УДК 528.4

І.В. Корнієнко

*Чернігівський національний технологічний університет, Чернігів*

# УПРАВЛІННЯ ЕФЕКТИВНІСТЮ АВТОМАТИЗОВАНОГО КАДАСТРОВОГО ОФІСУ

*Розглянуто проблему управління ефективністю автоматизованого кадастрового офісу. Визначені і проаналізовані механізми управління ефективністю та обґрунтована можливість управління ефективністю керуючим елементом відокремленого кадастрового офісу. Визначені напрямки підвищення ефективності автоматизованої кадастрової системи.*

***Ключові слова:*** *керування, ефективність, кадастр, автоматизована система.*

## Вступ

**Постановка проблеми.** Ефективність функціонування автоматизованих кадастрових систем (АКС) є нагальною проблемою розвитку національної економіки, відкритості та прозорості використання природних ресурсів, ефективності та інтенсивності бізнес процесів у державі. Незважаючи на суттєві зрушення у питанні автоматизації кадастрових систем досі невирішена проблема оцінки та управління їх функціональною ефективністю, через що спостерігається їх певна функціональна недосконаліть, неузгодженість (а то і відсутність інформаційної взаємодії між галузевими кадастровим організаціями), обмеженість автоматизації бізнес процесів та ефективного використання кадастрової інформації як в цілях управління об'єктами кадастрового обліку, так і в цілях продажу цієї інформації зацікавленим користувачам. З цих міркувань доцільним є проблематика створення функціонально-ефективних автоматизованих кадастрових комплексів та управління цією ефективністю.

**Аналіз останніх досліджень і публікацій.** Фундаментальним дослідженням створення та застосування АКС земельного кадастру в Україні присвячені роботи Лихогруда М.Г., питання формування вимог до АКС, їх створення, впровадження та розвиток досліджували Барладин А.В., Гавриленко Ю.Н., Даниленко А.С., Калюжный Н.Н., Кулініч В.В., Леонець В.О., Лященко А.А., Миколенко Л.І., Могильний С.Г., Муховіков А.М., Новаковський Л.Я., Сигитова та інші. Проблемам розвитку кадастрових систем регіону також присвячено багато робіт, зокрема [1, 2].

**Виділення невирішених раніше частин загальної проблеми.** Незважаючи на суттєву кількість наукових публікацій і досліджень, присвячених питанням створення та застосування автоматизованих систем для цілей кадастрового обліку, недостатньо висвітленим і розробленим залишається питання оцінки і управління ефективністю функціонування автоматизованих кадастрових офісів (АКО).

**Мета статті.** Розгляд проблеми управління ефективністю функціонування автоматизованого кадастрового офісу.

## Виклад основного матеріалу

В [3] досліджується проблема кількісної оцінки ефективності функціонування АКО, де оцінкою є успішність обслуговування вхідних заявок (виконання задач) представленої статистичним показником імовірності успішного обслуговування довільної заявки (виконання задачі) користувача системи

$$\Phi = P\left(\tau \le T^{доп}, q \ge Q^{доп}\right), \qquad (1)$$

де $\tau$ – випадковий час обслуговування довільної заявки; $q$ – випадкова якість обслуговування довільної заявки; $T_n^{доп}$, $Q_n^{доп}$ – допустимі значення часу та якості обслуговування.

Задача, що виникає для АКС, є характерною і для інших автоматизованих систем, наприклад [4], і може бути представлена у стандартній постановці, як здача постійного підтримання функціональної ефективності АКО на рівні не нижче заданого

$$\Phi(t) \ge \Phi^{доп},\ 0 \le t \le \infty. \qquad (2)$$

Конкретизуючи (2) з урахуванням (1) задача по управлінню ефективністю АКО може бути представлена у вигляді

$$\Phi = P\left(q \ge Q^{доп}\right) P\left(\tau \le T^{доп} / q \ge Q^{доп}\right), \qquad (3)$$

тобто задача ефективного управління ефективністю АКО розкладається на дві:

1. Успішне обслуговування вхідної заявки з імовірністю не менше заданої.

2. Підтримка на рівні не менше заданого умовної імовірності своєчасного обслуговування вхідної заявки з якістю не менше заданої.

Звідси видно, що ці дві задачі тісно пов'язані між собою, оскільки підвищення якості обслуговування може знижувати часові показники обслуговування (оперативність), і навпаки, прискорення обслуговування може вплинути на якість виконання задачі. Зважуючи ці задачі неважко бачити, що найважливішим частковим показником ефективності системи безумовно є якість функціонування АКО. Представимо процес обслуговування заявок у вигляді функціональної схеми (рис. 1).

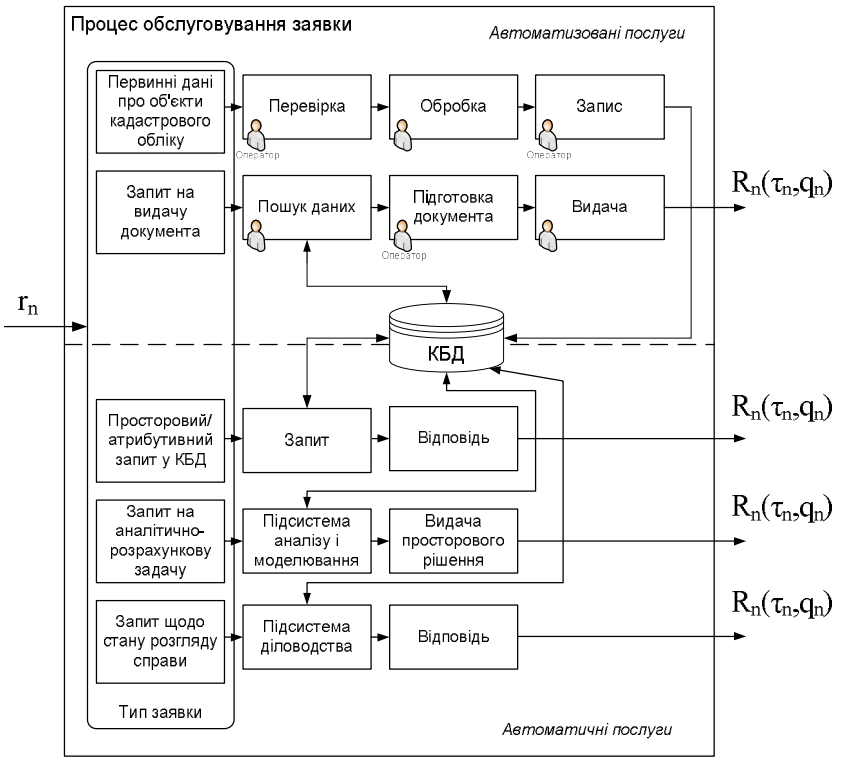


Рис. 1. Функціональна схема обробки вхідних заявок

На вхід АКО у випадковому порядку поступає множина заявок $r_n \in \Theta_r$, $n = \overline{1,N}$. Виходом АКО є множина обслугованих заявок (рішень) $R_n(\tau_n, q_n)$, кожна з яких, при оцінці ефективності, характеризується випадковим часом обслуговування $\tau_n$ та випадковою якістю обслуговування $q_n$. Вхідні заявки розрізняються за типом і способом надходження.

Зі схеми (рис. 1) видно, що відкидаючи апаратно-технічну складову (архітектура та технічні можливості ПЕОМ не є предметом розгляду даної статті), якість обслуговування заявки (або успішне рішення задачі) в геоінформаційних програмних комплексах (на платформі яких будуються автоматизовані кадастрові системи) в першу чергу визначається наявністю якісних просторових даних щодо об'єктів кадастрового обліку та алгоритмічно-методологічного апарату їх обробки. В свою чергу якість просторових даних визначається показниками точності позиціонування, повноти атрибутивного опису та актуальності даних про об'єкт кадастрового обліку, тобто залежить від якості роботи персоналу, що створює ці дані, перевіряє і вводить їх в кадастрову базу даних (КБД) та рівня функціональності програмного комплексу, якій має допомагати персоналу (контролювати та не допускати помилки) в обробці просторових даних. З цих міркувань можна записати основні складові, від яких залежить якість обслуговування вхідної заявки: функціональне наповнення програмного комплексу – $f$; рівень підтримки виробничого процесу засобами автоматизації – $p$; склад та можливості автоматизованих сервісів у наданні віддалених послуг – $s$; рівень підготовки та навченості персоналу – $l$, тобто задача (3) буде мати вигляд

$$\Phi = P\left(q\{f,p,s,l\} \geq Q^{\text{доп}}\right) \times$$

$$\times P\left(\tau \leq T^{\text{доп}} \,/\, q\{f,p,s,l\} \geq Q^{\text{доп}}\right),$$

де $q\{f,p,s,l\}$ якість обслуговування заявки, що визначається переліченими складовими $f,p,s,l$.

В такому представлені управління якістю функціонування АКО є багатокритеріальною задачею максимізації складових якості $f$, $p$, $s$, $l$, з обмежуючим чинником вартості витрат на подібну максимізацію $c_e$, який є обгрунтованим, поки спостерігається приріст дохідної частини від автоматизації кадастрової системи $c_p$.

Уникаючи багатокритеріальної задачі максиміна, де можна очікувати декілька екстремумів функції якості, доцільно зупинитися на рівні максимізації часткових показників якості, за якого $\max q \Leftrightarrow \max\left(c_p - c_e\right)$, що забезпечується методами математичного програмування.

Підсумовуючи розгляд задачі управління якістю обслуговування АКО можна зробити висновок, що управління якістю представляє собою скоріше задачу стратегічного ніж оперативного управління. Таке управління має здійснюватись централізовано АКО верхньої ланки по всій ієрархічній структурі системи одночасно (через функцію оновлень версій програмного забезпечення), або у вигляді експерименту під час тестування (досліджень) функціональних нововведень на окремому АКО. Тобто дворівнева система управління відокремленого АКО у питаннях управління якістю обслуговування заявки вироджується в однорівневу. Звідси справедливо вважати, що управління ефективністю функціонування окремого АКО (3) зводиться до задачі управління його оперативністю. Ця задача формулюється наступним чином. Маємо множину вхідних користувальницьких заявок, які надходять до АКО. Вимоги щодо оперативності їх обслуговування визначаються нерівністю

$$P_\tau = P\left(\tau \leq T^{\text{доп}} \,/\, q\{f,p,s,l\} \geq Q^{\text{доп}}\right) \geq P_\tau^{\text{доп}}, \quad (4)$$

де $P_\tau^{\text{доп}}$ – директивно визначене мінімально допустиме значення імовірності своєчасного обслуговування заявки. За допомогою функціональної схеми обробки заявок АКО (рис. 1) розглянемо чинники, що впливають на час обслуговування заявки.

Обслуговування всіх типів заявок здійснюється в автоматизованому або автоматичному режимах. Автоматизований режим характеризується участю операторів АКО в процесі обробки заявки. Вважатимемо, що рівень знань та навичок персоналу ідеальний, їх продуктивність постійна на протязі робочого дня, проте існує можливість допущення помилки (людський фактор). За цих умов швидкість обробки заявки при введенні первинних даних в кадастрову базу даних визначатиметься продуктивністю апаратно-програмного комплексу, ступенем автоматизації елементарних робіт на кожному етапі обробки даних (перевірка, обробка, запис), підтримкою програмним комплексом виробничого процесу та кількістю паралельних каналів обробки заявок.

Оперативність обслуговування заявки автоматичного режима визначається продуктивністю апаратно-програмного комплексу, складністю запиту, вибору методів аналізу та обробки просторових даних, інтенсивності потоку надходження заявок.

Такий розгляд дозволяє сформулювати основні чинники, що впливають на оперативність обробки потока заявок АКО: продуктивність апаратно-програмної платформи – $m$; ступінь автоматизації елементарних робіт – $a$; продуктивність і ефективність використовуваних алгоритмів аналізу і обробки просторової інформації – $e$; підготовленість первинних даних в заявках для введення їх в кадастрову базу даних – $d$; кількість паралельних каналів обробки вхідних заявок – $c$. Питання продуктивності $m$ апаратного-програмного комплексу далі розглядатися не будуть, так як це не є предметом дослідження статті, тільки відмітимо, що вирішення питання полягає у нарощувані продуктивності ПЕОМ, використанні алгоритмів паралельних обчислень, перерозподілу обчислювальних ресурсів тощо.

Перелік використовуваних алгоритмів аналізу і обробки просторових даних $e$ визначається користувачем і залежить від бажаного результату (рішення), відповідно справедливо вважати, що альтернативи цій операції немає. Рішенням цієї проблеми є підвищення продуктивності апаратно-програмної частини або введення пріоритетності обслуговування вхідних заявок по типу: «пріоритетний користувач» / «внутрішній користувач» / «зовнішній користувач» / «гість», що визначатиме важливість вхідних заявок.

Таким чином (4) прийме вигляд нерівності

$$P_\tau = P\left(\tau\{a,d,c\} \le T^{доп} / q\{f,p,s,l\} \ge Q^{доп}\right) \ge P_\tau^{доп}, \quad (5)$$

де $\tau\{a,d,c\}$ час обслуговування заявки, що визначається переліченими складовими $a,d,c$.

Таке представлення задачі управління своєчасністю обслуговування заявок також містить компоненту, що не залежить від дій керуючої ланки відокремленого АКО – це ступінь автоматизації елементарних робіт, що визначається функціональністю програмного комплексу. Тому, в інструментарії управління пропускною здатністю АКО залишаються можливість організації паралельних гілок обробки вхідних заявок та сприяння зменшенню помилок первинних даних. Щодо останнього, тут виявлені помилки (і, як свідчить досвід, переважним чином це помилки первинних даних просторового позиціонування об'єкта кадастрового обліку, що унеможливлює його топологічне укладання серед інших об'єктів даного класу в межах визначеного допуску), як правило, призводять до повернення заявки користувачу на доопрацювання, внаслідок чого, в кінцевому рахунку, збільшується інтенсивність вхідного потоку заявок. Отже, це підкреслює необхідність створення публічного сервісу, де можна одержати первинну кадастрову інформацію щодо об'єктів кадастрового обліку, яка не містить відомостей, заборонених до розголошення.

## Висновки і пропозиції

Розглянута проблема показала, що управління ефективністю відокремленого АКО є частковою проблемою управління ефективністю функціонування всієї автоматизованої кадастрової системи, яка, в свою чергу, в багатьом визначається функціональними можливостями програмного комплексу і ступенем автоматизації елементарних робіт. Разом з тим ступінь ефективності відокремленого АКО залежить також від доступності інформаційних ресурсів кадастрової бази даних для зовнішніх користувачів; з одного боку це забезпечує фінансові надходження за інформаційні послуги, з іншого боку зменшує вірогідність помилок первинних кадастрових даних.

## Список літератури

*1. O.Tereshchuk Current State of the National land cadastre in Ukraine: Problems and Prospects. (O.Pinchuk, O.Tereshchuk) // Scientific monograph - Some aspects of compulsory purchase of land for public purposes, Olsztyn, 2010, p.141-143.*

*2. Корнієнко І.В., Пантелєєва С.М. Актуальність застосування ГІС в управлінні земельними ресурсами [Електронний ресурс] / Матеріали X міжнародної НПК «Новітні досягнення геодезії, геоінформатики та землекористування – європейський досвід». – Чернігів: ЧДІЕУ, 2014. – С. 117-120. – Режим доступу: http://ibf.cn.ua/media/konferentsiya/zbirnyk-naukovyh-prats/2014-2/*

*3. Корнієнко І.В. Ефективність функціонування автоматизованої кадастрової системи / Вісник Чернігівського державного технологічного університету. Серія «Технічні науки та тахнології» : науковий збірник / Черніг. держ. технол. ун-т. − Чернігів : Черніг. держ. технол. ун-т., 2015. − №1 (1). − С. 94-98.*

*4. Кудрицький В.Д., Катков Ю.І., Корнієнко І.В. Оцінка і управління ефективністю функціонування автоматизованого командного пункту // Труди академії № 61. – К.: НАОУ, 2005. – С. 119 – 128.*

*Надійшла до редколегії 30.12.2014*

**Рецензент:** д-р техн. наук, доц. Д.П. Пашков, Екологічна академія післядипломної освіти, Київ.

**УПРАВЛЕНИЕ ЭФФЕКТИВНОСТЬЮ АВТОМАТИЗИРОВАННОГО КАДАСТРОВОГО ОФИСА**

И.В. Корниенко

*Рассмотрена проблема управления эффективностью автоматизированного кадастрового офиса. Определены и проанализированы механизмы управления эффективностью, обоснована возможность управления эффективностью управляющим элементом отдельного кадастрового офиса. Определены направления повышения эффективности автоматизированной кадастровой системы.*

***Ключевые слова:*** *управление, эффективность, кадастр, автоматизированная система.*

**PERFORMANCE MANAGEMENT AUTOMATED CADASTRAL OFFICE**

I.V. Korniyenko

*The problem of management efficiency of automated cadastral office. Identified and analyzed the mechanisms of performance management, the possibility of a performance management managing element separate cadastral office. The directions of increase of efficiency of an automated cadastre system.*

***Keywords:*** *management, efficiency, cadastr, automated system.*

---

UDC 681.3.06 (0.43)

O.G. Korol

*Simon Kuznets Kharkiv National University of Economics, Kharkiv*

# ENHANCED MAC ALGORITHM BASED ON THE USE OF MODULAR TRANSFORMATIONS

*The article considers the choice of cycle functions in the provable persistent key universal hashing scheme, proposed model and method of forming codes of integrity and authenticity of data on the basis of modular transformations, computational complexity reduce algorithm of the hashing schemes implementation using cyclic functions. The object of the research is the process of improving the integrity and authenticity of data packets in security protocols of telecommunication networks. The developed enhanced method of forming a cascade MAC differs from the known (algorithm UMAC) using modular hashing on the last stage of the MAC forming that provides high collision properties of strictly universal hashing and safety performance at the level of modern means of demonstrable strength protection.*

***Keywords:*** *codes of integrity and authenticity of data, a modular transformation, universal classes of hash functions.*

## Introduction

Studies have shown that the use of modular transformations allows realizing of provably resistant information hashing that satisfies the collisional properties of universal hash functions. Demonstrably safe level of strength is justified by reducing the problem of finding the source and / or the problem of recovering the secret key data to the solution of one of the well-known complexity-theoretic problems [1–3, 6].

At the same time, as shown by studies [1–3, 6], the universal hashing using modular transformations has a significant drawback - high computational complexity of the formation of the hash codes. In fact, for each information unit must perform a modular exponentiation that under transformation module appropriate orders significantly increases the time hashing information sequence. A promising direction in this regard is the development of multilayer universal hashing circuits using modular transformations on the last, the final stage of the hash code formation. This is as shown below, on the one hand provides a high collision properties of the resulting codes of integrity and authenticity of data generation circuit, on the other hand - provides high performance and provable strength level used transformations.

## Problem statement

The use of multilayer hash key circuits allows building of effective mechanisms for monitoring the integrity and authenticity of information in telecommunication systems and networks. However, the known multilayer structure (for example, the algorithm UMAC) together with the high speed and the cryptographic strength when applying a cryptographic transformation layer (using symmetric block cipher) lose universal hash properties, which leads to deterioration of the properties of the collision properties of generated message authentication codes. The purpose of the study is to develop a method of forming codes of integrity and authenticity of data based on provably resistant hash key that allows providing high levels of security and with applying certain restrictions on the modular transformations provide high collisional properties.

## Known methods

The analysis of [6–9] shows that the modular transformations are used today in the construction of keyless hash functions. Thus, in the fourth part of the international standard ISO/IEC 10118-4 defined two keyless hash function MASH-1 and MASH-2, which use modular arithmetic, namely the modular exponentiation to con-