільшити точність регулювання, звести статичну помилку до нуля.

Існуючий спосіб управління (рис. 4.) являє собою двоконтурну систему регулювання вологістю. Перший, внутрішній контур, утворений ділянкою підведення пари до провідної сушильної групі від місця установки регулюючого клапана до місця установки датчика тиску для вимірювання тиску пари. Регульованим параметром цього контуру є тиск пара.

Об'єкт регулювання цього контуру характеризується властивістю самовирівнювання і не має запізнювання. Контур виконує завдання стабілізації тиску пара і є стежить. Він має астатизм по каналу зовнішнього завдання, які не коливальний і володіє максимальною швидкодією.

Другий, зовнішній контур складається з провідної сушильної групи, паропроводу, датчика вологості і накату. Вхідним параметром контуру є тиск пара, вихідним - вологість картонного полотна. Перший з цих параметрів є регулюючим впливом, другий - регульованим параметром.

Зовнішній контур – інерційний, характеризується великою тривалістю перехідних процесів і має велике запізнювання і постійну часу .. Як обурення в АСР вологості використовується сигнал зі зміни маси 1 $м^2$ картонного полотна.

Структурна схема такої системи управління представлена на рисунку 4. Система знаходиться під дією випадкових збурень $W_{зовн}$, що впливають на кінцеву вологість $M_{кін}$.

Система підтримує задане значення вологості $M_{ЗД}$ шляхом зміни задання регулятору тиску, на компараторі якого формується сигнал неузгодженості, що відпрацьовується регулятором тиску.

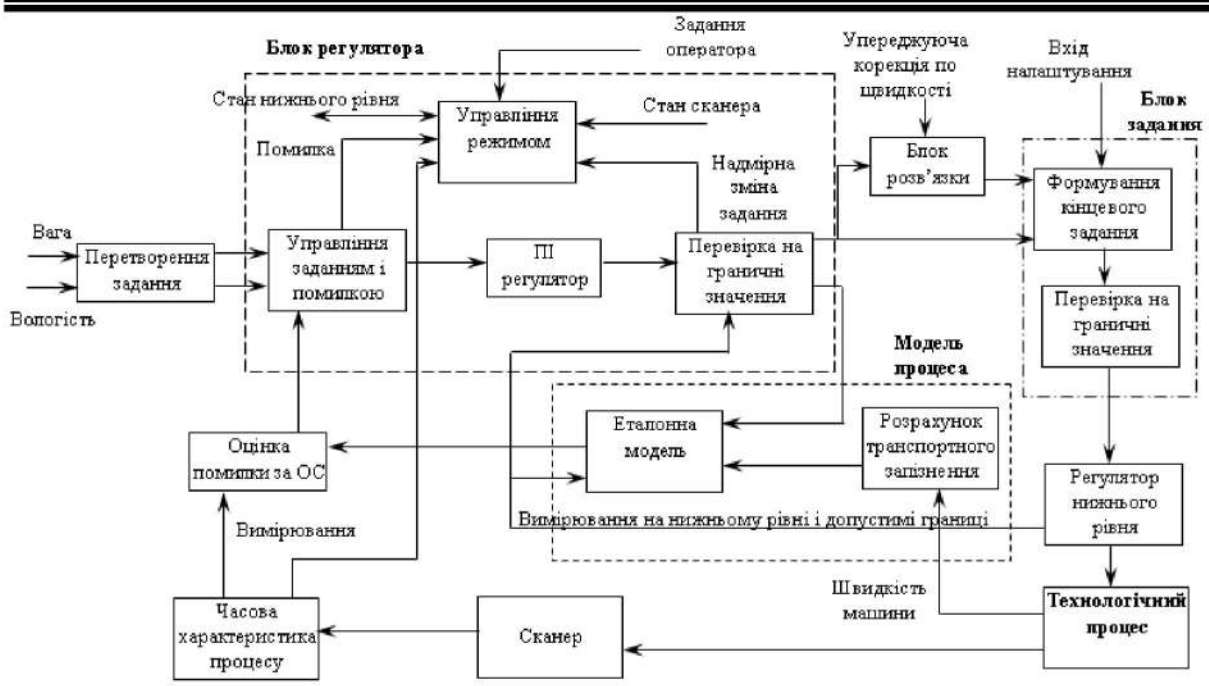


Рисунок 4 – Структурна схема системи управління виробництва картону

Для ефективного управління пропонується ввести дворівневу систему, в якій на нижньому рівні для управлінням рівнем вологості використано контролера фірми "SIEMENS" [2] SIMATIC S7-300 , а на верхньому рівні управління використовується контролер ABB [3] ACURAY 1190.

Висновки.

На основі проведеного аналізу технологічного процесу було встановлено, що вологість практично є визначальним параметром при виробництві картону. Також було розроблено структурну модель дворівневої системи управління, на основі якої розраховано та проаналізовано основні параметри налаштування автоматизованої системи регулюванням вологості картонного полотна. На основі цього розроблено структурну схему САУ виробництва картону на базі мікроконтроллерів фірм Siemens та ABB.

Перелік джерел.

1. Производство бумаги и картона / Б. В. Акулов, С. Г. Ермаков. — Пермь, Издательство Пермского государственного технического университета, 2010. — 432 с.

2. SIMATIC S7-300 - Proven multiple times! Режим доступу: https://new.siemens.com/us/en/products/automation/systems/industrial/plc/simatic-s7-300.html

3. Detailed information for: C170. Режим доступу: https://new.abb.com/products/C170/accuray-1190-system-funct

УДК 681.32

П.В. Гуменний, І.І. Вайда, І.В. Щур

Тернопільський національний економічний університет

ІНФОРМАЦІЙНА КОМП'ЮТЕРНО-ІНТЕГРОВАНА СИСТЕМА КЕРУВАННЯ ВИГОТОВЛЕННЯМ ХЛІБОБУЛОЧНИХ ВИРОБІВ

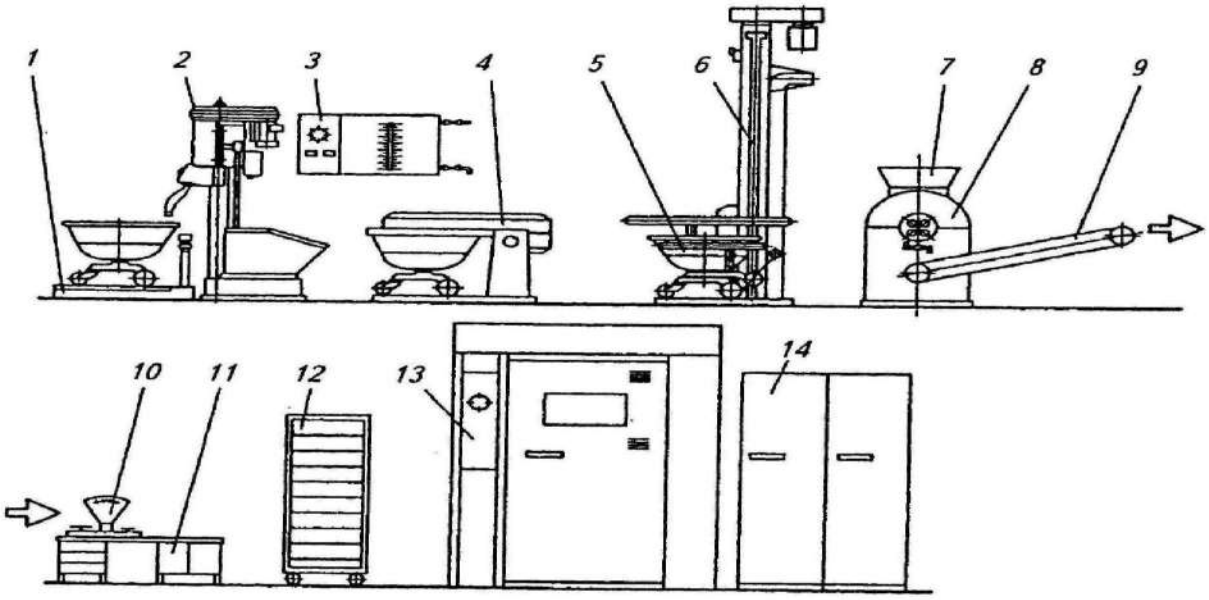
Вступ. Автоматизація технологічних процесів є одним з вирішальних факторів підвищення продуктивності і покращення умов праці, якості і розширення асортименту продукції на хлібобулочному виробництві. Виробництво кондитерських хлібобулочних виробів на сучасному хлібопекарському підприємстві здійснюється в основному на потоково-механізованих лінях, що складаються з комплексу машин і апаратів, у органічні технологічні процеси. Технологічний процес хлібопекарного виробництва є сукупністю операцій і перетворень, призначених для переробки сировини у готові вироби. Він характеризується великою кількістю потоків продуктів, що розгалужуються і з'єднуються, по структурі, володіє багатовимірністю, деякою невизначеністю та випадковим характером зміни параметрів [1]. Технологічний процес намагаються здійснювати по найкращому варіанту з безлічі можливих, базуючись в основному логікою, досвідом і інтуїцією проектувальників і експлуатаційників. Тому на даному етапі розвитку, кондитерська хлібопекарна промисловість потребує розробки комплексної автоматизації технологічних процесів шляхом використання інноваційних комп'ютеризованих технічних засобів.

Метою роботи є розробка автоматизованої системи керування для виготовлення кондитерських хлібобулочних виробів.

1. Дослідження вимог до систем автоматизації хлібобулочних виробництв

Технологічна схема виробництва хліба і хлібобулочних виробів включає в себе наступні етапи: зберігання і підготовка сировини до виробництва, приготування та оброблення тіста, випічка та зберігання хліба. Технологічний процес хлібопекарного виробництва як система-це сукупність послідовних фізичних, колоїдних, біохімічних, мікробіологічних і інших операцій і перетворень, що протікають при переробці сировини у готові хлібні і мучні кондитерські вироби.

Хлібопекарське виробництво оснащене сучасним устаткуванням, новітніми технологіями, що має в своєму розпорядженні могутню виробничу базу [2]. На рисунку 1. представлена схема, що реалізує технологічні процеси виробництва кондитерських хлібобулочних виробів на сучасному хлібзаводі.



1 – платформні ваги; 2 – просіювач; 3 – дозатор води; 4 – тістомісильна машина; 5 – підкатна діжа; 6 – діжоперекидач; 7 – завантажувальна воронка; 8 – тістоподільник; 9 – конвеєр; 10 – контрольні ваги; 11 – виробничий стіл; 12 – стелажний візок; 13 – хлібопекарська піч; 14 – розстоювальна шафа

Рисунок 1 – Машинно-апаратурна схема комплексу лінії з виготовлення хлібобулочних виробів

Для ефективної роботи устаткування хлібобулочного виробництва необхідно використовувати сучасні системи керування, що використовують програмовані логічні контролери. MicroPC 6040 є ідеальним засобом для побудови високоефективних систем автоматичного управління хлібопекарського виробництва малої потужності при мінімальних витратах на придбання обладнання і розробку системи. Контролери здатні працювати в реальному масштабі часу і можуть бути використані як для побудови вузлів локальної автоматики, так і систем розподіленого вводу-виводу з організацією обміну даними по PPI або MPI інтерфейсу, мережі PROFD3US-DP або AS-інтерфейсу[3].

Конструктивно контролер виконаний у вигляді двох щитів: власне щита контролера і з'єднувального щита з габаритними розмірами кожного 800-800-200 мм. З'єднання між ними здійснюються кабелями з роз'ємними з'єднаннями. Таке технічне рішення дозволяє легко демонтувати контролер і забезпечити його збереження при модернізації обладнання. Контролер зібраний на базі мікроконтролера MicroPC 6040 в монтажному каркасі 5206 RM з використанням виробів фірм Octagon Systems, Advantech, Grayhill і Fastwel. (рисунок 2).

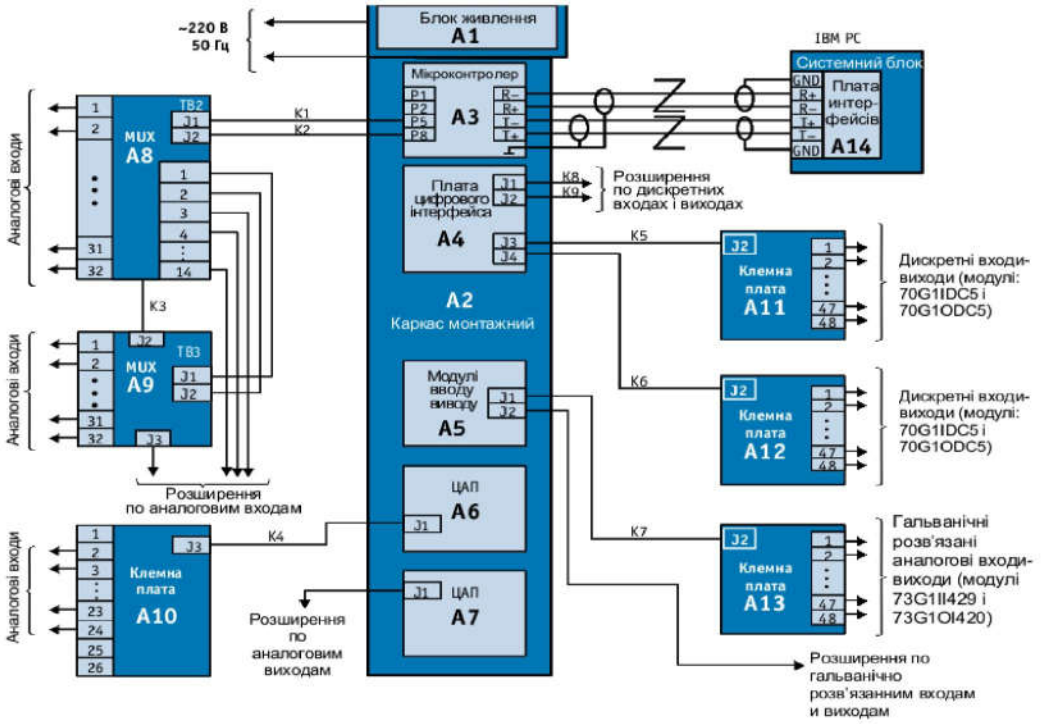


Рисунок 2 – Структурная схема контролера MicroPC 6040

Контролер MicroPC 6040 є повністю модульним. Він складається з шасі, модулів джерела живлення, процесора, дискретних і аналогових входів-виходів і інших модулів [4]. Використання контролера MicroPC 6040 дозволить автоматизувати роботу хлібопекарської печі та скоротити витрати використання природного газу.

2. Розробка структури автоматизованої системи керування хлібопекарською піччю

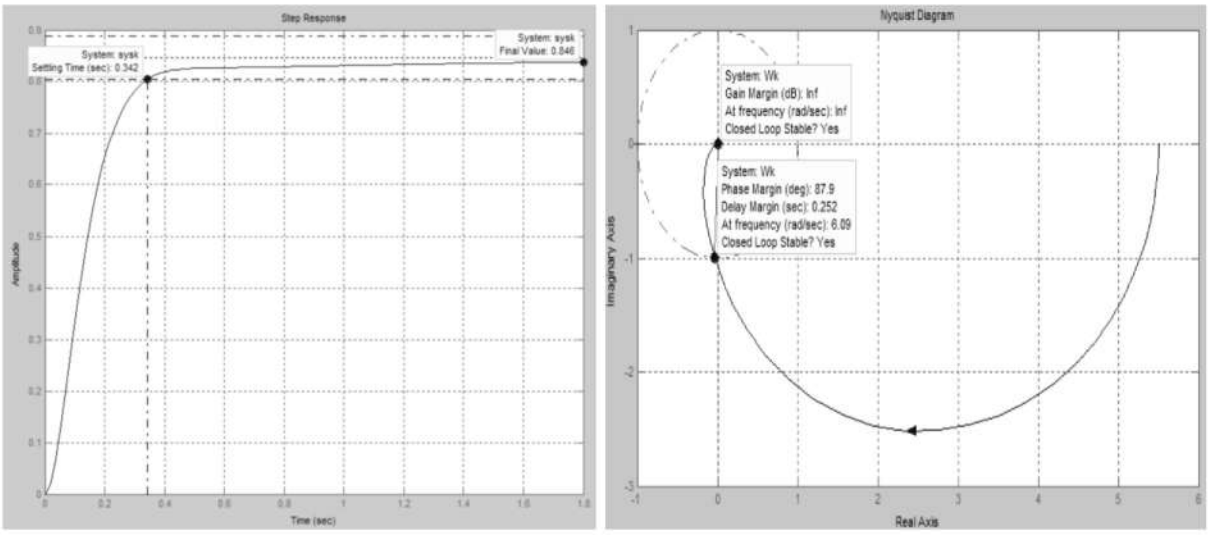
Розробка структури системи автоматизованого управління хлібопекарської печі полягає у виборі серед типових алгоритмів управління, що забезпечить потрібну якість процесу регулювання відносно

обраного критерію управління. В якості закону регулювання використаємо ПІ – закон. В ідеальному випадку даний закон забезпечує достатню якість і час регулювання та відсутність статичної похибки, але в реальних системах в яких присутня зона нечутливості, присутня також і статична похибка.

Передаточна функція замкнутої системи із послідовною коректуючою ланкою матиме вигляд:

$$W_з = \frac{W_к}{1+W_к} = \frac{7{,}042p + 5.504}{0.0486p^3 + 1.188p^2 + 9.487p + 6.504}.$$

Перехідна характеристика замкнутої системи зображена на рисунку 3(а) годограф АФЧХ розімкнутої системи - на рисунку 3 (б).



а, б)

Рисунок 3–Перехідна характеристика замкненої системи (а), годограф АФЧХ розімкнутої системи (б) з послідовною коректуючою ланкою за каналом завдання

Отже, введення послідовної коректуючої ланки дозволило зменшити час регулювання з 3,2 с до 0,342 с, усунути перерегулювання, збільшити запас стійкості системи по фазі з 52,20 до $87{,}9^0$, проте усталена помилка залишилась на рівні $\delta_{уст}= 0{,}15$.

Щоб усунути усталену помилку, ввдемо неодиничний зворотній зв'язок із коефіцієнтом передачі $k_{зз}=1\text{-}1/k_р$ де $k_р$ - коефіцієнт передачі розімкнутої системи:

$$k_{зз} = 1 - \frac{1}{k_p} = 1 - \frac{1}{5.504} = 0.8183.$$

Тоді структурна схема системи автоматичного регулювання температури (рисунку 4) в печі матиме вигляд:

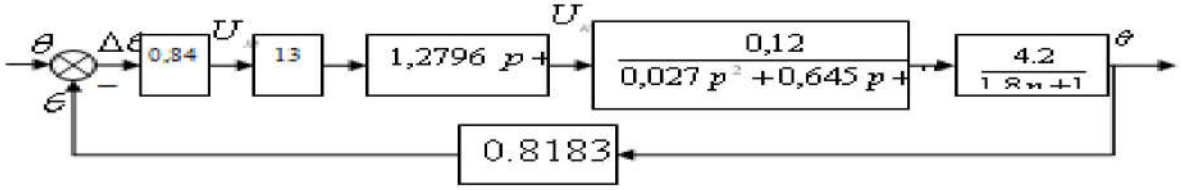


Рисунок 4 – Структурна схема системи автоматичного регулювання температури в печі після проведення коригування

Тоді передаточна функція замкнутої системи за каналом завдання матиме вигляд:

$$W_з = \frac{7{,}042p + 5.504}{0.0486p^3 + 1.188p^2 + 8.208p + 5.504} \quad (1)$$

Перехідна характеристика скоректованої системи автоматичного регулювання температури в печі має вигляд, зображений на рисунку 5.

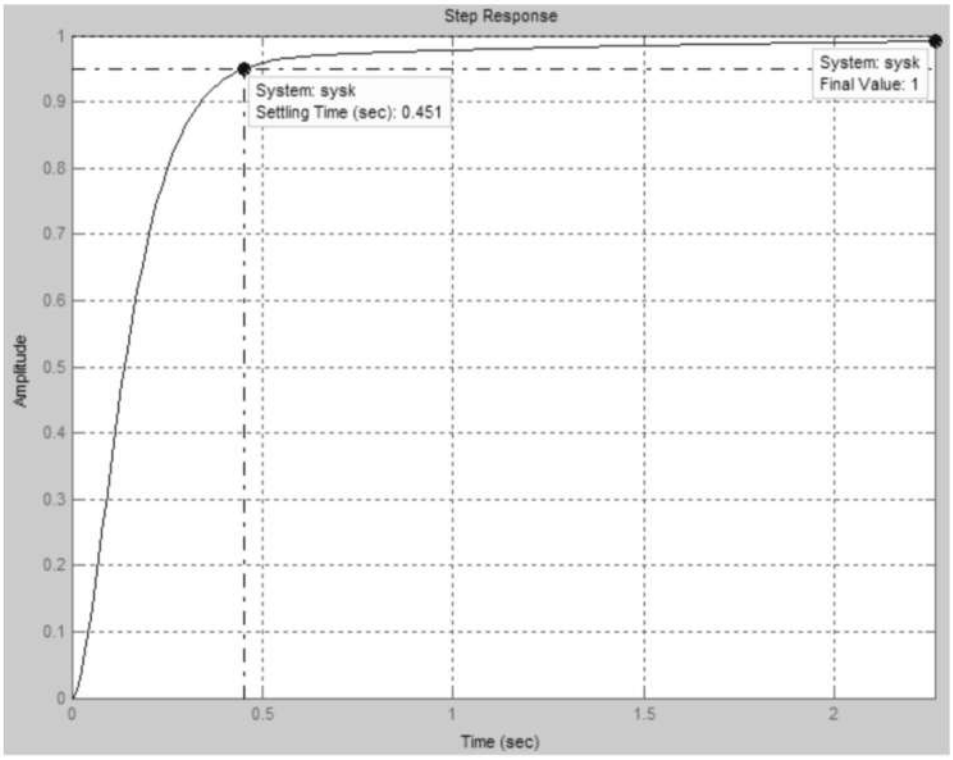


Рисунок 5 – Перехідна характеристика скоректованої системи за каналом задання

Покращення динамічних показників якості системи, показано в таблиці 1.

Таблиця 1 - Статичні та динамічні показники якості системи

Властивості системи автоматичного регулювання температури в печі		
Параметр	Система	
	до коригування	скорегована
Статичні властивості системи		
Усталена помилка	0,15	0
Динамічні властивості системи		
Час регулювання	3,2 с	0,451 с
Перерегулювання	24.57%	0
Кількість коливань на протязі часу регулювання	N=1	0
Коливальність	$\zeta = 0{,}0625$	-
Запас стійкості за фазою	52, 20	$87{,}9^0$

Отже, в результаті коригування автоматизованої системи управління для печі досягли покращення статичних та динамічних показників якості системи.

Висновки.

У роботі досліджено автоматизовану систем з виготовлення кондитерських хлібобулочних виробів встановлено, що на сучасному етапі розвитку даної промисловості передові позиції займають компактні лінії, з завершеним виробництвом. Досліджено принцип роботи контролера управління хлібопекарською лінією, а також досліджені принципи роботи температурних датчиків та витратомірів різних речовин. Проведено дослідження загальної структури системи автоматичного регулювання температури пекарної камери і вибір типу регулювання. Встановлено переваги двопозиційних регуляторів для систем керування хлібобулочним виробництвом, вони забезпечують хорошу якість регулювання для інерційних об'єктів з малим запізненням та не вимагають налаштування.

Перелік джерел.

1. Автоматика и автоматизация производственных процессов. Под ред. Г.К. Нечаева. – К.: Вища школа, 1985. – 274 с.

2. Емельянов А.И., Копник О.В. Проектирование систем автоматизации технологических процессов: Справочное пособие. – М.: Энергоатомиздат, 1983. – 400 с.

3. Зайцев Г.Ф., Костюк В.И. Основы автоматического управления и регулирования. – К.: Техника, 1977. – 472 с.

4. Береза А. М. Основи створення інформаційних систем: навч. посіб. / А. М. Береза. – 2 вид., перероб. і доп. – К.: КНЕУ, 2001. – 214 с.

УДК 681.32

Г.В.Войцешко

Тернопільський національний економічний університет

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ МОНІТОРИНГУ СТАНІВ ЕЛЕКТРИЧНОЇ ПІДСТАНЦІЇ

Вступ. Сьогодні важливим у електроенергетиці є виявлення перехідних процесів у високовольтних лініях електропередач. Висока швидкість перехідних режимів у ЛЕП потребує відповідної реакції контрольно-вимірювальних пристроїв, перетворювачів, пристроїв релейного захисту та контролерів, які повинні опрацьовувати результати перехідних процесів у реальному часі.

У процесі експлуатації високовольтних ЛЕП можуть виникати особливі перехідні режими та можливість виникнення пошкоджень обладнання електричних підстанцій. Такі пошкодження приводять до виходу з ладу технологічного обладнання. Також, небезпечним є пониження напруги у вузлових точках електроенергетичної системи внаслідок коротких замикань, що впливає на порушення технологічних процесів споживачів електроенергії та стійкості генераторів енергосистеми.

Метою роботи є розробка системи моніторингу станів електричних підстанцій високовольтних ЛЕП, яка включає розробку теоретичних основ та алгоритмів побудови комплексу моделей квазістаціонарних станів, аналіз структури та характеристик інформаційних потоків, які формуються на електричній підстанції для моніторингу їх станів.

1. Організація моніторингу систем контролю та управління технологічними процесами

Розробка та впровадження комп'ютеризованих систем моніторингу широкого класу технологічних об'єктів різних галузей промисловості, а також технічної та екологічної безпеки їх експлуатації є актуальною задачею.

Підприємства з розробки, виробництва та впровадження автоматизованих систем управління, релейного захисту, автоматики є гостро необхідними для об'єктів енергетики [1]. Сучасні технології дозволяють промисловим підприємствам та енергетичним компаніям підвищувати рівень свого виробництва, знижуючи при цьому негативний

вплив на зовнішнє середовище.

Від АСУ вимагається виконання таких функцій: збір даних від програмованих логічних контролерів (ПЛК); первинна обробка даних про технологічні процеси; архівація даних; уявлення мнемосхем енергетичного об'єкта в статиці і динаміці; уявлення графіків (трендів) вимірюваних величин параметрів режимів; повідомлення про несправності і аваріях; друк протоколів і звітів; введення в систему управління команд операторів; зв'язок з іншими автоматизованими робочими місцями (АРМ) операторів; рішення прикладних задач на основі поточних вимірювальних даних. До таких систем пред'являються вимоги щодо надійності системи (технологічна і функціональна); безпеки управління; точності обробки і представлення даних.

У структурі комп'ютеризованих систем контролю та управління промислових об'єктів моніторинг за їх станом та технологічними режимами роботи виконують оператори абонентських станцій. При цьому методи представлення, структуризація даних та технологія інтерактивної взаємодії "оператор – моніторингова система" (ОМС), надійність та результативність функціонування ОМС в реальному часі суттєво впливає на ефективність роботи об'єктів та інформаційної системи діагностування в цілому.

На сьогоднішній день передбачаються наступні способи подання інформації: мнемосхеми, графіки, звітні форми, АРМ "Диспетчерські графіки" станції.

Важливим елементом вказаної інформаційної взаємодії є інтерактивний режим реалізації моніторингу, а також надійне розпізнавання нештатних передаварійних та екологічно-небезпечних ситуацій на об'єктах. Особливе значення при цьому надається забезпеченню низької складності та високої швидкодії реакції оператора на зміни станів об'єктів.

2. Проектування структурної схеми системи моніторингу станів електричної підстанції

Створювана система повинна виконувати функції автоматизованого керування технологічними процесами об'єкта (підстанції) у нормальних, аварійних та післяаварійних режимах. Ключовим завданням створення системи моніторингу станів електричної підстанції є:

- підвищення надійності електропостачання;

- підвищення безвідмовності роботи системи;
- збереження навколишнього середовища.

Структурна схема системи моніторингу станів електричної підстанції приведена на рисунку 1, де використані наступні скорочення: РЗА – релейний захист та автоматика, БРП – блокова розподільна підстанція, ЗПК – загальний пункт керування, РП – розподільний пристрій.

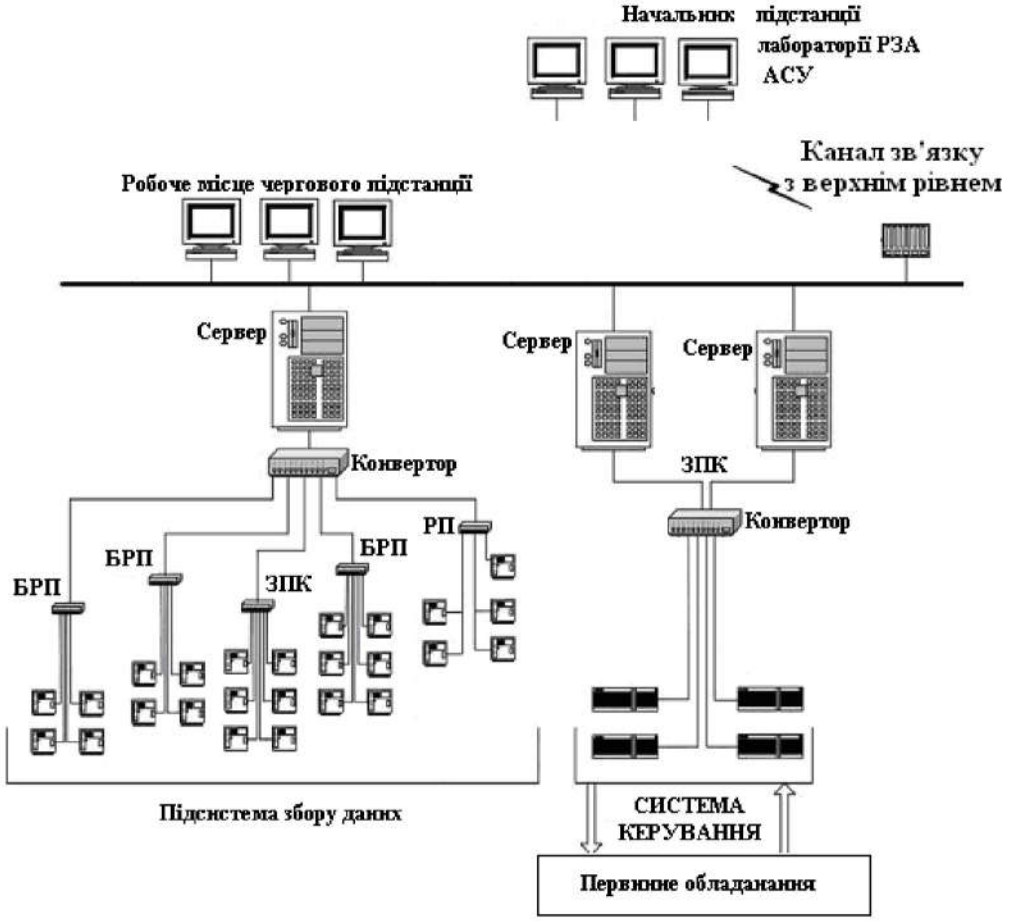


Рисунок 1 - Структурна схема системи моніторингу та керування станами електричної підстанції

Побудова системи автоматизованого моніторингу станів електричної підстанції у вигляді моделі відображення станів (МВС) полягає у тому, що існуючі методи характеризуються обмеженими функціональними можливостями, оскільки демонструють оператору тільки факт передаварійних чи аварійних станів об'єкта. Виявлення нештатного стану об'єкта потребує від оператора додаткових дій для ідентифікування конкретного параметру відхилення від норми. Таким чином відомі методи моніторингу об'єктів не забезпечують необхідну швидкодію реакції

оператора та правильність прийняття рішень по відновленню норми стану об'єкта.

Технологія побудови МВС, на відміну від відомих, шляхом інтегрованого представлення стану об'єкта, забезпечує покращені умови моніторингу та підвищення швидкодії реакції оператора на відхилення станів об'єкта від норми. При цьому забезпечується необхідний рівень вибухо- та екологічної безпеки енергетичних об'єктів [2, 3].

Таким чином, контроль параметрів технологічного процесу з можливістю передбачення розвитку передаварійних та аварійних станів технологічного процесу, здійснюється згідно послідовності операцій:

$X_{\hat{I}\acute{O}} = F(\{x_i\},\{x_j\},S_{\hat{i}\acute{o}}, M_x, M_j, M_v, D_x, \delta_x, R_{xx}, R_{xy}, S_w, L_i, \rho_{ij}, S_{ij}, P_{ij}, I_x)$,

де: $\{x_i\},\{x_j\}$ - масиви оцифрованих моніторингових даних параметрів ОУ; $S_{\hat{i}\acute{o}}$ - стани ОУ; M_x, M_j, M_v - відповідно вибіркове, ковзне та вагове математичні сподівання; D_x, δ_x - відповідно дисперсія та середньоквадратичне відхилення; R_{xx}, R_{xy} - автокореляційна та взаємокереляцйні функції; S_w - спектри параметрів ОУ; L_i – логіко-статистичні інформаційні моделі (ЛСІМ), $i \in \overline{1,5}$; $\rho_{ij}, S_{ij}, P_{ij}$ - відповідно матриці коефіцієнтів взаємокореляції, кластерної моделі ймовірнісних переходів та ентропійних станів; I_x - кореляційна міра ентропії стану ОУ.

У результаті виконання даних операцій досягається розширення функціональних можливостей контролю параметрів технологічного процесу; формування еталонного зображення МВС стану технологічного процесу "норма", порівняння параметрів еталонного стану з виміряними, спостережуваними та розрахованими параметрами технологічного процесу "норма", "прогноз аварії" та "аварія" та ідентифікацію стану технологічного процесу відображенням на моніторі оператора відповідної моделі.

Реалізація моделі відображення станів для різних станів ПС у порівнянні з еталонним, показано в таблиці 1. В таблиці 1 наведені інформаційні дані для побудови МВС, які включають наступні масиви: Сі – стани силових вимикачів, $i \in 1,k$; $V_i = (U_i, I_i, P_i, F_i, S_i)$ - вимірювальні параметри напруги, струму, потужності у вузлових точках ПС, промислової частоти та спектру гармонік, $i \in 1,n$; RZi – інформаційні дані

про стани засобів релейного захисту, $i \in 1,m$; $TR_i = (t,h,...)$ – інформаційні параметри силових трансформаторів, $i \in 1,r$; $PR_i = (N,C,Z)$ - ідентифікаційні параметри збурень.

Таблиця 1 - Стани технологічного процесу ПС у порівнянні з еталонним

Стан технологічного процесу	Параметри технологічного процесу												
	$\{C_i\}$	$\{V_i\}$	U_i	I_i	P_i	F_i	S_i	M_x	PR_i	RZ_i	TR_i	C	Z
Еталон	•	•	•	•	•	•	•		•			•	•
Норма	+	+	+	+	+	+	+		+			+	+
Прогноз аварії	+	-	+	+	-	-	+		+			+	+
Аварія	+	-	+	-	-	-	-		-			-	-

Таке відображення моделі дозволяє передбачати та прогнозувати розвиток передаварійних станів та підвищити інформативність контролю параметрів технологічного процесу.

Висновки.

В результаті розроблення системи автоматизованого моніторингу станів електричної підстанції проведено аналіз систем моніторингу технологічних об'єктів енергозабезпечення, визначено інтерфейсні та управлінські функції операторів названих систем. Сформульовано основні функціональні обмеження існуючих моніторингових систем, які не забезпечують оперативне виявлення та реагування операторів на складні передаварійні та аварійні ситуації на ПС. Технологія побудови системи моніторингу технологічного обладнання електричних підстанцій високовольтних ЛЕП дозволяють розширити функціональні можливості та швидкодію реакції операторів диспетчерських служб при виникненні передаварійних та аварійних ситуацій.

Перелік джерел.

1. Заміховський Л.М. Основи теорії надійності і діагностики технічних систем: Навч. посібн. / Л.М.Заміховський, В.П.Калявін / Івано-Франківськ: Полум'я, 2004. – 360с.

2. Структуризація, методи та моделі інтерактивної взаємодії оператор – інформаційна система моніторингу об'єктів нафтогазової галузі / Н.Я. Возна, Г.Я. Процюк, І.Р. Пітух, Я.М. Николайчук // Розвідка та розробка нафтових і газових родовищ. - Івано-Франківськ, 2015. - №2(55). – С.111-118.

3. Возна Н.Я. Образно-кластерна модель ідентифікації технологічних станів промислових об'єктів управління / Н.Я. Возна, Г.Я. Процюк // Збірник матеріалів проблемно-наукової міжгалузевої конференції "Юриспруденція та проблеми інформаційного суспільства" – Івано-Франківськ, 2016. – С.77-82.

УДК 681.32

В.І. Воробець, А.Я. Давлетова

Тернопільський національний економічний університет

АВТОМАТИЗОВАНА СИСТЕМА ЗБОРУ І ПЕРЕТВОРЕННЯ БІОЛОГІЧНИХ СИГНАЛІВ

Вступ. На сучасному етапі науково-технічного розвитку вітчизняною приладобудівною промисловістю серійно не випускається пристрої для проведення імпедансної томографії (ІТ). Такі прилади розроблені лише в одиничних примірниках в дослідних лабораторіях деяких експериментальних центрів.

Даний метод діагностики стану пацієнтів набуває на сучасному етапі розвитку медицини великого значення, тому дослідження структури та принципу роботи ІТ, схемних рішень та параметрів окремих вузлів, алгоритмів обробки та візуалізації зображень розподілу опору в середині організму пацієнта є актуальною задачею.

Впровадження комп'ютерних засобів у медико - біологічні технології дозволяє отримати швидко і достовірно необхідні результати.

Метою роботи є дослідження та проеткування автоматизованої системи збору та перетворення інформаці дослідження організму людини методом електроімпедансної томографії.

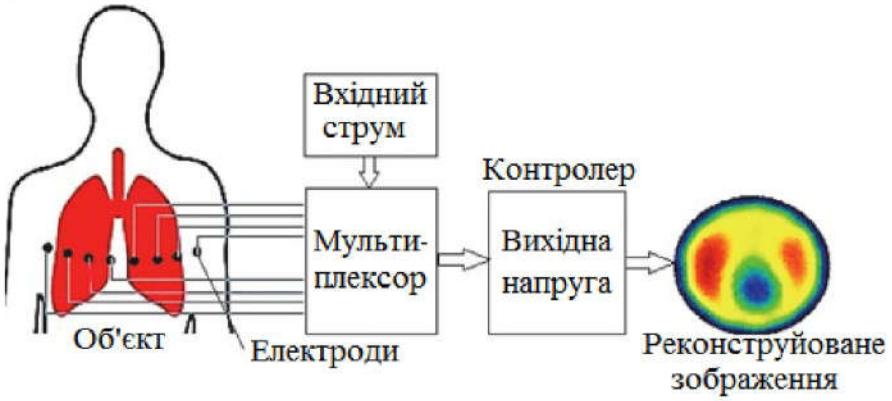
1. Досідження електричної імпедансної томографії

Електрична імпедансна томографія (EIT) - це техніка одержання зображення в зрізах об'єму тіла або на його поверхні за допомогою неінвазивного (не руйнуючого) електричного зондування, розрахунків і алгоритму реконструкції розподілу імпедансу [1].

Тому що різні тканини мають різний імпеданс, ми можемо диференціювати їхнє зображення, і існує можливість виявляти фізіологічні зрушення.

Перше імпедансне зображення вдалося одержати в 1978 році R.P. Henderson and J.G. Webster, а перше електричне імпедансне томографічне зображення було отримано Brian H. Brown and D.C. Barber в 1982 році [2].

Загальна структура системи EIT показана на рисунку1.



Риунок 1 – Загальна структура системи EIT

Для одержання зображення змінний струм інжектується в тіло через електроди, розташовані довкола нього й розраховуються синхронно прикордонні потенціали. Все це уможливлює одержання сукупності даних розподілу імпедансу, які через процесор за допомогою відновлювального алгоритму забезпечують імпедансну комп'ютерну томографічну картинку. Принцип EIT представлений на схемі рисунок 2 [2].

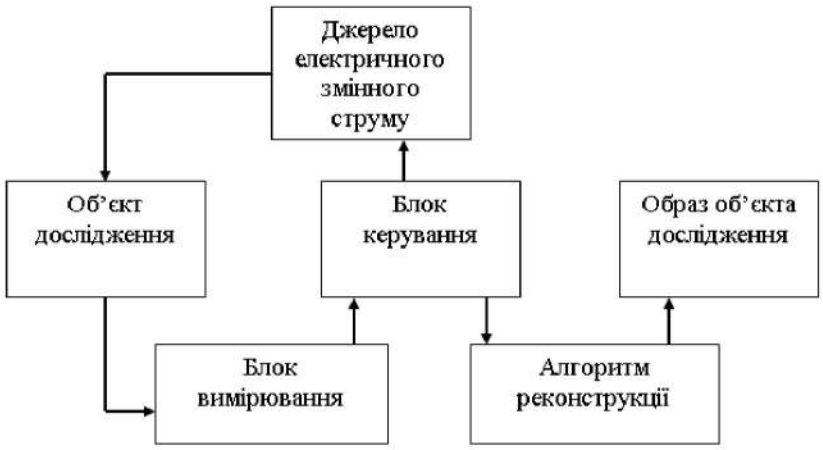


Рисунок 2 – Принцип EIT

Струм, протікаючи через середовище, створює об'ємний розподіл електричного потенціалу (напруг). Потенціал зменшується уздовж лінії струму в міру видалення від активного (інжектуючого струм) електрода. Спадання напруги на одиницю довжини (напруженість електричного поля) пропорційно величині струму й опору середовища відповідно до закону Ома. Вимірюючи спадання напруги й знаючи величину струму, можна обчислити величину опору. Томографічний алгоритм реконструкції дозволяє використати напруги, обмірювані тільки на поверхні тіла, для обчислення просторового розподілу питомого опору (або

електропровідності) усередині нього.

Томографічні методи базуються на вимірюванні проекцій, за якими реконструється образ [3]. Такими проекціями в імпедансній томографії є потенціали вимірювальних електродів (передаточні опори зі збуджуючих електродів, до яких відімкнене джерело струму, на вимірювальні електроди).

Отже радіоелектронний пристрій вимірювання проекцій є головною частиною імпедансного томографа, враховуючи використання для обчислень стандартних ПЕОМ. Відомі зразки імпедансного томографа мають спільну ідею схемотехнічної реалізації [1-3]. Структурно це виглядає наступним чином: стабільне джерело зондуючого (збуджуючого) струму – блок комутації з електродами – біооб'єкт – приймальна аналогова частина – цифровий блок обробки даних – система візуалізації зображення (рисунок 3).

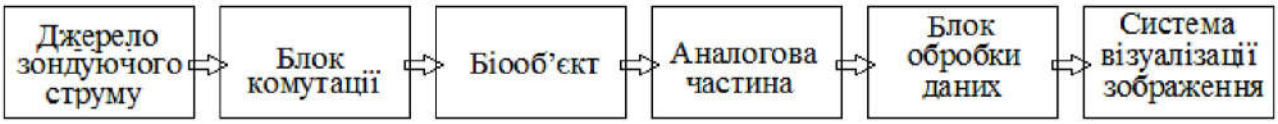


Рисунок3 – Структурна схема імпедансного томографа

2 Розробка структурної схеми комп'ютерного інтерфейсу імпедансного томографа

На риунку 4 показано структурну схему проектованого блоку інформаційного перетворення імпедансного томографа (ІТ), де задаючий генератор (G), схема затримки сигналу (ЛЗ), смуговий фільтр, аналогового інвертора сигналу, два перетворювачі напруга-струм (U/I), два комутатори електродів, диференційний підсилювач електродних сигналів, синхронний детектор, аналого-цифровий перетворювач (АЦП), два регістри пам'яті та блок живлення.

У наведеній структурні схемі задаючий генератор (G) виробляє періодичну послідовність імпульсів прямокутної форми з щілинністю, яка дорівнює 2, тобто прямокутний меандр. Ці імпульси далі поступають на і інтегратор, який складається із схем затримки сигналу (ЛЗ) на чверть періоду та формувачів. Задача інтегратора – сформувати протифазні сигнали для усунення завад від мережі змінного струму. Схема затримки формує з послідовності прямокутних імпульсів аналогічну послідовність імпульсів, але зсунуту відносно першої на половину періоду.

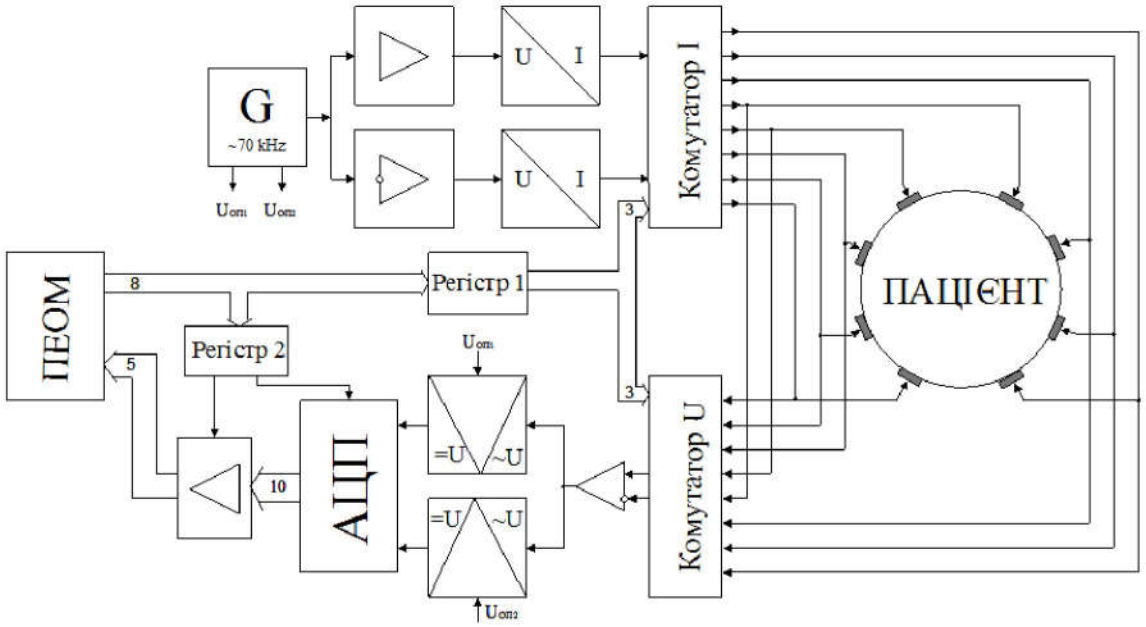


Рисунок 4 – Структурна схема інформаційного перетворення ІТ

Оскільки для вимірювань параметрів об'єкта потрібно використовувати два зондуючі сигнали - джерела струму гармонічної форми, зсунутих на 180^0 , то сигнал з виходу смугового фільтра подається на аналоговий інвертор сигналу і далі на два перетворювачі напруга-струм (U/I).

Отримані на виході перетворювачів напруга-струм (U/I) два зондуючі струмові сигнали гармонічної форми через комутатори (мультиплексори) електродів поступають на об'єкт вимірювання і викликають появу на поверхневих електродах напруг, пропорційних розподілу об'ємного опору в середині об'єкта. Далі комутаторами електродів вони перетворюються в різницеву міжелектродну напругу і подаються для підсилення на входи диференціального підсилювача міжелектродних сигналів.

Смуговий фільтр вибирає з першої періодичної послідовності прямокутних імпульсів основну гармоніку і тим самим формує сигнал гармонічної форми, необхідний для зондування об'єкта вимірювань. Сигнал з виходу диференціального підсилювача гармонічної форми та один з опорних сигналів прямокутної форми поступають на входи синхронного амплітудного демодулятора. В результаті на його виході формується постійна напруга, величина і полярність якої пропорційна міжелектродній напрузі об'єкта вимірювань і різниці фаз між опорною і вхідною напругою. Після фільтрації отриманого сигналу на фільтрах верхніх та нижніх частот і очищенні його від завад перехідних процесів у

фільтрі ФПП, у аналого-цифровому перетворювачі продетектована напруга перетворюється у двійковий вісьмирозрядний код і подається для проведення автоматизованої обробки інформації у вхідну інтерфейсну шину центрального мікропроцесора.

Для керування роботою комутаторів електродів, а також для керування роботою комутатора опорних напруг використовується вихідна інтерфейсна шина мікропроцесора. Оскільки інтерфейсна вихідна шина мікропроцесора має обмежену кількість розрядів (один байт), то це керування мікропроцесор виконує за три такти. Тому для запам'ятовування керуючої інформації з мікропроцесора для кожного такту зокрема використовуються регістри пам'яті (Рг1 і Рг2), з виходу яких збережена керуюча інформація подається далі на відповідні комутатори електродів, АЦП і ФПП .Процес вимірювання біологічних сигналів наведений на рисунку 5.

Рисунок 5 – Схема процесу вимірювання біологічних сигналів

Висновки.

Дана автоматизована система збору та перетворення інформації дослідження організму людини методом електроімпедансної томографії може бути використана у медичній практиці для лабораторних досліджень для візуалізації зображеннь наявності рідини в легенях, оскільки в них струм розповсюджується навколо наповнених повітрям альвеол і присутність рідини буде проявлятись як зона з пониженим питомим опором.

Перелік джерел.

1. Soleimani M. Electrical Impedance Tomography System // BioMedical Engineeeing OnLine, 2006.— May.—P.1—8.

2. Пеккер Я.С., Бразовский К.С., Усов В.Ю., Плотников М.П., Уманский О.С. Электроимпедансная томография. — Томск: Изд-во НТЛ, 2004.—192с.

3. Brown B.H. Electrical Impedance Tomography / B.H. Brown, D.C. Barber // Clinical Physics and Physiological Measurement., 1992. –Vol. 13, Suppl. A. –207p.

УДК 681.32

Ю.А. Матвіюк

Тернопільський національний економічний університет

АВТОМАТИЗОВАНА СИСТЕМА ОБЛІКУ ТОВАРІВ СКЛАДУ НА ОСНОВІ КОНТРОЛЕРА ПЛК-100

Вступ. Організація автоматизованого обліку товарів на складі є невід'ємною частиною сучасного промислового підприємства. Вимоги до роботи даної системи наступні:

- забезпечення швидкого та точного аудиту наявних товарів;
- зручний інтерфейс для зберігання та передачі інформації;
- високий рівень захищеності даних.

Класична система обліку товарів вимагає використання значної кількості людських ресурсів, портативних пристроїв сканування, а також механізмів для пересування по території складу у пошуках потрібного товару. На зміну великої кількості працівників та спеціальних пристроїв зчитування інформації та засобів пересування для кожного з них, приходить автоматизована система сканування та переміщення товарів з використанням новітніх мікроконтролерів, лазерних сканерів, ультразвукових або інфрачервоних датчиків, технології автоматичних конвеєрів[1].

Значну частку існуючих складів, поштових та приймально-транспортних відділень, можна з легкістю перевести на автоматизований режим роботи. В залежності від вимог, можливе створення як автономно працюючих систем обліку товарів, так і функціонуючих в складі глобальної мережі з системи контролю ресурсами підприємства. Отже, за основу у напрямі автоматизації в промисловому комплексі у сучасних умовах є забезпечення інформаційно-транспортних технологій керування.

Метою роботи є дослідження та розробка автоматизованої системи обліку товарів на складі підприємства з використанням сучасних пристроїв зчитування та передачі інформації під управлінням мікроконтролера ПЛК-100.

1. Дослідження вимог до систем автоматизації обліку товарів

Питання оптимального обліку товарів на складі є актуальним. Автоматизована система управління (АСУ) [2] дозволяє забезпечити зручність збору, обробки та захищеної передачі даних товарів

підприємства. Крім цього, встановлення такої системи дозволить значно підвищити швидкість процесу аудиту товарів, знизити до мінімуму похибку в обліку, виключивши людський фактор з технологічного процесу. Завдяки застосуванню надійного мікроконтролера та високочутливих сканерів можна уникнути отримання недостовірних даних про наявність або відсутність товарів, а також знизити ризик їх механічного пошкодження.

Значно зростає рівень безпеки на складі. Це є результатом зниження до мінімуму кількості нещасних випадків за рахунок використання мінімально можливої кількості персоналу. Важливим для досягнення даної мети є використання автоматичних конвеєрів у якості транспортних засобів з переміщення потоку товарів. Вдало спроектована конвеєрна система, у поєднанні з швидкісними сканерами і надійним контролером в основі якісної системи автоматизованого управління, дозволить уникнути зайвого пересування по складському приміщенні.

2. Проектування структури автоматизованої системи

АСУ призначена для автономного обліку та розподілення товару на складі. На рисунку 1 наведена структурна схема автоматизованої системи, де БУ – мікроконтролер ПЛК-100[4] використано у якості блока управління, С-1, С-2, С-3 – сенсори, О – оператор, Ш-1, Ш-1 – штовхальні елементи.

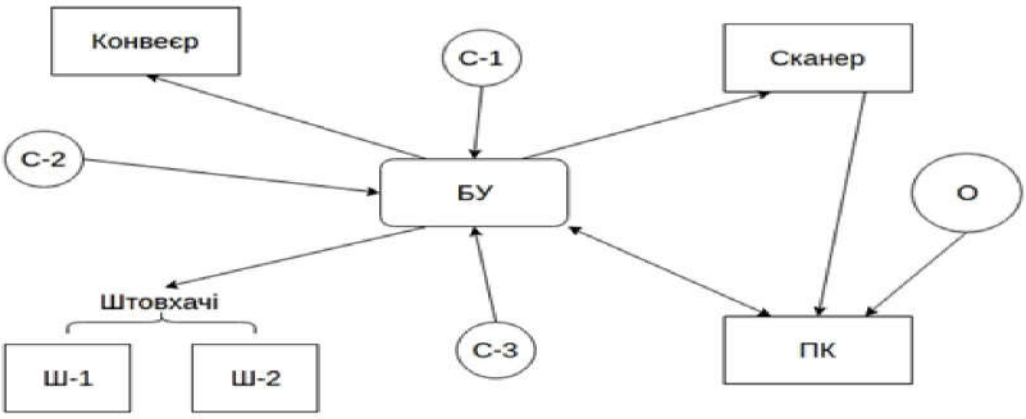


Рисунок 1 – Структура автоматизованої системи обліку товару на складі

Дана система може мати дуже гнучку структуру як з різною кількістю сенсорів та штовхачів, так і з розгалуженим деревом конвеєрних ліній. При необхідності, система може підключатися до локальної або глобальної мережі та в режимі реального часу передавати дані на різні відстані.

Принцип роботи АСУ полягає у точному визначенні розташування коробки з товаром на конвеєрній лінії та виконанні потрібних маніпуляцій компонентів системи у потрібний час. Ультразвукова індикація кожної секції конвеєра сповіщає контролеру про необхідність тих чи інших маніпуляцій.

Спосіб підключення елементів системи до контролера зображено на рисунку 2.

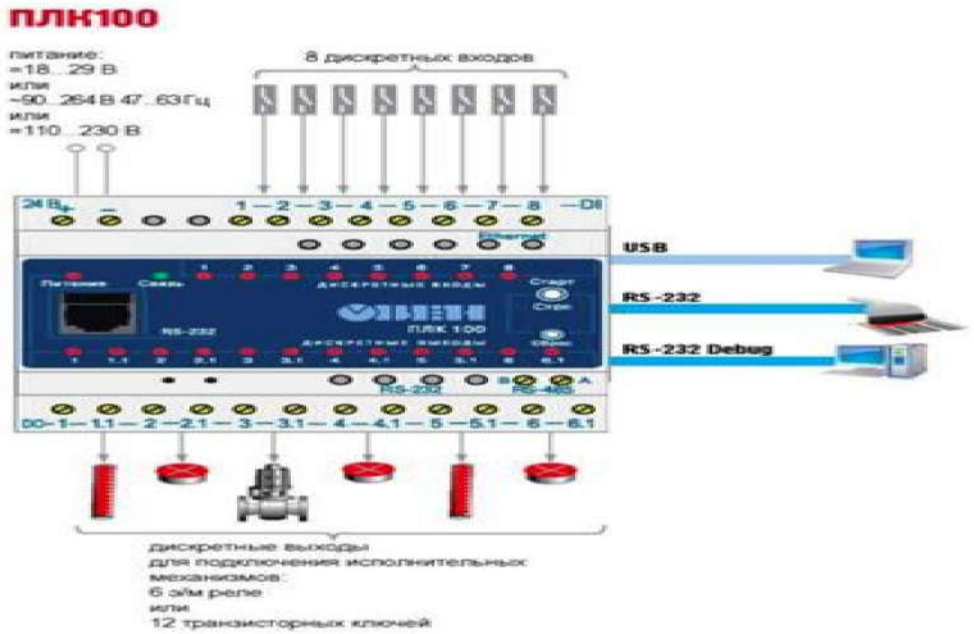


Рисунок 2 – Спосіб підключення елементів системи до контролера

В таблиці 1 наведені характеристики та властивості мікроконтролера Овен ПЛК-100.

Таблиця 1 - Технічні характеристики мікроконтролера Овен ПЛК-100

Конструктивне виконання	Кріплення на DIN-рейку
Рівень захисту корпуса	IP20
Напруга живлення	264 В змінного струму з частотою 47... 63 Гц
Потужність	10 Вт
Індикація передньої панелі	1 індикатор живлення, 8 індикаторів входів,12 індикаторів виходів
Центральний процесор	32-х розрядний RISC-процесор 200 МГц на базі ядра ARM9

Продовження таблиці 1

Об'єм оперативної пам'яті	8 Мбайт
Розмір Retain-пам'яті	4 кбайт
Час виконання циклу ПЛК	Мінімальний 250 мкс (нефіксований), базовий від 1 мс
Кількість дискретних входів	8
Гальванічна розв'язка дискретних входів	Є, групова
Інтерфейси	Ethernet 100 Base-T RS-232 – 2 канали RS-485 USB 2.0 -Device
Максимальна частота сигналу, що подається на дискретний вхід	1 кГц при програмній обробці 10 кГц при застосуванні апаратного лічильника і обробника кодера
Протоколи	ОВЕН, ModBus-RTU, ModBus-ASCII DCON, ModBus-TCP, GateWay (протокол CODESYS)

Керуючий мікроконтролер має забезпечувати взаємодію усіх компонентів системи. АСУ обліку товару здатна:

- знизити кількість людських ресурсів на виробництві;
- значно пришвидшити процес проведення обліку.
- знизити до мінімуму кількість помилок та розбіжностей даних, у зв'язку з виключенням людського фактору;
- полегшити процес сортування товару;
- знизити ймовірність нещасних випадків;
- забезпечити високий ККД при потенційному зниженню собівартості з плином часу.

На рисунку 3 представлено приклад транспортно-сортувальної частини автоматизованої АСУ з використанням конвеєра та штовхачів.

Рисунок 3 - АСУ з використанням конвеєра та штовхачів

Система є дуже гнучкою та простою у використанні й обслуговуванні. Варіації кількості сенсорів та штовхачів дозволяють легко доповнювати систему та розгалужувати конвеєрну лінію, тим самим забезпечити ефективність процесу сортування.

Висновки.

Запропонована система автоматизації дозволяє полегшити та пришвидшити процес обліку товарів на складі. Дана АСУ здатна виключити більшість недоліків, які зустрічаються у процесі ручного обліку. Гнучкість на простота в налаштуванні дозволяє задіювати меншу кількість працівників до обслуговування системи. Підключення до локальної мережі дозволяє контролювати процес з будь-якого місця підприємства, а у зв'язці з використанням методів шифрування можна передавати інформацію про процес по мережі інтернет без ризику витоку даних.

Дана АСУ може бути вдосконалена збільшенням кількості сенсорів та сортувальних механізмів, розгалуженням конвеєрної лінії, використанням більшої кількості сканерів, застосуванням систем шифрування для передачі інформації у реальному часі до баз даних підприємства (наприклад інформації про наявність товару у інтернет-магазині).

Перелік джерел.

1. Смехов А.А. Автоматизированные склады / А.А. Смехов, – 4-е изд., перераб. и доп. М.: Машиностроение, – 1987. – 295 с.

2. Попович М. Г. Теорія автоматичного керування : Підручник – 2-ге вид., перероб. / М.Г. Попович, – К.: Либідь, – 2007. – 656 с.

3. Технологія зчитування штрих-коду – [Електронний ресурс], Режим доступу: http://cash.ru/index.php/tehnologii-schityvaniya-shtrih-koda.html

4. ПЛК100. Програмований логічний контролер - [Електронний ресурс], Режим доступу: https://owen.ua/ua/programovani-logichni-kontrolery/owen-plk100-programovanyi-logichnyi-kontroler

УДК 681.32

О.В. Міщенк, В.Б. Шпак

Тернопільський національний економічний університет

АВТОМАТИЗОВАНА СИСТЕМА АКТИВНОЇ НАВІГАЦІЇ НА ПАРКОВКАХ

Вступ. Організація автоматичного паркінгу є невід'ємною частиною сучасного житлового комплексу. Вимоги користувачів парковки прості: забезпечення безпеки автомобіля, зручний і швидкий проїзд для економії особистого часу, наявність вільних місць. Класична система в'їзду на парковку вимагає докласти певних зусиль, які можуть бути вкрай незручні. Наприклад, висовуватися з вікна або чекати реакції охоронця. На зміну високовартісних радіобрелків, необхідності частої заміни елементів живлення, низького рівня безпеки карток приходить автоматизована система в'їзду на основі технології ультрависокочастотної ідентифікації.

Нині існуючі паркінги [1], парковки і новобудови можуть бути з легкістю автоматизовані. В залежності від вимог, можливе створення автономно працюючих систем автоматизованої парковки так і функціонуючих в складі загальної системи контролю доступу. Таким чином головним напрямом автоматизації в промисловому комплексі на сучасному етапі є створення інформаційно-комунікаційних технологій управління.

Метою роботи є дослідження та розробка автоматизованої системи мониторингу паркомісць та навігації на автомобільних парковках.

1. Дослідження вимог до систем автоматизації паркування автомобілів

Питання оптимального паркування автомобілів на парковках є актуальним. Автоматизована система управління (АСУ) [2] дозволяє забезпечити безпеку припаркованих машин. Крім цього встановлення такої системи дозволить відстежувати переміщення всіх машин по території парковки за допомогою візуальної навігації. При використанні контрольно-пропускної системи можна уникнути зловживання своїми повноваженнями та халатність з боку, як персоналу, так і відвідувачів.

Істотно зростає рівень сервісу, це відбувається за рахунок створення максимально можливого комфорту при паркуванні. Важливим для цього є розпаралелення потоку машин на два – бажаючих заїхати та виїхати. Добре

розмічена паркувальна зона в сукупності з якісною системою автоматизації дозволить уникнути безладного пересування на території [3].

2. Розробка структури автоматизованої системи навігації на парковці

АСУ призначена для автономного контролю за наявністю вільних місць на парковці. На рисунку 1 наведена структура системи, де ЦК-центральний контролер, КД – контролер дисплею.

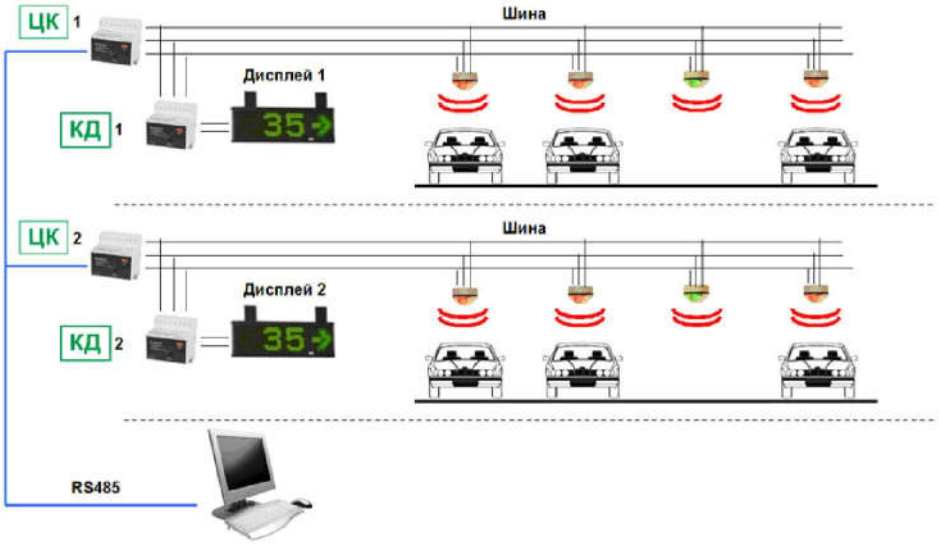


Рисунок 1 – Структура автоматизованої системи моніторингу паркомісць

Ультразвукові датчики, які встановлюються над паркомісцем, забезпечують виявлення наявності автомобіля про що сигналізують за допомогою LED-індикаторів (зелений \ червоний). Кількість вільних місць відображається на дисплеї в цифровому вигляді. Запропонована система може мати як лінійну так і розподілену структуру. При необхідності, система може підключатися до АРМ оператора для ведення обліку завантаженості і моніторингу вільного місця на парковці.

Принцип роботи АСУ полягає у точному визначенні розташування вільних і зайнятих місць і / або в підрахунку кількості в'їхали і виїхали машин. Світлова індикація кожного паркувального місця та інформаційні табло вказують водію вільні місця і оптимальний маршрут до них. АСУ забезпечує оперативний і постійний контроль завантаженості з наданням персоналу всієї необхідної інформації, управління світлофорами, табло та шлагбаумами.

Принцип реалізації автоматизованої системи навігації на парковці наведений на рисунку 2.

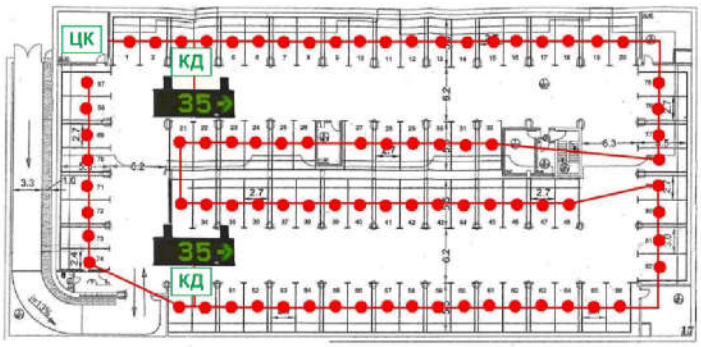


Рисунок 2 – Принцип реалізації автоматизованої системи навігації на парковці

В таблиці 1 наведені компоненти для різних варіантів системи автоматизованої системи навігації на парковці: 1 - для визначення статусу місця парковки, 2 - для визначення статусу рівня парковки та 3 – комбінованої.

Таблиця 1 - Компоненти ас навігації на парковці

Компоненти системи	1	2	3
Сервер з процесором Intel Core i3-3210	+	+	+
Мікроконтролер PIC16F84A	+	+	+
Мережевий контролер BPOS101-2-PM-B	+	+	+
Ультразвуковий датчик присутності автомобіля S400L	-	+	+
Індикатор зайнятості місця S400-RI25	-	+	+
Лічильник-суматор BPOS882SUM	+	-	+
Навігаційне табло TBA90	+	+	+
Інформаційне табло TB3D90-A	+	+	+
УЗ або ІЧ датчики виїзд/в'їзд автомобіля S400MS	+	-	+
Джерело живлення табло і датчиків	+	+	+

На рисунку 3 представлена структура комплексної АСУ активної навігації на парковках.

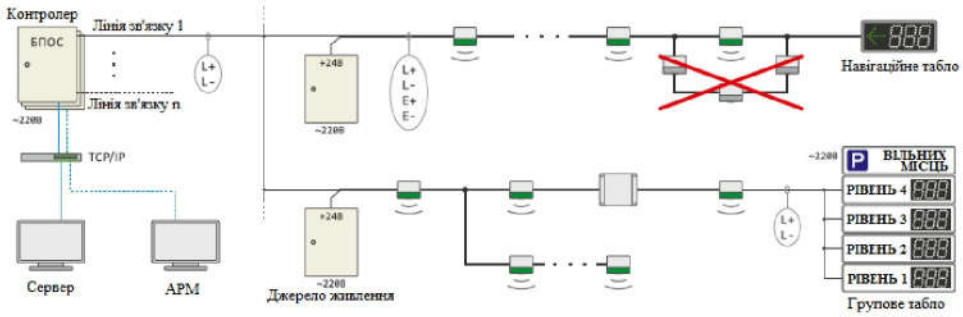


Рисунок 3 - Структура АСУ парковки

Керуючий мікроконтролер має забезпечувати взаємодію усіх компонентів системи. АСУ паркування автомобілів дозволяє:

- зменшити затрати часу на паркування автомобілів, оскільки інформативні табло надають водієві інформацію про наявність вільних місць і він не витрачає свого часу;

- підвищити продуктивність за рахунок оперативного контролю наявності автомобіля, що допомагає швидше заповнювати порожні паркомісця;

- знизити витрати енергоресурсів та покращити екологійчну ситуацію, тому що при пошуку вільного місця на парковці водій витрачає на 20% менше бензину;

Простий монтаж за рахунок знімних коннекторівдозволяє здійснювати швидке налаштування системи через програматор. Система має широкі комунікаційні можливості, підключення до PC для центрального моніторингу, контролю та ведення статистики через SCADA систему.

Висновки.

Запропонована система автоматизації навігації на парковці дозволяє інформувати водія транспортного засобу про вільне місце в різних секторах парковки. Така спеціальна навігація по території допомагає в найкоротший час знайти вільне місце на будь-якому з вільних рівнів парковки за допомогою спеціальних табло та різних індикаторів, що дозволяє відрегулювати транспортні потоки на території парковки. АСУ забезпечує фіксацію всіх даних про час в'їзду та виїзду будь-якої машини на паркувальні місця, що дозволить збирати статистичні дані про те, в який час паркінг найбільш завантажений. Для подальшого вдосконалення системи передбачена можливість її розширення відповідно до збільшенння кількості паркувальних місць.

Перелік джерел.

1. Система управления парковкой (автоматизация паркинга) . Електронний ресурс. Режим доступу: https://leater.com/services/sistema-upravleniya-parkovkoy.html

2. Береза А. М. Основи створення інформаційних систем: навч. посіб. / А. М. Береза. – 2 вид., перероб. і доп. – К.: КНЕУ, 2001. – 214 с.

3. Харазов В.Г. Интегрированные системы управления технологическими процессами.- 592 с.– СПб.: Профессия, 2009. –процессами.

УДК 681.32

О.І. Смагула

Тернопільський національний економічний університет

ОПТИМІЗАЦІЯ УПРАВЛІННЯ ПРОЦЕСУ ОЧИЩЕННЯ СТІЧНИХ ВОД

Вступ. У зв'язку із значним розвитком комп'ютерної техніки вона широко застосовується у багатьох сферах людської діяльності, а тому є невід'ємною складовою більшості виробничих та організаційних процесів. З допомогою електронних обчислювальних машин реалізуються операції, які вимагають великої точності, швидкодії, а значить не можуть бути виконані людиною.

Охорона навколишнього середовища є одним з основних завдань народного господарства. У зв'язку з цим проблема очищення стічних вод промислових підприємств і населених місць придбала особливо важливе значення. Тому актуальним завданням є розробка нових та вдосконалення існуючих способів очищення, зниження капітальних і експлуатаційних витрат на очищення води, організація замкнутих систем водопостачання промислових підприємств, широке впровадження автоматизації і механізації.

Метою роботи є дослідження процесу очишення стічних вод та розробка системи управління цим процесом на базі мікроконтролера.

1. Досідження процесу очищення стічних вод

Стічні води повинні очищатися від іонів важких металів (міді, цинку, нікелю і ін). Традиційно воду від з'єднань важких металів очищають шляхом перекладу їх в нерозчинні у воді з'єднання, які потім видаляють відстоюванням, флотацією, фільтрацією і іншими способами розділення твердої і рідкої фаз. Переклад в тверду фазу в основному здійснюють введенням лугу з утворенням гідроксидів, гідроксокарбонатів, карбонатів, а також сульфідних іонів, що приводить до утворення водонерозчинних сульфідів важких металів.

Згідно діючим нормативним документам скидання стічних вод в системи каналізації населених пунктів і у водні об'єкти допустимі у випадках, якщо вони характеризуються величиною pH=6.5 - 8.5. У тому випадку, коли pH стічних вод відповідає кислій (pH< 6.5) або лужній (pH>8.5) реакції, стічні води підлягають нейтралізації, під якою

розуміють зниження концентрації в них вільних Н+ або ОН - іонів до встановлення pH в інтервалі 6.5-8.5 [1].

Для нейтралізації стічних вод найчастіше застосовують вапно, яке додають у воду у вигляді грубої суспензії - вапняного молока. При нейтралізації вапном стічних вод, що містять вільну сірчану кислоту і її солі, утворюється сульфат кальцію, який досягши певної концентрації випадає в осад. Присутній у вапняному молоці шлам сприяє коагуляції частинок гідроксидів металу і інших нерозчинних домішок. Розчинність осаду залежить від його структури, яка в свою чергу визначається умовами проведення процесу нейтралізації Теоретичні витрати деяких реагентів на реакцію приведені в таблиці 1.

Таблиця 1 - Теоретична витрата реагентів на осадження металів з розчинів

ІОН	Витрата реагенту на 1гр іона металу, г			
	CaO		CaO	
Cu2+	0.88	1.16	1.26	1.67
Fe3+	1.51	1.99	2.15	2.85
Fe2+	1.00	1.32	1.43	1.90
Zn2+	0.86	1.13	1.22	1.62
Al3+	3.11	4.11	4.45	5.89
Ni2+	0.95	1.26	1.36	1.81
Cr3+	1.61	2.13	2.31	3.06

Технологію очищення стічних вод можна розділити на декілька загальних стадій: накопичення стоків, їх обробка, розділення рідкої і твердої фаз, остаточне очищення води, обезводнення осаду.

2. Розробка комп'ютеризованої системи управління процесом очищення води

При виборі основних контурів необхідно визначити цільове призначення процесу, взаємозв'язок його з іншими процесами виробництва, показник ефективності і значення, на якому він повинен підтримуватися, статичні і динамічні характеристики об'єкту, що обурюють дії і можливості їх усунення до надходження в апарат. Особливу увагу необхідно звернути на стабілізацію вхідних параметрів, оскільки з їх зміною в об'єкт поступають найбільш сильні обуренняї [1]. Для забезпечення необхідного режиму роботи гальванокоагуляційної установки і отримання зрештою очищеної води заданої гранично

допустимій концентрації виникає необхідність в автоматичному регулюванні ряду технологічних параметрів (таблиці 2).

Таблиця 2 – Параметри регулювання

№	Параметри	Канали внесення регулюючих дій	Технічні засоби автоматизації
1	Рівень в першій ємності стічних вод	Трубопровід подачі стічних вод	акустичний рівнемір ЭХО-3
2	Кислотність в першій ємності стічних вод	Трубопровід подачі сірчаної кислоти	потенціометр ДПг-4М
3	Концентрація нікелю в другій ємності стічних вод	Трубопровід видачі стоку із ємності для подачі на гальванокоагулятор	аналізатор вмісту металів в розчинах типу "Спектр-4А"
4	Кислотність стоків в другій ємності	Трубопровід подачі вапняного молока в ємність	потенціометр ДПг-4М
5	Концентрація заліза в другій ємності стічних вод	Трубопровід подачі хлорної вапно в ємність	аналізатор вмісту металів в розчинах типу "Спектр-4А"
6	Рівень мула в першому відстійнику	Трубопровід видачі мула з першого відстійника	акустичний рівнемір ЭХО-3
7	Рівень мула в другому відстійнику	Трубопровід видачі мула з другого відстійника	акустичний рівнемір ЭХО-3
8	Рівень освітленої води в 1-ій буферній місткості	Трубопровід видачі освітленої води з 1-ої буферної місткості	акустичний рівнемір ЭХО-3
9	Рівень освітленої води в 2-ій буферній місткості	Трубопровід видачі освітленої води з 2-ої буферної місткості	акустичний рівнемір ЭХО-3
10	Контроль та сигналізація тиску стислого повітря	Трубопровід подачі освітлених вод	перетворювач тиску САПФІР - 22ДИ

Навдені в таблиці 2 контури контролю і регулювання дозволяють вести процес очищення в оптимальному режимі.

На рисунку 1 наведена структура комп'ютеризованої системи управління процесом очищення води, яка складається з контролера (1), сервера (2), засобу доступу до інтернету (3), ПК (4 та 7), пульта дистанційного керування (5) та мобільного пристрою (6).

Система обладнана модулем дистанційного зв'язку(wi-fi, GSM, radio) обмінюється інформацією з сервером, який опрацьовує отриману інформацію, має доступ до інтернету та дозволяє дистанційно управляти установкою через інтернет(ПК – використання веб інтерфейсу, мобільні пристрої з IOS та Android за допомогою спеціального ПЗ) та через модулі безпровідного звязку (ПК та пультом дистанційного управління).

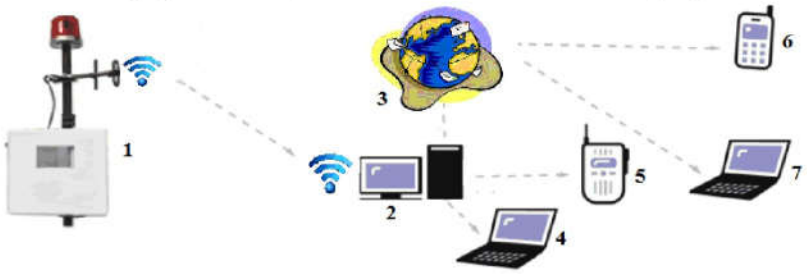


Рисунок 1 – Структурна схема мікропроцесорного вимірювача тиску

Комп'ютеризована система певним чином реагує на вхідний сигнал з датчиків і здійснює його відповідну обробку, тому для роботи з цифровими даними потрібна мікропроцесорна система, яка змогла б ефективно виконувати поставлену перед нею задачу. Оскільки процес реєстрації вхідного сигналу не є досить енергозатратним і продуктивним, то в якості такої мікропроцесорної системи вибрано мікроконтролер AVR Atmega32 [2].

Висновки.

Розроблена комп'ютеризована система управління очищенням води на базі мікропроцесорного контролера Atmega 32.

Практична цінність роботи полягає в тому, що для реалізації такої схеми потрібно порівняно небагато затрат, а ефективність при цьому не погіршиться а навіть покращиться..

Перелік джерел.

1. Закон України Про питну воду, питне водопостачання та водовідведення від 18.05.2017 р. N 2047-VIII

2. Мікроконтролер AVR Atmega32. [Електронний ресурс].- Режим доступу: https://avrlab.com/ATmega32-AVR-datasheet-32Kb

УДК 681.32

М.В. Серветник, І.Р. Пітух

Тернопільський національний економічний університет

МІКРОПРОЦЕСОРНИЙ ПРИСТРІЙ КОНТРОЛЮ ТИСКУ РІДКИХ ТА ГАЗОПОДІБНИХ РЕЧОВИН

Вступ. Вимірювання і реєстрація тиску широко розповсюджені як в промисловості, так і в повсякденному житті: метеорологічні барометри показують атмосферний тиск, медичні тонометри - тиск у манжеті.

Забезпеченість України паливно-енергетичними ресурсами одне з найголовніших завдань національної економіки, без розвитку якого неможливе успішне здійснення соціальних, економічних і науково-технічних програм. Газ набув дуже широкого використання в нашому житті, оскільки є не лише висококалорійним паливом, але і цінною сировиною для хімічної промисловості.

На даний час розроблено багато засобів вимірювання тиску газу [1]. Актуальність ж розробки інформаційно-вимірювальної системи тиску газу полягає в необхідності підвищення точності, швидкодії та одночасному контролі декількох параметрів, а саме тиску, розрідження та перепаду тиску у газопроводі, а також вимірювання температури за допомогою однієї системи та представлення її оператору в зручному вигляді на одному відеотерміналі. Сполучення інформаційно-вимірювальної системи з комп'ютером дозволяє швидко отримувати, обробляти та зберігати для подальшого використання великі потоки інформації.

Метою роботи є дослідження засобів вимірювання тиску та розробка мікропроцесорного пристрою контролю тиску газів та рідин із підвищеною точністю вимірювань.

1. Досідження характеристик сенсора тиску

Мікропроцесорний вимірювач тиску проектується на базі сенсора тиску фірми Honeywell. Для підвищення точності вимірювання тиску необхідно дослідити його характеристику та розробити математичну модель вимірювання. Характеристика сенсора наведена у технічному описі у вигляді графічних залежностей [2].

Зокрема, на рисунку 1 показано залежність похибки від температури (1 psi = 6 894,75729 Паскаля).

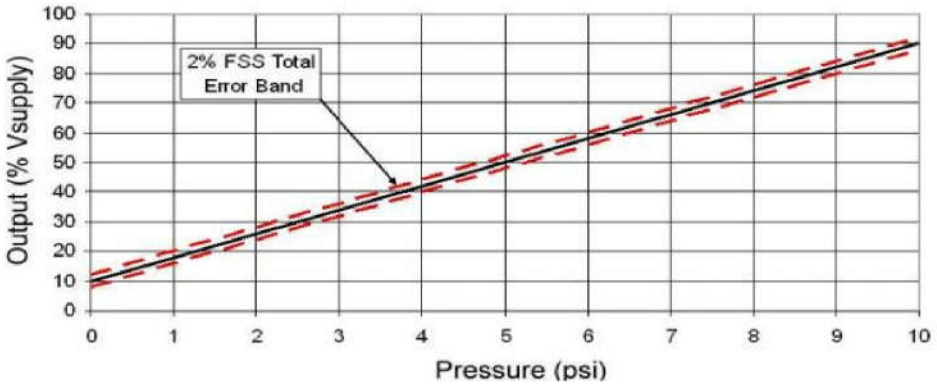


Рисунок 1- Залежність похибки від температури для ASDX

В результаті вимірювань встановлено значення за формулою:

$$Output(V)=(0.8*Vsupply / Pmax–Pmin)*$$
$$*(Preassureapplied–Pmin)+0.10*Vsupply$$

Маючи ці дані, можна побудувати таблицю залежностей між реальним тиском і результатами, які отримуємо від сенсора. Здійснивши декілька вимірів отримаємо реальні значення тиску (PSI), значення при неперервному вимірюванні і опорною напругою 5В (V output) і значення, отримані шляхом вимірювання сенсором (PSI(error)) (таблиця 1).

Таблиця 1 - Значення тиску шляхом вимірювання сенсором

PSI	V output	PSI(error)
1	0.594	1.02
2	0.859	2.04
3	1.122	3.06
4	1.386	4.08
5	1.65	5.1
6	1.914	6.12
7	2.178	7.14
8	2.442	8.16
9	2.739	9.18
10	2.97	10.2

Для підвищення точності результатів вимірювань, застосовано апроксимацію характеристики датчика тиску. В результаті досліджень було отримано аналітичну форму представлення функції залежності результуючої тиску від тиску на виході сенсора. Маючи ці дані, можна підвищити точність вимірювання нашої системи.

$$f(x)= -0.0000448081 * EXP (-0.00000224136*x) + 448078.4566655$$

де x - результат, отриманий від сенсора, а $f(x)$ – функція після коректування.

2. Розробка структурної схеми вимірювача тиску

Мікропроцесорний вимірювач тиску складається з наступних вузлів: сенсора тиску, схеми синхронізації, стабілізатора напруги, мікропроцесора, символьного індикатора, вузла RS-485 для передачі виміряних значень в інформаційно-вимірювальну систему (рисунок 2).

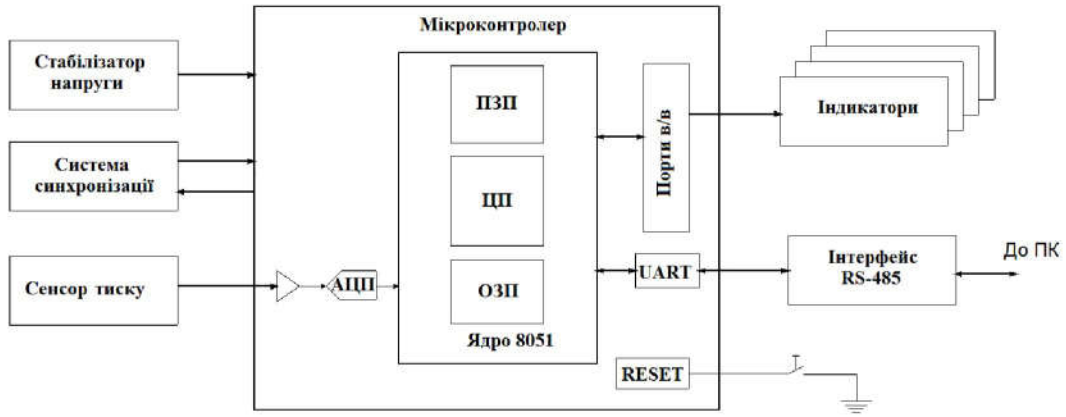


Рисунок 2 – Структурна схема мікропроцесорного вимірювача тиску

Для реалізації пристрою було обрано мікроконтролер MSC1211Y5, який являє собою основу системи та не вимагає для свого функціонування жодних додаткових зовнішніх компонентів. Оскільки проектований мікропроцесорний вимірювач тиску призначений для промислових потреб то навантаження на нього буде значним і доцільно використати датчик Honeywell серії ASDX-DO.

Технічний інтерфейс (RS-485) забезпечує можливість інтеграції спеціалізованої системи діагностики в різні технічні системи. Сигнали інтерфейсу RS-485 передаються диференціальними перепадами напруги величиною (0,2 ... 8) В, що забезпечує високу стійкість і загальну довжину лінії зв'язку до 1 км. Для передачі виміряних значень в інформаційно-вимірювальну систему через RS-485 використано мікросхему фірми Maxim MAX481. Для виводу отриманої інформації про тиск використаємо динамічну індикацію, семисегментні світлодіодні індикатори.

3. Розробка алгоритму роботи міккропоцесорного пристрою

Програма, з якою повинен працювати мікроконтролер, має два загальних блоки: перший – це ініціалізація основних вузлів

мікроконтролера, другий – це керування роботою мікроконтролера (рисунок 3).

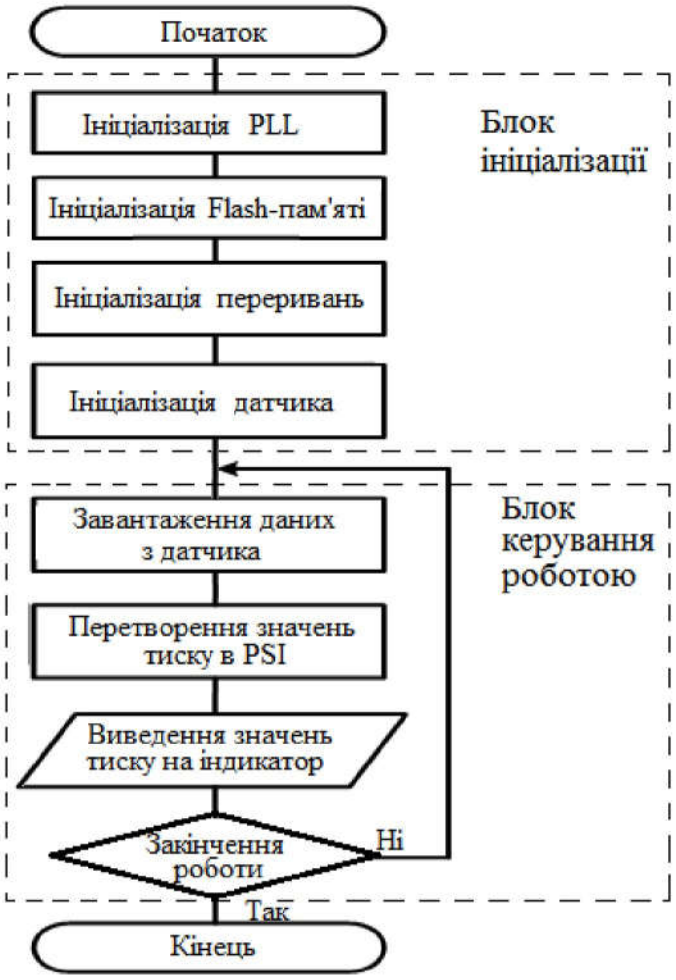


Рисунок 3 - Схема алгоритму роботи програми

Робота програми полягає у завантаженні даних з датчика їх перетворенні у PSI і виведення даних на індикатор. Всі дії відбуваються багаторазово з визначеним інтервалом який у нашому випадку складає менше 0.2 сек.

Висновки.

Розроблено мікропроцесорний вимірювач тиску газу із підвищеною точністю вимірювань Пристрій може використовуватись в різних системах вимірювання як для промислових так і для побутових потреб.

Перелік джерел.

1. Основи метрології та вимірювальної техніки. Т. 2. Вимірювальна техніка. За ред Б. Стадника. Львів: Видавництво Львівської політехніки, 2005Т. 656 с. .

2. ASDXRRX100PD7A5 - Датчик Тиску, серія ASDX. [Електронний ресурс]. Режим доступу: http://www.farnell.com/datasheets/1676926.pdf?_ga= 2.18131705.1164198456.15736399 71 -1980142734.1573639971

УДК 681.32

С.М.Недошитко

Тернопільський національний економічний університет

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ДОЗУВАННЯ СИПУЧИХ МАТЕРІАЛІВ

Вступ. Автоматизація виробництва - основа розвитку сучасної промисловості, основний напрямок технічного прогресу. Мета автоматизації виробництва полягає в підвищенні ефективності праці, поліпшенні якості продукції, що випускається, створення умови для оптимального використання всіх ресурсів виробництва. Автоматизація змінює характер праці людини, виконуючи функції технічного обслуговування, необхідні для заданого функціонування автоматичної системи.

Сучасні автоматизовані ваговимірювальні комплекси забезпечують надійну інформацію про технологічні параметри процесу та показниках кількості зважуваних матеріалів. Зворотній зв'язок дозволяє своєчасно діагностувати і коригувати відхилення від технологічного процесу, і, завдяки, цьому, скорочувати матеріальні і фінансові втрати [1, 2].

Метою роботи є розробка автоматизованої системи керування комплексом технологічного порційного вагового дозування сипучих матеріалів, яка забезпечує високу продуктивність при високій точності дозування.

1. Обгрунтування створення систем автоматизованого зважування і дозування

Етапи зважування продукції традиційно виконуються за участю людини, і саме на цих ділянках технологічного процесу відбуваються основні помилки оформлення, з'являються похибки зважування, які в результаті і приводять до накопичуваної помилки відпуску. Це є основною причиною автоматизації процесів зважування [1, 2].

Особливо актуальними є процеси зважування і дозування для харчової галузі та виробництва сипучих, штучних товарів, кількість яких визначається на вагу, зокрема: харчова промисловість; зернопереробна промисловість; прийом і відпуск продукції на оптових складах; багатокомпонентна продукція; добрива; нитки синтетичні або штучні і волокна; цукор.

У електронних зважувальних машин є істотні переваги в порівнянні з електропневматичними. До них входять: наявність дисплея для індикації ваги при кожному зважуванні; автоматичне саморегулювання ваги; автоматичний контроль передачі товару з зважувального бункера в мішок; програмоване тарування з контролем ваги бункера; узгодження фаз зважування з автоматичним регулюванням швидкості і частоти зважування. Важливим є те, що електронними вагами можуть комплектуватися будь-які пакувальні машини.

Електропневматичні зважувальні пристрої не характеризуються вищеописаними перевагами, проте є простими й економічними. Вони складаються з бункера ваг, в який надходить продукт, що підлягає зважуванню, коромисла з плечима однакової довжини, кронштейна для установки контрвантажу.

Електронні зважувальні пристрої в потоці призначені для зважування сипучих продуктів у потоці, коли вони переміщуються з однієї ємності в іншу. Як правило, такі пристрої застосовуються всередині виробничого циклу для контролю кількості товару.

Такі системи відрізняються зменшеними розмірами і простотою в установці. Електронний керуючий пристрій, як і в інших типах систем зважування, складається з клавіатури для програмування і введення даних, і цифрового дисплея для відображення результатів зважування.

2. Проектування системи автоматизованого фасування сипучих матеріалів

Нерідко постає доволі проста задача рівномірного наповнення певної ємності (бункера, силосу, бака і т.д.) сипучими матеріалами такими, як зерно, тирса, мінеральні добрива, гранульовані будівельні суміші, харчові складники.

Автоматизована система управління призначена для контролю процесу порційного зважування та змішування сипучих і рідких продуктів в автоматичному і ручному режимі, відповідно до заданого рецепту. Функції системи:

- автоматичне і дистанційне керування двигунами дозаторів, засувками та іншими виконавчими механізмами, які беруть участь в роботі системи з безперервним контролем їх роботи;

- візуальний контроль за роботою системи на екрані дисплея;

- сповіщення обслуговуючого персоналу в разі виникнення аварійної ситуації;

- збереження в архів повної інформації про роботу системи;

- зв'язок по комп'ютерній мережі з іншими системами (комп'ютерами) для оперативного обміну інформацією.

Пропонується варіант надійної та недорогої водночас схеми системи автоматичного дозування (рисунок 1). Система автоматизації забезпечує можливість управління в ручному та автоматичному режимах комплексом обладнання ваг, контролю за технологічними параметрами.

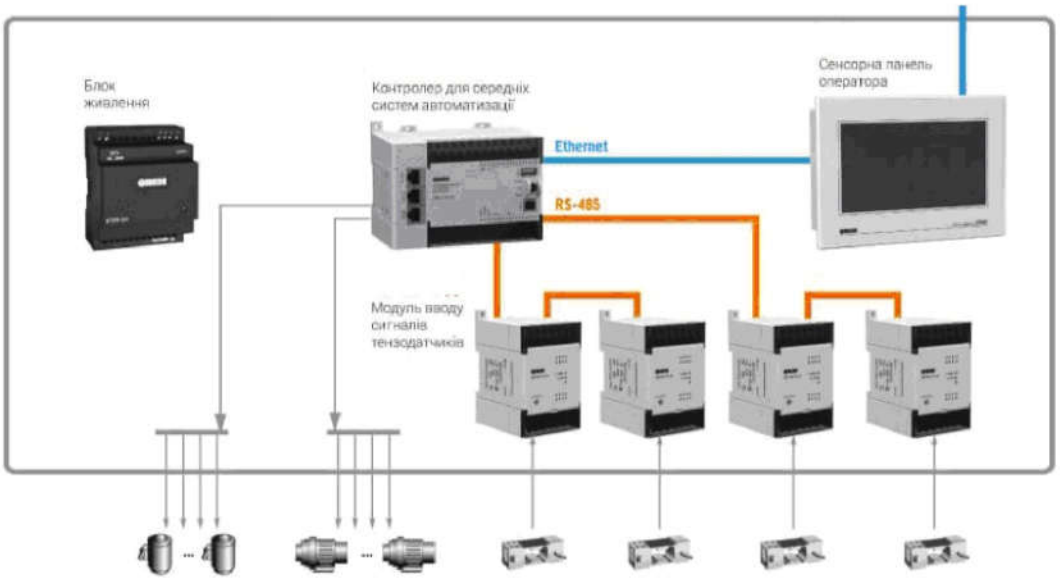


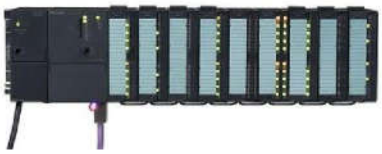
Рисунок 1 - Структура системи автоматизації

Основні завдання, які вирішуються системою: збільшення точності зважування та надійності системи; скорочення часу відвантаження; автоматична фіксація і підсумовування значень схилів; виключення впливу людського фактору на результат вимірювань; протоколювання роботи системи і дій оператора.

Склад системи автоматизації представлений на рисунку 2.

Центральним елементом системи є контролер VIPA 300S з встановленими двоканальними ваговими модулями SIWAREX U і модулями I\O. Вимірювана інформація і функції управління виводяться на місце оператора за допомогою текстової панелі VIPA OP03.

За місцем встановлюються ваговимірювальні датчики SIWAREX R і ємнісні датчики верхнього рівня Carlo Gavazzi EC3025. Управління засувками здійснюється за допомогою конічних мотор-редукторів TRANSTECNO серії GKR.



ПЛК VIPA 300S

Ваговимірювальна електроніка SIWAREX U

Ваговий процесор ПВ-310

Панель оператора OP 03

Ваговий датчик Siemens SIWAREX WL

Датчик рівня сипучих матеріалів ProGap-S

Рисунок 2 – Компоненти системи автоматизації

Високопродуктивна система управління серії ПЛК 300S базується на технології SPEED7, завдяки якій вона є однією з найшвидших і ефективних в застосуванні систем управління в своєму класі. Програмування здійснюється за допомогою WinPLC і / або STEP7 компанії Siemens.

Контролери відрізняє не тільки їх високу швидкодію. При необхідності їх швидкість реакції додатково може бути істотно збільшена за допомогою швидкісної системної шини SPEED-bus.

Висновки.

Проведене дослідження технологічного процесу дозування і фасування показало, що підвищення точності дозування, істотно впливає на продуктивність технологічного процесу. Для вирішення цієї проблеми в даній роботі розроблена автоматизована система фасування сипучих речовин, яка забезпечує високу продуктивність при високій точності дозування.

Перелік джерел.

1 Барало О.В. Автоматизація технологічних процесів і системи автоматичного керування: Навч. посібник / О.В. Барало, П.Г. Самойленко, С.Є. Гранат, В.О. Ковальов – К.: Аграрна освіта, 2010. – 557 с.

2. Ельперін І. В. Автоматизація виробничих процесів: підр. / І.В. Ельперін, О.М. Пупена, В.М. Сідлецький, С. М. Швед. – К.: Вид-во Ліра-К, 2015. – 378 с

УДК 681.32

С.А. Труш, А.О. Вітвіцький

Тернопільський національний економічний університет

МІКРОПРОЦЕСОРНИЙ ПРИСТРІЙ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Вступ. Важливим елементом забезпечення цілісності конфіденційної інформації є захист від несанкціонованого доступу до ресурсів інформаційних систем, що викликає необхідність створення надійних і зручних систем контролю доступу. Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та автентифікації. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. В результаті їх виконання користувач або отримує доступ до певних ресурсів інформаційної системи, або не отримує.

На даний момент, технології розвиваються з великою швидкістю, оскільки ми живемо в часи технологічного прогресу. Саме тому прийнято вважати, що одним з найкращих напрямом для беззаперечної ідентифікації особи є автоматичне визначення її особистих характеристик, які називаються біометричними. Відповідно до цього з'явилась і нова технологія ідентифікації - біометрична. Біометрія й основані на її принципах системи стали ефективним засобом убезпечення всіх видів власності, захисту від шахрайства, фальсифікації та криміналу [1-3]. Їх подальше впровадження в різні галузі є актуальним завданням, адже забезпечить створення зручних і надійних інструментів як для державного сектора, індустріальних і комерційних структур, так і для окремих громадян.

Метою роботи є дослідження методів біометричної автентифікації та проектування спеціалізованого пристрою ідентифікації персони за біометричними даними, а саме відбитками папілярних візерунків на пальцях.

1. Порівняльні характеристики та аналіз методів автентифікації

Ідентифікація – процедура розпізнавання користувача в системі за допомогою наперед визначеного імені (ідентифікатора) або іншої інформації про нього, яка сприймається системою. Вона є початковою

процедурою надання доступу до системи, після неї здійснюється автентифікація та авторизація [1].

Автентифікація – це процедура перевірки належності ідентифікатора об'єкту, тобто встановлення чи підтвердження дійсності, і перевірка чи є об'єкт або суб'єкт, що перевіряється, справді тим, за кого він себе видає. Біометрія – це сукупність автоматизованих методів і засобів ідентифікації людини, заснованих на її фізіологічній або поведінковій характеристиці [1].

Загалом, всі системи біометричної автентифікації виконують дві основні функції реєстрацію та розпізнавання [2]. Розпізнавання відбувається шляхом порівняння даних зі зчитувального пристрою з єдиним шаблоном, що відповідає людині яка перевіряється або з усіма зареєстрованими шаблонами.

Всі методи біометричної автентифікації можна розділити на дві групи [3]:

- статичні методи грунтуються на фізіологічній характеристиці людини, тобто унікальній властивості, даному йому від народження і невід'ємне від нього;

- динамічні методи грунтуються на поведінковій (динамічної) характеристиці людини, тобто враховують особливості, характерні для підсвідомих рухів у процесі відтворення певної дії (рисунок 1).

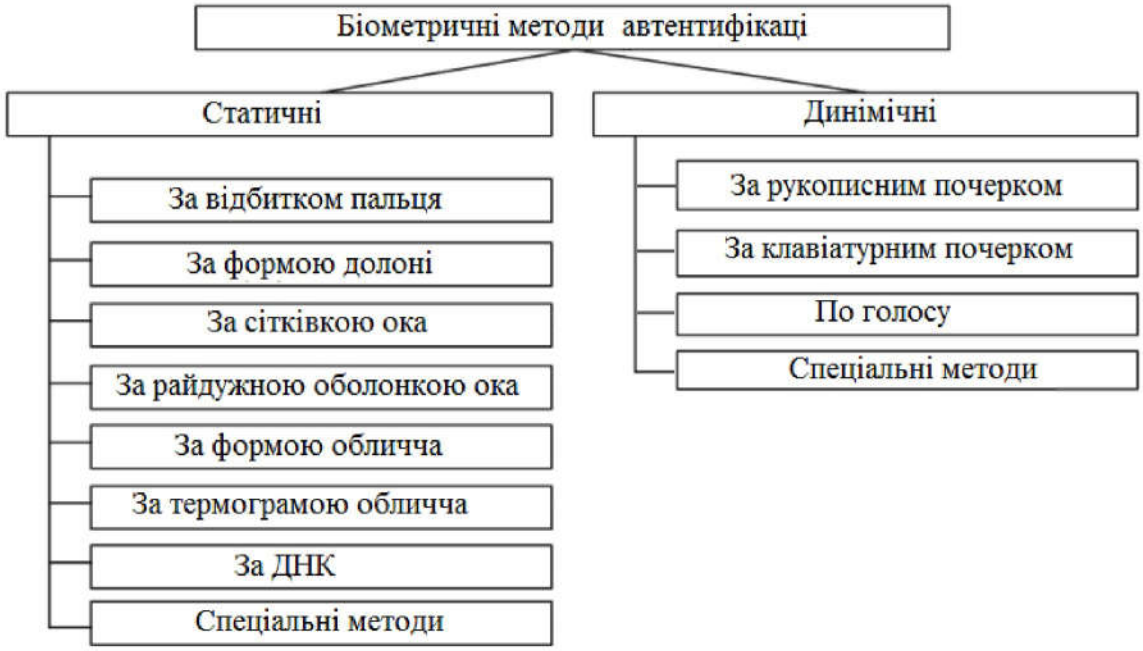


Рисунок 1 - Класифікація методів біометричної автентифікації користувачів

У найпоширеніших приладах біометричної автентифікації успішно використовуються візерунки сітківки очей, геометрія руки та відбитки пальців. Всі ці методи ідентифікації є статичними.

Автентифікація по візерунках сітківки очей ефективна при виявленні спроб зловмисників видати себе за законного користувача. Рівень невизнання законних користувачів знаходиться в межах декількох відсотків при практично повній відсутності помилкової автентифікації.

У системах автентифікації за допомогою геометрії руки в результаті сканування отримують кілька силуетів руки за допомогою підсвічувальних діодів, а після цього будується тривимірне зображення. У системах такого типу висока можливість (10-75%) помилкової автентифікації.

Аутентифікація за відбитками пальців найпоширеніший метод біометричної ідентифікації, в основі якого лежить унікальність для кожної людини малюнка папілярних візерунків на пальцях. Зображення відбитка пальця, отримане за допомогою спеціального сканера, перетвориться в цифровий код (згортку) і порівнюється з раніше введеним шаблоном (еталоном) або набором шаблонів (у випадку ідентифікації).

2. Розробка мікропроцесорного пристрою автентифікації

Мікропроцесорний пристрій біометричної ідентифікації за відбитком пальця може використовуватись для реалізації різних технічних рішень. Цифрові елементи обробки сигналів у сканері відбитків пальців виконують функції цифрової обробки сигналів, таких як фільтрування, перетворення, виділення ознак, операції зіставлення (порівняння) та інші алгоритмічні функції (рисунок 2).

Рисунок 2 - Схема автентифікації за відбитками пальців

Структурна схема мікропроцесорного приладу автентифікації персони за біометричними даними наведена на рисунку 3. Основним елементом мікропроцесорної системи є васне сам процесор. Живлення може здійснюватися як від блоку живлення змінного струму, так і від порту USB 2.0. Для зручності експлуатації пристрою передбачене

під'єднання додаткової периферії, зокрема аудіо- підсилювача та сенсорного рідкокристалічного дисплею. У якості сенсора для зняття відбитків пальців використовється сканер AT77C105A фірми Atmel.

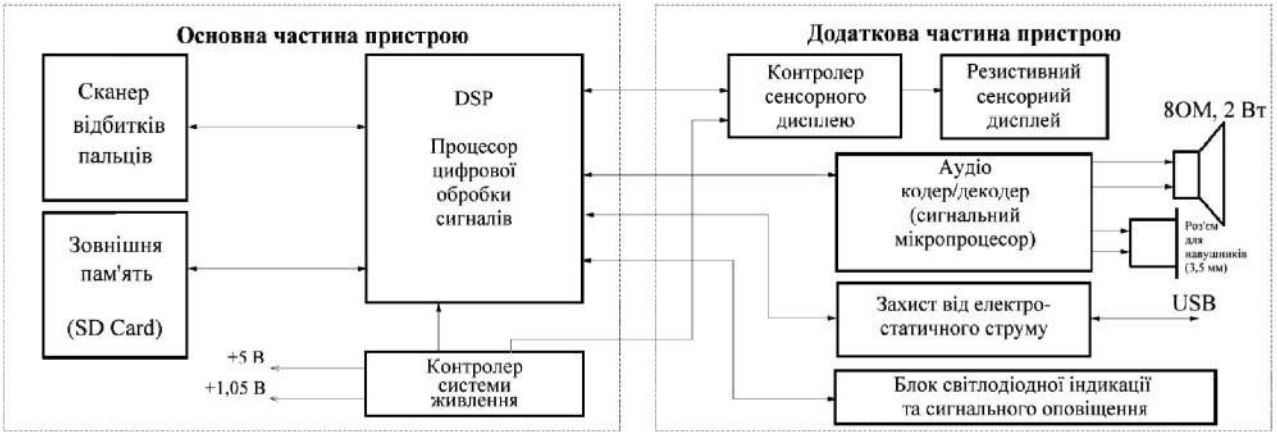


Рисунок 3 - Структурна схема мікропроцесорного пристрою автентифікації персони за біометричними даними

Розроблений мікропроцесорний пристрій ідентифікації персони за біометричними даними, а саме відбитками папілярних візерунків на пальцях має наступні технічні та естетичні характеристики, які роблять спроектований виріб конкурентоспроможним зразком на ринку, тобто: споживана потужність <= 5Вт,висока щвидкість обробки інформації, можливість додаткової периферії для зручності керування, можливість під'єднання до загального серверу, назька вартість пристрою.

Висновки.

Запропонований мікропроцесорний пристрій біометричної автентифікації персони за відбитком пальця на базі процесора цифрової обробки сигналів TMS320C5514 фірми Texas Instruments може використовуватись для реалізації різних технічних рішень, включаючи електронні дверні замки, системи запалювання двигунів внутрішнього згорання, USB флеш-накопичувачі з контролем доступу за відбитком пальця, та багато інших.

Перелік джерел.

1. Широчин В.П., Мухин В.Е., Кулик А.В. Вопрсы проектирования механизмов защиты информации в компьютерных системах и сетях. Киев., "ВЕК+", 2000. -122с.

2. Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. Политехника, 2001, 240с.

3. Сеньор Э.У. Руководство по биометрии / Э. У. Сеньор, Н. К. Ратха, Ш. Панканти, Дж. Х. Коннел, Р. М. Болл. – М.: Техносфера, 2007 г. - 368 стр.

УДК 681.32

Р.О. Люлькун

Тернопільський національний економічний університет

ОПТИМІЗАЦІЯ СИСТЕМИ ВИМІРЮВАННЯ ТА РЕЄСТРАЦІЇ ТЕЛЕМЕТРИЧНИХ ПОКАЗНИКІВ ЛЮДИНИ

Вступ. Проблема моніторингу здоров'я людини є дуже важливою проблемою сьогодення. У лікарнях є багато різного спеціального устаткування для такого контролю.Такі системи повинні забезпечити моніторинг загального стану і здоров'я людини, бути компактними, мобільними та не дорогими, здійснювати моніторинг стану людини в реальному часі.

Пристрої для вимірювання температури тіла є одними з найстаріших діагностичних пристроїв та дають лікарю важливу інформацію про фізіологічний стан пацієнта. Визначення тиску крові пацієнта є стандартним клінічним вимірюванням, що здійснюється, як в амбулаторних умовах, так і в умовах стаціонару. Знання артеріального тиску пацієнта допомагає лікарю оцінити стан серцево-судинної системи хворого. Задача оптимізації системи вимірювання телеметричних показників є актуальною через надзвичайну важливість таких параметрів організму, як температура та артеріальний тиск.

Метою роботи є дослідження методів та засобів вимірювання температури та тиску та проектування комп'ютерно-інтегрованої системи для вимірювання телеметричних даних людини.

1. Досідження методів та засобів вимірювання телеметричних показників

У випадках коли температуру не потрібно реєструвати безперервно, стандартним засобом вимірювання залишається ртутний термометр. Проте у випадках, коли необхідно забезпечити безперервний моніторинг за температурою пацієнта, вимірювальний пристрій не повинен створювати дискомфорту. Тому електронні термометри часто замінюють ртутні. Ці пристрої, що мають зручні для використання датчики, дозволяють отримати відлік температури значно швидше, а самі показання зчитувати значно зручніше, ніж на звичайному термометрі. Для вимірювання температури можна використовувати термопари, оптоволоконні термодатчики, напівпровідникові датчики температури та ін.[1-3].

Знання артеріального тиску пацієнта допомагає лікарю оцінити стан серцево-судинної системи хворого. Для визначення тиску у людини використовуються різні прямі (інвазивні) та непрямі (неінвазивні) методи вимірювання. Для кожного з методів повинні бути оцінені ступінь його придатності в даній клінічній ситуації і точність вимірювання.

У переважній більшості випадків індикація тиску здійснюється за допомогою деформації пружних тіл, наприклад діафрагми, трубки Прудона чи гофрованої мембрани датчика. На даний час у якості датчиків тиску широкого використання набули тензометри. Особливо перспективними є напівпровідникові тензометри дифузійного типу. Дифузійні тензометри на кремнієвій підкладці володіють високою чутливістю, малими габаритами та мають можливість легкого інтегрування з необхідними периферійними пристроями та схемами. Резистивний тензометричний датчик це основа із закріпленим на ній резистивним елементом, що під дією сили змінює свої розміри (стискається чи розтягується) [4-5].

2. Проектування комп'ютерно-інтегрованої системи контролю телеметричних показників

Запропонована мобільна система, яка призначена для контролю за станом здоров'я людини в режимі реального часу (рисунок 1).

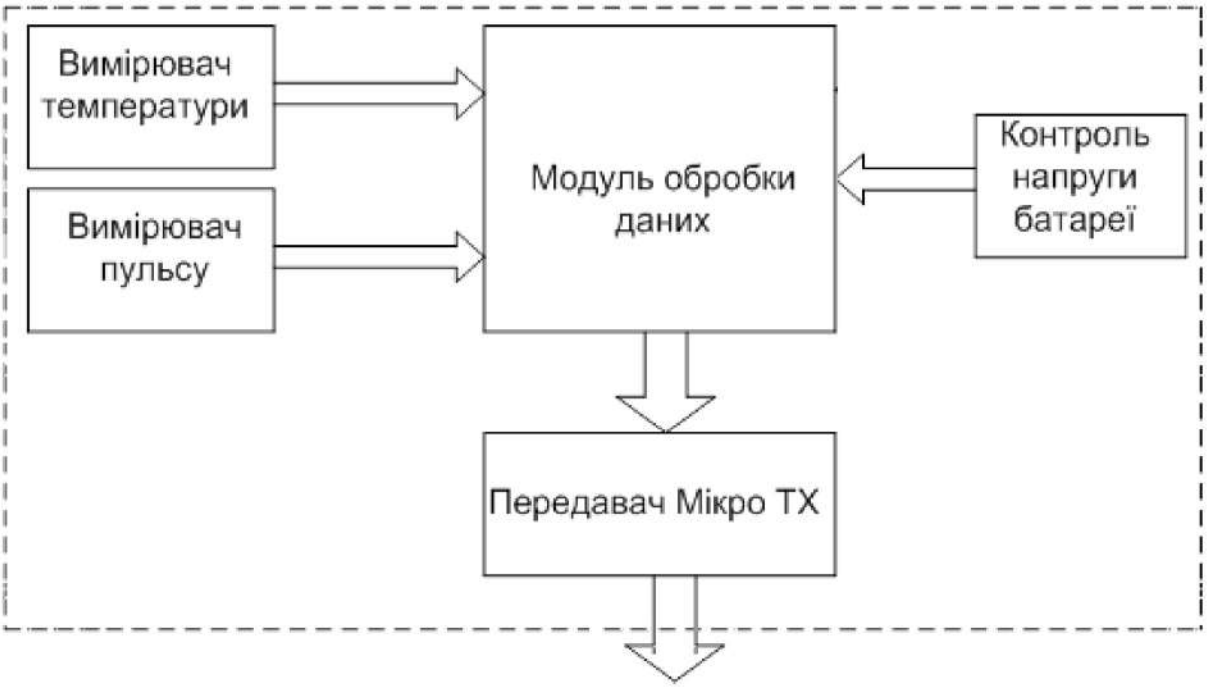


Рисунок 1 - Схема комп'ютерно-інтегрованої системи контролю телеметричних показників людини

Отримані датчиками телеметричні дані (температура, пульс) передаються на приймач через радіо канал АМ, побудований на устаткуванні Low Power Radio Solutions Ltd. - Мікро Tx модуль передавач і модуль приймач AM2000 [6]. У цьому каналі використовується пакетна передача даних з перевіркою цілісності пакету. Для мінімізації рівня помилок під час передачі пакетів використовується Манчестерське кодування.

У приймача є три основні завдання:

– отримання телеметричних даних від датчиків;

– перетворення аналогового голосового сигналу який поступає на мікрофон в цифрову форму;

– передача даних.

У всіх радіо-каналів є здатність автоматичної пересинхронізації у разі втрати сигналу.

На рисунку 2 зображено функціональну схему комп'ютерно-інтегрованої системи контролю телеметричних показників людини

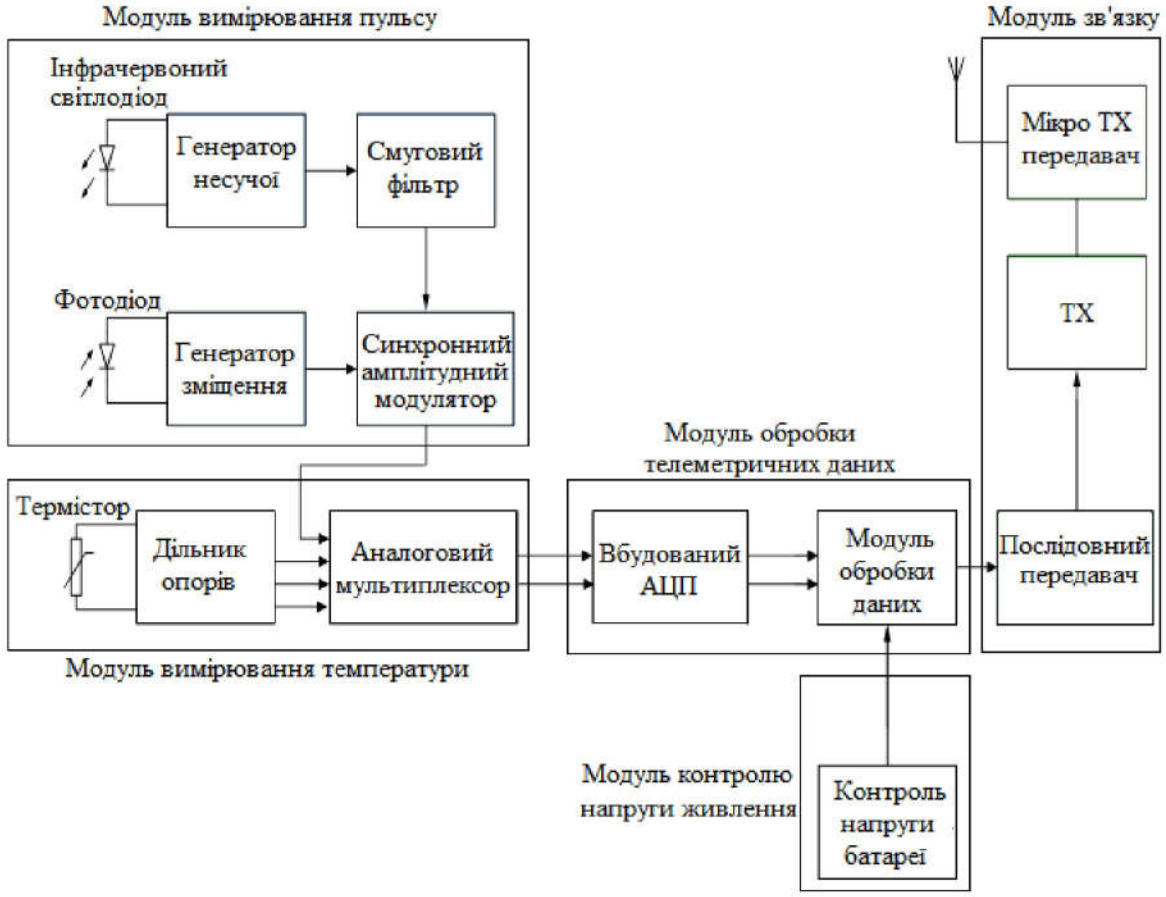


Рисунок 2 – Функціональна схема комп'ютерно-інтегрованої системи контролю телеметричних показників людини

Згідно наведеної функціональній схеми комп'ютерно-інтегрована система контролю телеметричних показників людини складається з наступних модулів:

– модуль вимірювання температури;

– модуль вимірювання пульсу;

– модуль контролю напруги батареї живлення і розміщення пристрою;

– модуль обробки даних;

– модуль комунікації.

В якості датчика температури вимірювальний модуль використовує дільник опорів, побудований на прецизійному резисторі і термісторі. Сигнал напруги через аналоговий мультиплексор послідовно подається до аналого-цифрового перетворювача. Отримані цифрові значення також опрацьовуються телеметричним модулем обробки даних і використовуються для наступних обрахунків на приймаючому модулі.

Модуль управління напруги батареї дає інформацію про загальний стан пристрою. Всі телеметричні дані, включаючи інформацію стану пристрою використовуються для упаковки пакетів що будуть відсилатись. Готові пакети даних відсилаються послідовним передавачем через модуль ТХ і мікропередавач ТХ.

Висновки.

Запропонована комп'ютерно-інтегрована система для контролю телеметричних даних людини, що дозволяє здійснювати реєстрацію та контроль необхідних показників у реальному часі.

Перелік джерел.

1. Джон Г.Вебстер Медицинские приборы. Разработка и применение.–М.: Медторг, 2004, –620 с.

2. Козявкін В.І., Маргосюк І.П., Гордієвич С.М., Качмар О.О. Системи моніторингу в медичній реабілітації / Основи медико-соціальної реабілітації дітей з органічними ураженнями нервової системи. — К.: Інтермед, 2005. — С. 183-185.

3. Стеценко Г.С., Пенішкевич Я.І та інш. Медична техніка. -Луцьк: Надстир'я, 2002, -320 с.

4. Метрологія та вимірювальна техніка /Поліщук Є.С., Дорожовець М.М., Яцук В.О. та ін.: Підручник – Львів: Бескид Біт, 2003. – 544 с.

5. Туяхов А.І. Практична метрологія і виміри. Навчальний посібник – Севастополь: «Вебер», 2003. – 288 с.

6. Когутяк, М. І. Технічні засоби автоматизації : навч. посіб. / М. І. Когутяк. - Івано-Франківськ : ІФНТУНГ Факел, 2008. - 212 с.

УДК 681.32

І.Б. Албанський, І.І. Ясінчук

Тернопільський національний економічний університет

ІНТЕГРОВАНІ СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ НА ОБ'ЄКТИ ЗАКРИТОГО ТИПУ

Вступ. Контроль доступу - одна із складових частин комплексного поняття, процесу забезпечення безпеки підприємства. Системи контролю і управління доступом (СКУД) сьогодні невід'ємна частина інтегрованих систем безпеки. СКУД дозволяє обмежити, регламентувати, впорядкувати контроль доступу в різні приміщення, при цьому фіксуючи інформацію про переміщення для подальшого її використання. Застосування систем контролю доступу дозволяє фіксувати як загальна кількість людей, що знаходяться на об'єкті, так і місцезнаходження кожного з них, дозволяє вести табельний облік співробітників.

Сучасні мережеві системи контролю доступу (СКД) по своїх можливостях можуть забезпечити необхідний рівень охорони на великих об'єктах, що містять тисячі точок доступу і десятки тисяч користувачів. Крім цього, системи служать основою для побудови інтегрованих систем безпеки, які об'єднують охоронну та пожежну сигналізацію, засоби телевізійного контролю.

Системою контролю та управління доступом (СКУД) і системою контролю доступу (СКД) називається сукупність програмно-технічних засобів і організаційно-методичних заходів, за допомогою яких вирішується завдання контролю і управління відвідуванням окремих приміщень, а також оперативний контроль переміщення персоналу і часу його перебування на території об'єкта.

Метою роботи є аналіз систем контролю та управління доступом та розробка методу виявлення загроз СКУД.

1. Аналіз систем контролю та управління доступом за їх функціональним призначенням

Впровадження СКУД дозволяє забезпечити безпеку і контроль об'єктів без залучення великої кількості працівників охорони і стабільну роботу автоматизованих систем в режимі 24/7 (наприклад, банкоматів, які встановлені в окремих приміщеннях відділень).

Засоби контролю доступу класифікують [1]:

- керовані перегороджуючі пристрої (в складі перегороджують конструкцій і виконавчих пристроїв СКД);

- пристрої введення ідентифікаційних ознак (в складі зчитувачів і ідентифікаторів);

- пристрої управління (у складі апаратних і програмних засобів контролю доступу).

За ступенем складності побудови системи, їх можна розділити на наступні види: автономна та мережева СКУД.

Автономні СКУД призначені для управління одним або декількома загороджувальними пристроями без передачі інформації на центральний пульт і без контролю з боку оператора[2, 3].

Зазвичай це найпростіші СКУД що складаються з автономного контролера, зчитувача і замикаючого пристрою, для відкриття останнього зсередини приміщення, зазвичай використовується або кнопка, або сенсор–комутатор руху. Якщо система повинна керувати доступом не в одне–два приміщення, а в кілька десятків, то вона будується за мережевим принципом.

Мережеві СКУД призначені для забезпечення контролю і управління доступом на великих об'єктах (банки, установи, підприємства і т. п.) для управління декількома пунктами проходу (прохідні, офісні приміщення). Взаємодіє з пропускними конструкціями, обмін інформацією здійснює з центральним пультом. Оператор може оперативно управляти системними пристроями – дистанційно заблокувати замки або їх відкрити (наприклад, у разі пожежі).

Мережева СКУД являє собою сукупність об'єднаних автономних систем. В ній всі контролери управління мають спеціальні контакти для підключення зовнішнього інтерфейсу і об'єднані в одну локальну мережу.

Інтегрована СКУД, може бути частиною загальної системи охоронної і пожежної безпеки, яка об'єднує в собі комплекс технічних та програмних засобів із забезпечення безпеки підприємства та його життєдіяльність.

2.Основні елементи і технічні пристрої СКУД

Залежно від сфери застосування в систему можуть входити різні компоненти обладнання. Система в загальному випадку складається з наступних елементів, які можна розділити на категорії [3]:

1.Технічні засоби:

- Стаціонарне обладнання, таке як сервер, станція оператора і т. д.

- Керуючий пристрій – контролер.

Один з найголовніших пристроїв системи. Безпосередньо саме цей пристрій приймає рішення про пропуск або заборону доступу на об'єкт, що охороняється, шляхом безпосереднього управління запираючими пристроями.

В енергонезалежній пам'яті зберігає базу ідентифікаторів доступу, права доступу, події надання або відмови в доступі.

- Замикаючі пристрої. До них відносяться турнікети, дверні замки, засувки, шлюзові кабіни, шлагбауми, суцільні двері.

- Зчитувальний пристрій, призначений для зчитування даних з ідентифікаторів доступу і відправляють їх на контролер.

- Ідентифікатори доступу, це магнітні, штрих–кодові карти, радіобрилки, біометричні дані людини (малюнок сітківка ока, геометрія долоні, відбиток пальця), проксіміті карти і т. д.

- Блоки живлення, забезпечують живлення елементам системи.

- Пристрої сповіщення про тривожні ситуації, такі як в злом дверей, несанкціонований прохід і т.д.

2. Програмне забезпечення:

- адміністрування системи, можливість віддаленого управління доступом;

- моніторинг в реальному часі;

- облік робочого часу.

Основою будь-якої системи є блоки концентраторів з підключеними зчитувачами ідентифікаційних ключів, охоронними сенсорами і електромеханічними запірними пристроями, наприклад, замками, шлагбаумами, турнікетами і т.д. (рисунок 1).

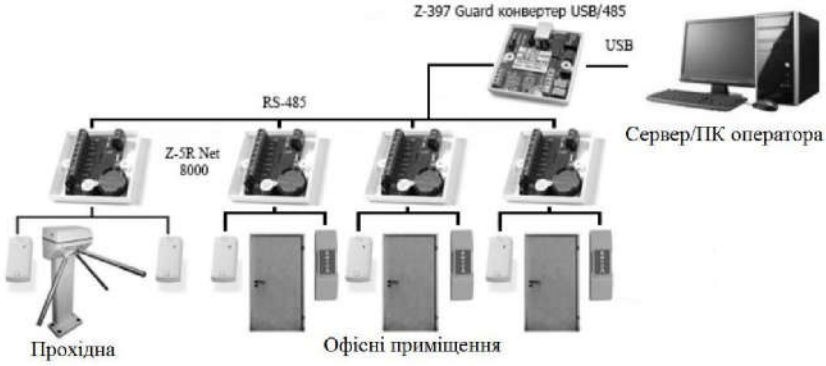


Рисунок 1 – Основні елементи СКУД

Контролер - це основна частина системи управління доступом. Саме контролер приймає рішення, пропустити чи ні людини в ті чи інші двері. Контролери виконавчих пристроїв СКУД - складні електронні прилади, які можуть бути реалізовані у вигляді окремих блоків або вбудовані в корпус відповідного виконавчого пристрою. Контролер зберігає у своїй пам'яті коди ідентифікаторів зі списком прав доступу кожного.

Структурна схема включення контролера представлена на рисунку 2. Контролери об'єднуються в мережу з використанням інтерфейсу RS–485 і працюють під управлінням комп'ютера. Спеціалізоване ПЗ, дозволяє програмувати контролери, управляти їх роботою, завантажувати події, реєструвати користувачів в системі, виробляти віддалене управління відкриттям дверей і турнікета. Кожен контролер працює автономно, приймаючи рішення про наданні доступу по картці / ключу незалежно від того, підключений він до ПК чи ні. Контролери з'єднаються між собою послідовно один за друг. Номер контролера в мережі виставляється спеціалізованим ПЗ. Спочатку всі контролери мають мережеву адресу 1. При установці необхідно призначити нові мережеві адреси контролерам. Максимум в мережі може бути 255 контролерів такого типу [4].

В структурі рисунка 2 під номером 1 вказано типове джерело живлення ИБПС–12–1, із входом 220В і виходом 12В, в герметичному виконанні, 2 зображений зчитувач Matrix II, 3 вказано електромагнітний замок YM–180. Підключення контролера Z–5R net можливо також і до електромеханічних замків. Під номером 4 показаний сенсор відкриття дверей, контролер не включить замок, поки доводчик закривання дверей не притисне її до косяка. Номером 5 позначена вихідна кнопка, що встановлюється всередині приміщення.

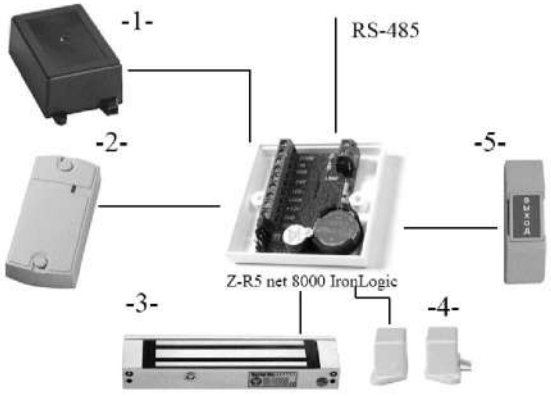


Рисунок 2 – Схема підключення контролера до основних елементів системи

Зчитувач (рідер) - це пристрій, призначений для зчитування спеціальної кодової інформації, що зберігається в ідентифікатор, і її передачі у вигляді заздалегідь визначеного сигналу в контролер.

Залежно від принципів роботи ідентифікатора змінюється і технологія зчитування коду. Зчитувач повинен бути відділений від контролера, щоб зовні ланцюга, за якими можливо відкривання замка, були недоступні. Найбільш вандалостійкими є зчитувачі безконтактних карт. В якості засобів доступу (ідентифікатора особистості) можуть бути застосовані будь-які контактні або безконтактні карти, електронні ключі або навіть сигнал від відеокамери, яка, визначивши номер автомашини, подасть команду на відкривання шлагбаума. В системі контролю і управління доступом стан контрольованих зон, події і звіти можуть відображатися в реальному масштабі часу на екрані комп'ютера.

3. Метод виявлення загроз СКУД

СКУД володіють великою кількістю недоліків і критичних вразливостей, що загрожують безпеки підприємства, яке вона призначена охороняти. Під порушенням безпеки мається на увазі як несанкціоноване проникнення на територію об'єкта, що охороняється, так і несанкціонований доступ до корпоративної мережі об'єкта, що, в свою чергу, призводить до витоку персональної інформації, комерційної таємниці, розкрадання матеріальних цінностей, диверсіям на території об'єкта, а також безпосередньо до загрози життю і здоров'ю людей. Тому для досягнення максимального рівня захисту системи необхідно звернути пильну увагу на кожну потенційну вразливість.

Вразливість (об'єкта) – це ступінь невідповідності вжитих заходів щодо захисту об'єкта прогнозованим загрозам або заданим вимогам безпеки[6].

Вразливості можна розділити на наступні групи [4]:

- фізичні вразливості апаратури;
- вразливості мережі СКУД;
- поведінкові вразливості.

Рішення задачі виявлення загроз поділяється на кілька етапів. На першому етапі збирають і оптимізують дані: збір даних системою КУД, їх фільтрація і агрегування. На етапі збору даних СКУД реєструє всі події, що надходять від контролерів системи, і інциденти від сенсорів контролю.

Отримані набори даних не піддаються аналізу без попередньої їх обробки, тому вони надходять на етап фільтрації, де зайві і некоректні дані відсіваються. Дані, отримані від СКУД і минулі етапи фільтрації, надходять на етап агрегування і приймають формат атрибутів (таблиця 1).

Таблиця 1 – Вхідні дані системи виявлення загроз

Атрибут	Опис
X1={0|1|X}	Ознака робочого часу
X2={0|1|X}	Перше відвідування об'єкта
X3={0:n|X}	Рівень доступу карти
X4={0:n|X}	Рівень доступу об'єкта
X5={0|1|X}	Спроба доступу до забороненого об'єкта
X6={0:n|X;Obj;L}	Кількість спроб доступу; об'єкт; рівень доступу об'єкта
X7={0|1|X;Obj;L}	Ознака відмови обладнання; об'єкт; рівень доступу об'єкта
X8={0:n|X}	Множинний вхід в різні об'єкти без виходу
X9={0|1|X;Obj;L}	Відключення електроживлення; об'єкт; рівень доступу об'єкта
X10={0|1|X;Obj;L}	Відкриття дверей, без події проходу; об'єкт; рівень доступу об'єкта
X11={0|1|X;Obj;L}	Не замкнені двері; об'єкт; рівень доступу об'єкта
X12={0|1|X}	Доступ всередині об'єкту, що охороняється, без проходу на територію підприємства

Примітка: 0 – критерій не встановлений; 1 – критерій встановлений; X – критерій не визначено; 0:n – цілочисельне значення; Obj – об'єкт, під ним розуміється охороняється приміщення або вся будівля об'єкту, що охороняється в цілому; L – рівень доступу об'єкта.

На другому етапі вибирають методи для вирішення завдання. На виході підсистеми виявлення загроз, очікується визначити клас загрози, а також в якості необов'язкових параметрів джерело загрози і сектор, в якому виявлено загрозу. Приблизний формат вихідних даних представлений на рисунку3.

$$Y = \begin{Bmatrix} [l_x(\text{ Джерело загрози }),][S_x(\text{ Сектор }),] \\ \{Y_0(\text{Нема загрози}) \mid Y_1(\text{ Незначна загроза }) \mid Y_2(\text{ Критична загроза }) \mid Y_n\} \end{Bmatrix}$$

Рисунок 3 – Формат вихідних даних

Таким чином, поставлено завдання виявлення загроз, яка буде вирішуватися методами машинного навчання (МН). Процес МН вимагає достатньої кількості даних, що відповідають як нормальному режиму роботи системи, так і аномальних ситуацій. Тому МН здійснюється на змодельованих наборах даних за участю експерта.

Існує кілька основних алгоритмів для побудови і навчання моделей класифікаторів, застосовних для вирішення завдання виявлення загроз [5]. Найбільш широкого розповсюдження знайшли методи:

- метод k–найближчих сусідів(nearest neighbour);
- метод опорних векторів (Support vector machines, SVM);

- метод, що базується на динамічних байесовских мереж;
- метод, що базується на основі нейронних мереж.

Розглянувши основні методи вирішення поставленого завдання, прийнято рішення реалізувати механізм виявлення загрози застосовуючи метод випадкових лісів [6]. Математична модель являє собою ансамбль бінарних дерев рішень, побудованих на навчальній бутстреп вибірці по усіченому набору параметрів. Алгоритм роботи математичної моделі представлений на рисунку 4.

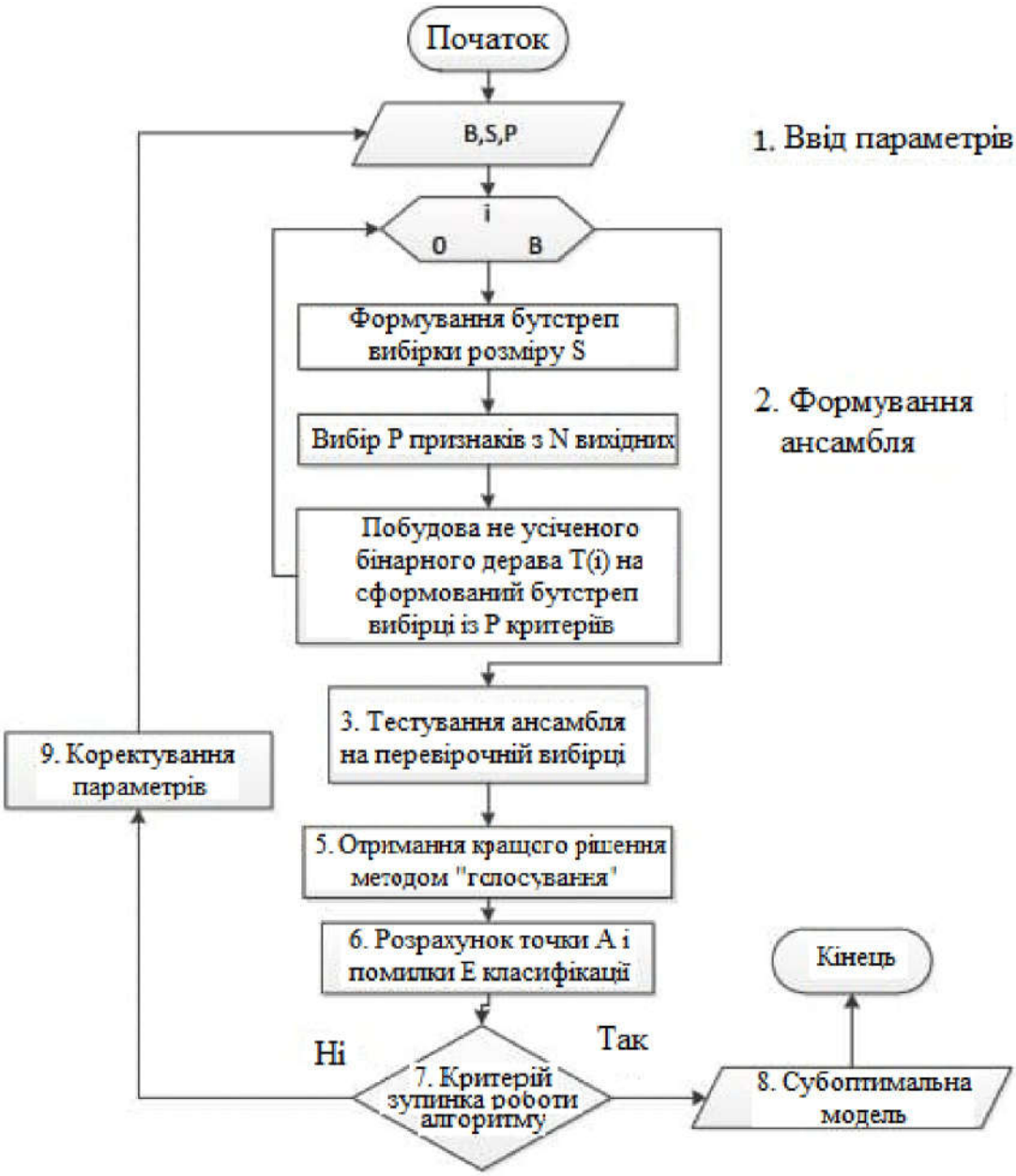


Рисунок 4 - Алгоритм роботи математичної моделі запропонованого методу

Метод побудови бутстреп вибірки полягає в наступному. Нехай є вибірка X розміру N. Рівномірно з вибірки береться M об'єктів з

поверненням. Це означає, що з усіх вихідних N об'єктів вибірки M раз вибирається довільний об'єкт (вважається, що кожен об'єкт вибирається з однаковою ймовірністю 1/N). В результаті вибірки серед об'єктів можуть виявитися повтори. Нова вибірка позначається X1. Повторюючи процедуру H разів, згенерується H підвибірок X1 , ... , XH. Усічений набір параметрів може бути отриманий так: з набору K вихідних критеріїв розмірністю N вибирається P критеріїв. Повторюючи процедуру H раз, згенерується H під наборів K1, ..., KH.

На підставі отриманих вибірок і піднаборів критеріїв будується ансамбль з H двійкові не рубаних дерев рішень. В результаті аналізу всіх побудованих дерев рішень методом голосування визначається потенційна загроза. Метод голосування полягає в тому, що в якості остаточного рішення приймається значення,найчастіше зустрічається в ансамблі дерев.

На третьому етапі тестування отриманої на другому етапі моделі (перевірка придатності модель).

Висновки.

В статті проаналізовано складові системи контролю та управління доступом, а також типи побудови СКУД. Запропоновано фізичну модель реалізації системи. Дано визначення загроз безпеці. Розглянуто задачу виявлення загроз в система. Розглянуто основні методи застосовувані для вирішення поставленого завдання. Описано метод випадкових лісів, який планується застосувати для вирішення поставленої завдання.

Перелік джерел.

1. Ворона В. А. Система контроля и управления доступов / В. А. Ворона, В. А. Тихонов. – М.: Горячая линия – Телеком, 2010. – 272с.

2. Рыжова В. А. Проектирование и исследование комплексных систем безопасности //СПб: НИУ ИТМО. – 2012.

3. Юрьев Н. Н. Система контроля и управления доступом / Н. Н. Юрьев, Т. А. Васяева, С. Д. Бельков, Н. С. Суббота // Информатика, управляющие системы, математическое и компьютерное моделирование. – 2017. – № 7. – С. 601–604.

4. Волхонский В.В. Основные положения концепции обеспечения безопасности объектов // Научнотехнический вестник СПбГУ ИТМО. – 2011. – № 3(73). – С. 116–121.

5. Носков А.Н., Чечулин А.А., Тарасова Д.А. Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных // Труды СПИИРАН. 2014. Вып. 37. С. 208–224.

6. Информатика, управляющие системы, математическое и компьютерное моделирование (ИУСМКМ – 2018) / Материалы IX международной научно–технической конференции – Донецк: ДонНТУ, 2018г. – с. 126–129.

УДК 681.3

О.М. Заставний, С.І. Прийма

Тернопільський національний економічний університет

ЗАВАДОСТІЙКЕ КОДУВАННЯ В БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

Вступ. У сучасному високотехнологічному суспільстві сенсорні мережі широко впроваджуються у всі сфери людського життя. Це як системи моніторигу на різноманітних промислових об'єктах та і в різноманітних системах охоронних та пожежних сигналізацій і засобах інтернету речей. Часто такі сенсорні системи використовуються для збору інформації з засобів обліку енергоносіїв, моніторингу температури, вологості тощо. Тобто в більшості випадків дані сенсори передають періодично невеликі обсяги інформації з невеликою переріодичністю, що цілком логічно приводить до вимог тривалої автономної роботи а також надійного передавання інформації в умовах житлових приміщень та промислових об'єктів, а тому дослідження методів та засобів завадостійкого кодування в безпровідних сенсорних мережах є актуальною науковою задачею.

Метою роботи є дослідження завадостійкого кодування у безпровідних сенсорних мережах.

1. Модулі сенсорних систем

Широкого поширення в IOT системах набули технології bluetooth, WiFi та різноманітні пропрієтарні системи радіозв'язку. На рисунку 1 представленні приклади засобів з використанням даних технологій.

а) б)

Рисунок 1 – Приклад сенсорних модулів: а – на базі bluetooth 4.0; б – на базі пропрієтарних радіомодулів

Оскільки важливою вимогою до таких систем є можливість роботи в умовах різноманітних завад та перешкод, тому що при низькій завадостійкості є потреба встановлення додаткових репітерів що ускладнює розгортання даних систем та не завжди є можливість їх встановлення.

2. Завадостійке кодування

Завадостійке кодування зокрема шумоподібні кодові послідовності(ШПК) широко використовуються в системах зв'язку таких як WiFi, Bluetooth, GSM, CDMA, GPS та інших. Рівень завадостійкості шумоподібних кодів залежить від довжини послідовності та часто вибирається як компроміс між довжиною коду і швидкодією, оскільки кожен інформаційний біт замінюється ШПК і відповідно зростає навантаження на канал зв'язку. Тому в системах зв'язку де потрібно висока швидкість передавання даних (WiFi, Bluetooth, GSM і т.д.) довжина ШКП обмежена і в якості ШКП використовуються коди Баркера, які мають найкращі кореляційні властивості, проте максимальна довжина кодів Баркера складає 13біт, що обмежує їх завадостійкість і відповідно не дозволяє ефективно працювати на великих відстанях при низькії потужності передавача.

Для сенсорних мереж часто немає потреби передавати великі обсяги даних, а тому можна збільшувати довжину коду та відповідно підняти завадостійкість та відстань передавання.

Проте існуючі ШКП, такі як М-послідовності, коди Голда, коди Кассамі мають нижчу завадостійкість на кількість біт послідовності порівняно з кодами Баркера, а в сеносорних мережах також є обмеження на потужність передавача, а також обмежена потужність джерела живлення вимагає використання максимально ефективних кодових послідовностей.

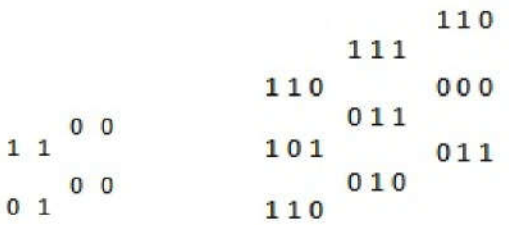
Перспективним є використання тримірних ШКП. Кореляційна яких обробка здійснюється згідно з виразом:

$$K_{(x,y,z)} = \sum_{i=1}^{m}\sum_{j=1}^{h}\sum_{u=n}^{1} F(x_{j,i,u}y_{j,i,u}) + \sum_{i=1}^{m}\sum_{j=h}^{1}\sum_{u=n}^{1} F(x_{j,i,u}y_{j,i,u}) + \sum_{i=1}^{m}\sum_{j=1}^{h}\sum_{u=1}^{n} F(x_{j,i,u}y_{j,i,u})$$

В якості функцій цифрової кореляції $K_{(x,y,z)}$ можуть бути ефективно використані кореляційні функції: знакова; релейна; коваріаційна;

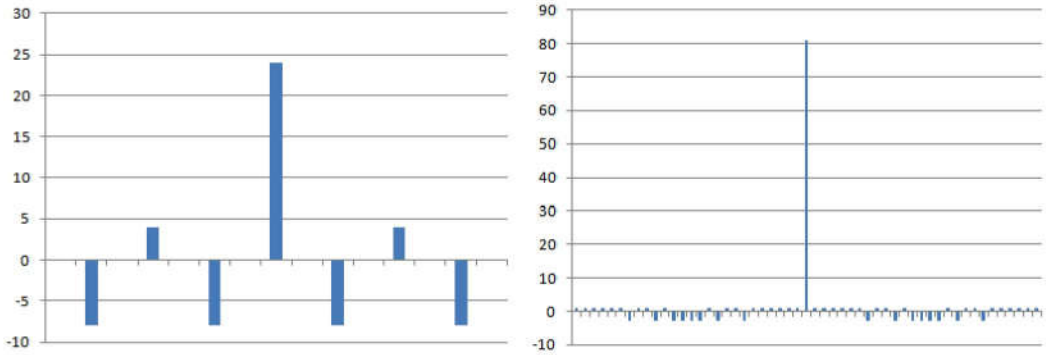
кореляційна; нормована кореляційна; структурна; модульна; еквівалентності.

На рисунку 2 наведені тримірні кодові послідовності та на рисунку 3 наведені їх кореляційні властивості.



а) б)

Рисунок 2 – Матриці тримірних кодів (а) – 2х2х2, б) – 3х3х3)



а) б)

Рисунок 3 - Графіки кореляційних властивостей тримірних кодів для матриць: а) - 2х2х2, б) – 3х3х3.

З даних рисунків видно, що зі зростанням розрядності тримірні ШКП маю доволі високу ефкнтивність по відношенні піку головної пелюстки до бокових.

Висновки.

Використання тримірних ШКП в сенсорних мережах дозволить півищити їх ефективність, зокрема підвищити дальність роботи та знизити витрати енергії на передавання інфомації.

Перелік джерел

1. Khurshid Aliev, Francesco Rugiano, Eros Pasero The Use of Bluetooth Low Energy Smart Sensor for Mobile Devices Yields an Efficient Level of Power Consumption / ALLSENSORS 2016 : The First International Conference on Advances in Sensors, Actuators, Metering and Sensing, 2016

Заставний О.М. Дослідження системних характеристик трьохмірних шумоподібних кодів з особливими кореляційними властивостями / Збірник матеріалів міжнародної координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, економіки, моделювання та управління» (ICSM-2014) – Тернопіль, 2014.-С.78-82.

УДК 004.056.57

А.О. Пеляк

Тернопільський національний економічний університет

ШТУЧНА ІМУННА СИСТЕМА ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМ

Вступ. Побудова штучної імунної системи для захисту інформації ґрунтується на базових принципах і механізмах біологічної імунної системи [1]. Це такі механізми як генерація і навчання різноманітних по своїй структурі детекторів, відбір небажаних детекторів, здатність детекторів до виявлення вірусів, клонування і мутація детекторів, формування імунної пам'яті.

Метою роботи є розробка алгоритмів інтелектуального пошуку шкідливих програм комп'ютерних системах на основі штучних імунних систем.

1. Побудова структури штучної імунної системи.

1. Генерація імунних детекторів. На цьому кроці відбувається створення детекторів певної конфігурації. Структура імунних детекторів може бути різноманітною. Наприклад, це можуть бути бінарні рядки фіксованої довжини, рядки різної довжини, що складаються з ASCII кодів і т.д. По аналогії з біологічними імунними системами, спочатку сформовані детектори не вміють класифікувати образи і коректно розпізнавати аномалії. Для набуття таких властивостей вони повинні пройти через етапи навчання і відбору.

2. Навчання детекторів. На цьому етапі відбувається набуття детекторами властивостей коректно класифікувати існуючі образи, а, отже, виконувати призначені імунологічні функції - виявлення вторгнень. Як правило, для навчання імунних детекторів, формуються навчальні вибірки, що містять об'єкти, що відносяться до різних класів. Навчені імунні детектори реагують на аномальні образи, і в той же час ігнорують «нормальні» образи. Також, як і зрілі лімфоцити біологічної імунної системи реагують на специфічний антиген, так штучні імунні детектори, що пройшли навчання, реагують на специфічні аномалії, наприклад, специфічні вторгнення. Такі імунні детектори циркулюють в системі, виконуючи задані функції. Проте не усі сформовані імунні детектори здатні до навчання і коректної класифікації. Такі детектори можуть

реагувати і на «чисті» файли і програми, генеруючи неправдиві сигнали. Для позбавлення від «неправильних» детекторів в штучній імунній системі існує механізм, що називається селекцією, або відбором, детекторів.

3. Відбір (селекція) імунних детекторів. Стадія відбору в штучній імунній системі запобігає появі в системі «небажаних» детекторів. Небажаними вважаються такі детектори, у функціонуванні яких є різні недоліки, наприклад, некоректна класифікація образів. Для виявлення недоліків в роботі імунних детекторів їх функціонування перевіряється на заздалегідь сформованій тестовій вибірці і аналізуються результати класифікації. Якщо імунний детектор відносить об'єкти чистого класу до шкідливого, він вважається небажаним і знищується. Завдяки механізму відбору, небажані детектори знищуються, а «виживають» тільки ті, які набули здатність до коректної класифікації.

4. Функціонування імунних детекторів. Детектори, що пройшли стадії навчання і відбору, «допускаються» до виконання призначених функцій, а саме, виявлення вторгнень. Кожен окремий детектор може бути розглянутий як деякий автономний агент, який сканує область вибраного простору пам'яті, перевіряючи файли комп'ютерної системи на приналежність їх до класу «чистих» об'єктів, або до класу шкідливих програм. Як правило, в комп'ютерній системі одночасно може знаходитися певна обмежена кількість імунних детекторів. Це обмеження безпосередньо пов'язане з ресурсами комп'ютерних систем - чим більше діючих імунних детекторів, тим більше системних ресурсів для функціонування вони вимагають.

5. Знищення імунних детекторів після закінчення часу. Існує ймовірність такого варіанту, коли імунний детектор тривалий час знаходиться в комп'ютерній системі, скануючи її об'єкти, проте не виявляє шкідливі програми, внаслідок того, що такого ймовірного комп'ютерного вірусу не існує, або в силу особливості структури детектора. Для того, щоб такий «даремний» детектор не витратив марно ресурси комп'ютерної системи він має бути знищений. Для знищення «слабких» імунних детекторів існує механізм, що називається «часом життя». Суть такого механізму полягає в тому, що при створенні, кожному детектору виділяється деякий обмежений час, впродовж якого він може знаходитися в комп'ютерній системі і виконувати задані функції. Після закінчення цього часу, якщо детектор не виявляє шкідливу програму, він знищується,

тим самим звільняючи місце для нового, ймовірно «сильнішого» детектора.

6. Виявлення шкідливих програм. На цьому етапі відбувається виявлення імунними детекторами шкідливих програм, що проникли в комп'ютерну систему. Цей етап характеризує перехід усієї штучної імунної системи в активний режим функціонування, оскільки саме вірус є «каталізатором» переходу штучної імунної системи в активний режим захисту.

7. Клонування імунних детекторів. При проникненні комп'ютерних вірусів в обчислювальну систему, існує висока ймовірність зараження великої кількості об'єктів цієї системи, наприклад виконуваних файлів. Для забезпечення швидкого виявлення усіх можливих заражених об'єктів, імунний детектор, що виявив в системі комп'ютерний вірус, піддається процесу самореплікації або клонуванню. В результаті клонування, створюється велика кількість однотипних імунних детекторів, що реагують на виявлений вірус, які за короткий проміжок часу перевіряють усі об'єкти комп'ютерної системи.

8. Мутація імунних детекторів. Процес мутації відбувається паралельно з процесом клонування і полягає у внесенні незначних змін до структури клонованих детекторів, дозволяючи імунним детекторам набути нових властивостей і адаптуватися до виявленого комп'ютерного вірусу. У результаті імунна система «вивчає» вірус, що проник в організм, і вчиться ефективніше з ним боротися, пристосовуючись до нього.

9. Формування імунної пам'яті. З числа детекторів вибирається найбільш пристосований імунний детектор і трансформується в детектор імунної пам'яті. Детектори імунної пам'яті зберігають інформацію про минулі інфекції і знаходяться в комп'ютерній системі досить тривалий час для організації своєчасної реакції на повторне зараження.

Висновки.

Таким чином, запропонована штучна імунна система для виявлення вторгнень, яка характеризується самоорганізацією в процесі функціонування, що дозволяє їй пристосовуватися до виявлення різних шкідливих програм, включаючи невідомих.

Перелік джерел.

1. Ройт, А. Иммунология / А. Ройт, Д. Бростофф, Д. Мейл. – М.: Мир, 2000. – 592 с.

Наукове видання

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2019)

Редактор коректор: Гуменний П.В.
Технічний редактор: Давлетова А.Я.

Підписано до друку 21.08.2019
Формат60х84/16. Піпір офсетний.
Друк офсетний. Замовлення №9-1517
Умов.-друк арк.17. Обл-вид. арк. 15.5
Тираж 30 прим.

Віддруковано ФОП ШПАК В.Б.
Свідоцтво про державну реєстрацію В02 № 924434 від 11.12. 2006
Свідоцтво платника податку: Серія Е № 897220
М. Тернопіль, вул. Просвіти 6
Тел.80972993899, 422-388
Email: tooums@ukr.net