УДК 331.211:519.86

Дунаєва Т.А.,
к.ф.-м.н., доцент
Проноза Т.О.
студентка групи УК-31м
Національний технічний університет України „КПІ”

МОДЕЛЮВАННЯ ПРОЦЕСУ ВИЯВЛЕННЯ ШАХРАЙСТВА З ПЛАСТИКОВИМИ КАРТКАМИ

Анотація

В даній статті, для виявлення шахрайських транзакцій пропонується використовувати сучасний метод карт Кохонена що самоорганізуються, який базується на теорії нейронних мереж і відноситься до алгоритмів навчання без учителя.

Summary

In this article, for the exposure of knavish transactions it is suggested to utillize the modern method cards of Kokhonena that self organization, which is based on the theory of neuron networks and behaves to the algorithms of studies without a teacher.

Ключові слова

Транзакція, нейронна мережа, карта Кохонена, профайл, моніторинг, процесинговий центр.

Вступ

На сьогоднішній день впровадження банківських пластикових карток є однією з найважливіших тенденцій розвитку технології безготівкових розрахунків у банківській діяльності. Подібний засіб розрахунків надає всім особам і організаціям, які його використовують, масу переваг. Для клієнтів це зручність, надійність, практичність, економія часу та відсутність необхідності мати при собі великі суми готівки. Для кредитних організацій – підвищення конкурентоспроможності й престижу, наявність гарантій платежу, зниження витрат на виготовлення, облік і обробку паперово-грошової маси, мінімальні тимчасові витрати й економія живої праці. Це лише неповний перелік позитивних якостей пластикових грошей, що обумовили їхнє визнання на світовому ринку.

Офіційної статистики про діяльність шахраїв в Україні на сьогоднішній день не існує. Якщо банки й проводять роботу з моніторингу шахрайських операцій, то інформація ця є строго конфіденційною. По неофіційним же

даним, збитки від діяльності карткових ловкачів в Україні становлять порядку 1% обсягу операцій з картами. Згідно ж вимог Visa і Europay, ця цифра не повинна перевищувати 0,14% [1].

Для ефективного виявлення підозрілих на шахрайство транзакцій з платіжними картками використовують автоматизовані системи моніторингу. Такі системи дозволяють банкам емітентам і екваєрам зміцнювати захист від шахрайства, знижувати ризики й втрати як самих банків, так і їхніх клієнтів.

Побудова таких автоматизованих систем для процесингового центру і банків вимагає розробки спеціальних моделей, методів і правил аналізу, які створюють образи джерел ризику, моделюють ”поведінку” власника карти, способи попередження шахрайських операцій, а також генерують варіанти прийнятих рішень при виникненні небезпечних ситуацій.

Постановка задачі

Банки-учасники платіжної системи ведуть бази даних всіх емітованих ними пластикових карток, які є в обігу в платіжній системі. По кожній карті в базі даних утримується інформація про її номер, номер пов'язаного з нею рахунку, установлених лімітах операцій, поточного стану рахунку (баланс рахунку), а також основні відомості про власника платіжної карти [5].

Нехай $C_n = \{c_1,...,c_k,...,c_{k_n}\}$ − множина записів у базі даних про платіжні картки, де $c_k = (c_1^k, c_2^k,..., c_s^k)$ запис у базі даних з відомостями про карту c_k. c_1^k – унікальний номер платіжної карти.

Позначимо множину транзакцій, виконаних у платіжній системі до деякого моменту часу t_n через $X_n = \{x^1,...,x^i,...,x^n\}$, а $x^{n+1}, x^{n+2},..., x^{n+k}$ – нові транзакції, зроблені після моменту часу t_n й до t_{n+k}.

Задача виявлення шахрайських транзакцій у платіжній системі полягає в тому, щоб при надходженні в процесинговий центр кожної нової транзакції $x^{n+1} = (x_1^{n+1};...; x_j^{n+1};...; x_m^{n+1})$, на основі інформації, яка міститься в базі даних C_n про платіжні картки і X_n раніше виконані транзакції, класифікувати транзакцію x^{n+1}, тобто визначити клас до якого вона належить (законна (*legal*) або шахрайська (*fraud*)).

Методологія

На сьогоднішній день існує багато різних підходів до розв’язання поставленої задачі, найбільш простими з тих, що використовуються у платіжних системах є:

1. Технологія «Фільтр транзакцій» – використовується для попереднього аналізу всіх транзакцій і автоматичного визначення тих транзакцій, які є «абсолютно законними». Такий фільтр дозволяє скоротити кількість

транзакцій, які потрапляють на етап аналізу [2].

2. Технологія «Статистичне відхилення» - дозволяє швидко виявити випадки явного, значного відхилення від типової поведінки власника карти. Необхідність застосування даної моделі обґрунтовується тим, що можуть виникнути ситуації, при яких транзакція класифікується як законна, однак вона значно відхиляється від типової поведінки власника карти й вимагає більш детального аналізу [3].

Ці методи були покладені в основу перших автоматизованих систем для виявлення шахрайства із платіжними картками, однак вони мають наступні істотні недоліки [2,3]:

1. Ефективність і точність даних методів залежить наскільки точно та повно відображена інформація в базі даних про шахрайські транзакції;

2. Моделі, побудовані таким чином, можуть бути використані для виявлення шахрайства тільки тих видів, які раніше вже зустрічалися в навчальній вибірці;

3. Набір правил необхідно змінювати і доповнювати вручну для того, щоб він відповідав поточним способам шахрайства;

В даній статті пропонується використовувати сучасний метод карт Кохонена що самоорганізуються, який базується на теорії нейронних мереж і відноситься до алгоритмів навчання без учителя [4].

Аналіз транзакцій методом Кохонена представимо у вигляді блок-схеми алгоритму (Рис.1). Процес моніторингу транзакцій складається із трьох фаз: накопичення даних, навчання (побудови профайлу власника карти) і перевірки транзакцій.

На етапі накопичення даних відбувається збір транзакцій, що виконувались по карті c_k. Якщо потужність множини X_{c_k} перевищує певний рівень, достатній для побудови адекватного профайлу поведінки власника карти, то процес моніторингу переходить до фази 2.

На етапі навчання створюється профайл власника карти W_{c_k}:

– використовуючи перетворення φ (кожному символьному параметру транзакції ставиться у відповідність числове значення) формується множина P_{c_k};

– виконується навчання на основі навчальної вибірки P_{c_k};

– у результаті процесу навчання будується профайл $W_{c_k} = \left\| w_k^s \right\|_{\substack{s=\overline{1;d} \\ k=1;M}}$.

Після фази навчання переходимо до фази перевірки транзакцій, що складається з наступних кроків:

– до кожної нової транзакції x^{n+1}, що надійшла на перевірку, застосовується перетворення φ й будується вектор $p^{n+1} = \varphi(x^{n+1})$;

– обчислюється відхилення $\delta_0 = \delta(x^{n+1}, W_{c_k})$ даної транзакції від створеного на етапі навчання профайлу W_{c_k};

– значення δ_0 порівнюється з установленим для профайлу W_{c_k} граничним значенням параметра ε_l (ε_l є граничним значенням ступеня подробиці транзакцій по карті c_k її профайлу W_{c_k} й дозволяє відкидати транзакції, які відхиляються від прийнятої норми. Параметр ε_l дозволяє управляти точністю виявлення шахрайських транзакцій.);

– якщо $\delta_0 \le \varepsilon_l$, то транзакція x^{n+1} розцінюється як типова й множина $X_l = X_{c_k}$, поповнюється вектором x^{n+1};

– якщо $\delta_0 > \varepsilon_l$, то транзакція x^{n+1} розцінюється як підозріла на шахрайство й записується в множину X_f для подальшого експертного аналізу.

Результати дослідження

Застосування запропонованого методу будо реалізовано на прикладі за допомогою програмного продукту Delphi 7. Для оцінки транзакцій були обрані наступні показники: x_1 – дата та час транзакції, x_2 – тип транзакції (ATM, POS), x_3 – тип ретейлера, x_4 – код транзакції, x_5 – валюта, x_6 – сума транзакції, x_7 – країна термінала, x_8 – місто термінала.

Для того, щоб перевірити точність роботи даної моделі поведінки власника карти у вибірці для навчання розглядалося 218 транзакцій, а у тестовій вибірці– 24 транзакції, що характеризували поведінку власника карти (дані були змодельовані).

Для карти було побудовано модель типової поведінки власника карти. В результаті проведених розрахунків було знайдено наступні дані: averrl, averrt – середньо допустима похибка у навчальній і тестовій множинах відповідно, maxerrl, maxerrt – максимально допустима похибка у навчальній і тестовій множинах відповідно.

Нові транзакції, які будуть надходити до процесингового центру не повинні перевищувати середню та максимально допустиму похибку. Якщо транзакція перевищує максимальну похибку, то вона вважається підозрілою і вірогідність того, що вона є шахрайською досить велика, у порівнянні з транзакцією, яка перевищує лише середню похибку.

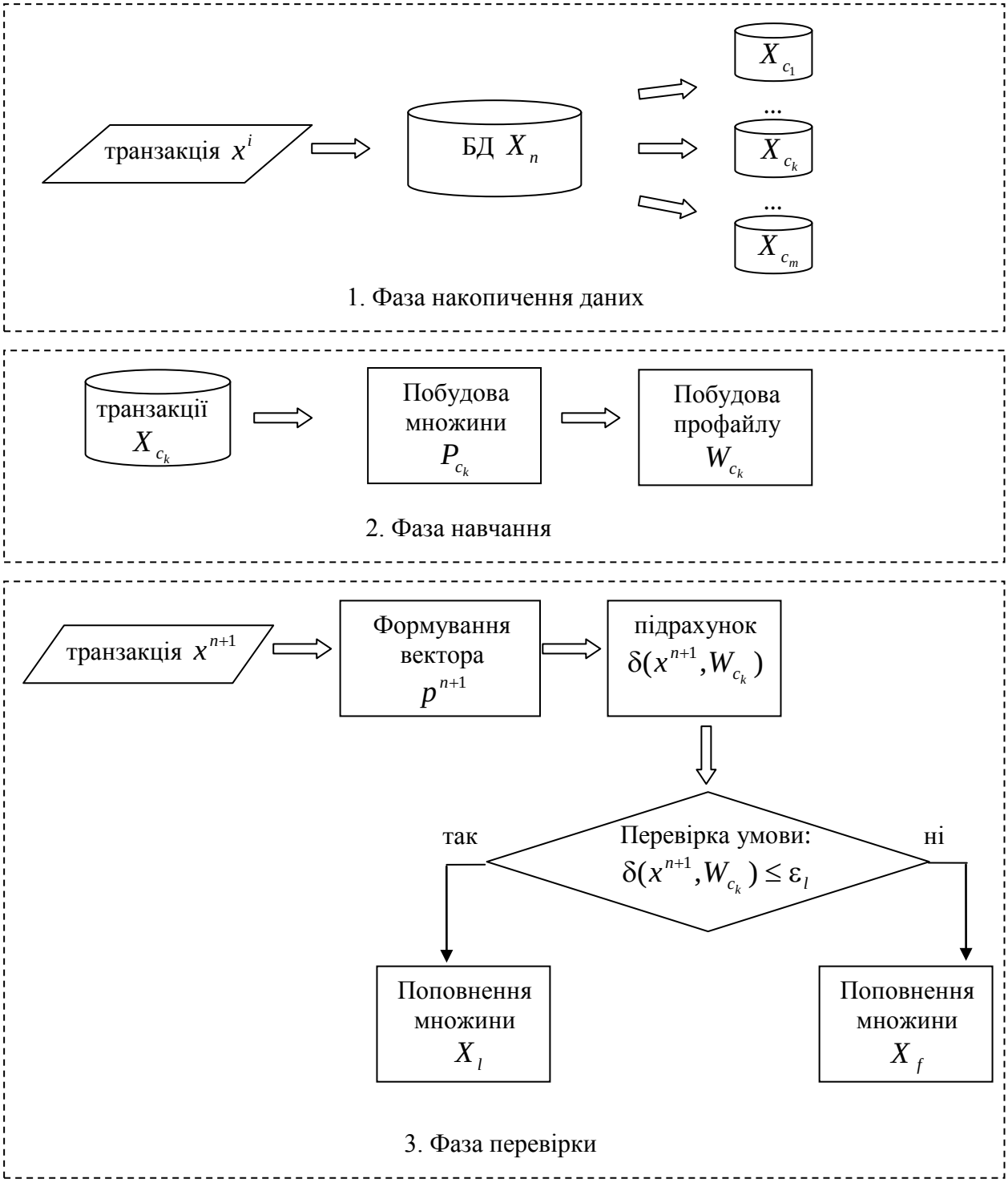

Рис.1. Блок-схема алгоритму аналізу транзакцій

Для моделі поведінки власника карти була побудована карта Кохонена. На рис.2 наведені кластери, отримані в результаті побудови моделі типової поведінки власника карти.

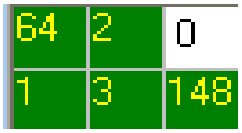

Рис 2. Карта Кохонена

З карти кластерів видно, що поведінка власника карти має два яскраво виражені типи, які можна назвати ”Типові транзакції”, а також декілька ”Нетипових транзакцій”.

Після того, як закінчився процес навчання, на вхід до системи було подано дві нові транзакції, одна з яких була типовою для власника карти, а інша підозріла на шахрайську. Отримані результати наведені на рис. 3 і 4.

Розрахунок відхилення транзакції

	avverl	maxerrl	avvert	maxerrt
Карта :	0,9428441	3,7115973	1,8694986	3,4521453
Транз-я:	0,0357792	0,0357792	0,0357792	0,0357792
Відхил-я:	0,9070648	3,675818	1,8337193	3,416366

Рис 3. Результат перевірки типової транзакції

Розрахунок відхилення транзакції

	avverl	maxerrl	avvert	maxerrt
Карта :	0,9428441	3,7115973	1,8694986	3,4521453
Транз-я:	15,7123206	15,7123206	15,7123206	15,7123206
Відхил-я:	-14,7694765	-12,0007233	-13,842822	-12,2601753

Рис 4. Результат перевірки транзакції підозрілої на шахрайство

Першу транзакцію система прийняла як законну, оскільки її параметри не перевищують жодного з допустимих значень (Рис. 3). Другу транзакцію система визнала підозрілою на шахрайську, оскільки всі допустимі значення було перевищено (Рис. 4). Отримані результати відповідають дійсності.

Висновки

Для виявлення підозрілих на шахрайство транзакцій у платіжній системі в даній статті було розглянуто метод карт Кохонена що самоорганізуються. Цей метод у процесі навчання дозволяє автоматично виробити правила обробки транзакцій і періодично їх удосконалювати в умовах інформації, що динамічно змінюється в автоматизованій системі.

Запропонований метод має наступні переваги: цей метод зручно використовувати навіть в тих випадках, коли відсутня попередня інформація про спостереження по транзакціях з різних класів. Достатньо мати інформацію лише по одному класу транзакцій (законних або шахрайських); метод карт Кохонена дозволяє визначити як вже відомі, так і раніш не зафіксовані типи шахрайства; при оперуванні великою кількістю транзакцій забезпечується проста візуалізація даних.

В результаті на основі побудованої моделі виявлення шахрайства з пластиковими картками стає можливим оцінка транзакцій платіжних карт, та прийняття рішень відносно законності даних транзакцій. Адекватність моделі експериментально підтверджено.

Література:

1. Вертузаев М.С., Кондратьев Я.Ю., Пугачев С.Е., Юрченко А.М. Способы совершения преступлений с использованием банковских платежных карт // Інформаційні технології та захист інформації: Зб. наук. праць.- Запоріжжя: Юридичний ін-т МВС України,1999. - Вип 3. – №1. – С.50-67. – ISBN 966-95343-1-3.
2. Гинзбург А.И. Пластиковые карты [Текст]. – СПб.: Питер, 2004. – 128с. – 2000 пр. – ISBN 546-90016-5-2.
3. Рубинштейн Т.Б., Мирошкина О.В Пластиковые карты [Текст]. – СПб.: Питер, 2005. – 416с. – 1000 пр. – ISBN 5-85438-118-4.
4. T. Kohonen, Self-Organizing Maps (Third Extended Edition) [Text], New York, 2001, 501 pages. – ISBN 3-540-67921-9.
5. Быстров Л. В., Воронин А. С., Гамольский А. Ю. и др. Пластиковые карты [Текст]. – СПб.: Питер, 2007. – 624с. – 1000 пр. – ISBN 5-93306-066-6.