DOI: 10.18372/2410-7840.21.13769
УДК 004.056.5:336:004.8(045)

ВИЯВЛЕННЯ ФІНАНСОВИХ ШАХРАЙСТВ ЗАСОБАМИ МАШИННОГО НАВЧАННЯ

Андрій Фесенко, Ганна Папірна, Мадіна Бауиржан

Система виявлення фінансових шахрайств засобами машинного навчання – сучасний інструмент забезпечення інформаційної безпеки у фінансових установах і комерційних організаціях. У даній роботі формалізовано задачу виявлення фінансових шахрайств з платіжними картками у термінах машинного навчання. Обґрунтовано вибір математичного апарату для функціонування моделі виявлення фінансових шахрайств з платіжними картками. Також було адаптовано математичні алгоритми до розв'язання задачі класифікації транзакцій і наведено покроковий алгоритм реалізації даної задачі машинного навчання. Розроблено та обґрунтовано технічну реалізацію системи виявлення фінансових шахрайств з платіжними картками на базі хмарних служб Microsoft Azure. Проведено оцінку ефективності роботи запропонованої системи виявлення шахрайських транзакцій, де критерієм ефективності було обрано загальноприйняті показники у теорії машинного навчання чутливість та специфічність.

Ключові слова: *системи виявлення фінансових шахрайств, машинне навчання, хмарні сервіси, системи підтримки прийняття рішень, безпека операцій.*

Вступ

Відповідно до Огляду ринку платіжних карток та платіжної інфраструктури України за 2018 рік [1] Національного Банку України, тренди розвитку безготівкових операцій та безконтактної платіжної інфраструктури є позитивними та продовжують зростати із року в рік. Станом на 1 січня 2019 року українські банки емітували майже 59,4 млн платіжних карток. Кількість безготівкових операцій за цей період зросла майже на 33,0% порівняно з 2017 роком і становила 3,1 млрд одиниць.

В той же час, згідно [2], протягом 2018 року в Україні до кіберполіції надійшло близько 6 000 звернень; третина з них була пов'язана з кримінальними правопорушеннями стосовно платіжних систем на загальну суму понад 25 млн гривень. Із загальної кількості кіберзлочинів левова частка припадає на карткове шахрайство. Що стосується держателів карток, то суми, якими заволодівають шахраї, можуть бути абсолютно різними – від 100 грн до 30 тис. грн.

За такої статистики виникає актуальне завдання, а саме: необхідність впровадження систем виявлення шахрайств з платіжними картками у банківських та фінансових установах, а також у комерційних організаціях, які отримують прибуток за рахунок безготівкових операцій (інтернет-магазини, сервіси бронювання квитків та інші).

Метою роботи є: моделювання циклу побудови системи виявлення шахрайства із платіжними картками засобами машинного навчання.

Аналіз останніх досліджень та публікацій

Проблемою розробки алгоритму та моделювання системи виявлення шахрайств у сфері платіжних карток займалися у своїх дослідженнях такі закордонні науковці: S. Bhattacharyya, C. Whitrow, L. Akoglu, M. Snoeck, B. Baesens, C. Bravo, O. Caelen, T. Eliassi-Rad, S. K. Jha, K. K. Tharakunnel, J. C. Westland, D. J. Hand, P. Juszczak, D. Weston, N. M. Adams, V. Van Vlasselaer та інші. Серед вітчизняних науковців таких досліджень не проводилось.

Сучасні дослідження стосуються створення математичної моделі та алгоритмів для виявлення шахрайств, але не охоплюють технічну реалізацію такої системи із забезпеченням конфіденційності даних.

Аналіз функціоналу більшості сучасних систем виявлення шахрайств у сфері платіжних карток [3 С. 190-199] показав, що вони забезпечують аналіз транзакцій на основі правил, які явно задаються відповідальними особами. Даний підхід є застарілим, адже для підтримки чинних правил і критеріїв оцінки транзакцій на стабільному рівні ефективності, потрібно постійно вручну уточнювати умови аналізу.

Системи, засновані на правилах виявляють шахрайства за поверхневими і очевидними сигналами. Нетипово великі транзакції або ті, які відбуваються в нетипових місцях, очевидно, заслуговують додаткової перевірки. Такий підхід тягне за собою використання алгоритмів, які виявляють лише декілька сценаріїв шахрайств. Сьогодні в таких системах застосовують в середньому близько 300 різних правил для схвалення транзакції, в той же час вони залишаються занадто простими. Адже, ручне коригування сценаріїв не дозволяє виявити неявні кореляції. Крім того, засновані на правилах системи часто використовують застаріле програмне забезпечення, яке навряд чи може обробляти потоки даних в реальному часі, що має

вирішальне значення для оперативного прийняття рішення щодо транзакції.

Якщо в установі є кваліфіковані фахівці, здатні постійно створювати правила і підтримувати їх в актуальному стані, то цього буде досить для організації ефективного захисту від шахрайства в платіжній сфері та підтримки ризиків на прийнятному рівні.

Однак, у будь-якій установі або приватному підприємстві, що має справу з платіжними операціями, не існує можливості постійного розширення штату фахівців, які будуть займатися супроводом системи виявлення шахрайств за мірою збільшення кількості транзакцій. Таким чином, виникає потреба у розширенні автоматизації даного процесу і зведенні до мінімуму участі людини в ньому.

Системи виявлення поведінкових шахрайств на основі машинного навчання потребують участі людини тільки на початковому етапі впровадження (тобто, на етапі самого навчання) і на етапі розслідування неоднозначних випадків. Основними перевагами таких систем є їхня адаптивність до появи нових типів та фактів шахрайства. Машинне навчання дозволяє створювати алгоритми, які обробляють великі набори даних з багатьма змінними і допомагають знаходити приховані кореляції між поведінкою користувача і ймовірністю шахрайських дій. До мінусів слід віднести складність побудови, а також необхідність наявності моделей або для кожного клієнта або для характерної групи клієнтів, поведінка яких є досить типовою. Додатково, системи на основі машинного навчання добре поєднуються з рішеннями для відслідковування поведінкової аналітики, допомагаючи скоротити кількість етапів верифікації при здійсненні транзакції.

Постановка завдання

Незважаючи на велику кількість наявних на ринку готових систем виявлення фінансових шахрайств, більшість з них не задовольняє вимогам ведення бізнесу та інформаційної безпеки.

Наприклад, у приватних організаціях у сфері електронної комерції передача будь-яких даних системам третіх сторін найчастіше є небажаною та часто забороненою політикою інформаційної безпеки організації. Тому, виникає потреба у створенні власної системи виявлення шахрайств у сфері платіжних карток.

Ще однією причиною потреби у створенні власної системи виявлення шахрайств у сфері платіжних карток є те, що архітектура, алгоритми та, часто, загальна логіка побудови таких систем, наявних на ринку, є закритими. Таким чином, замовнику невідомо, які саме дані про транзакцію обробляються та за якими параметрами класифікуються, а також куди передаються під час процедури обробки.

Отже, виходячи із вище сказаного, завданням даного дослідження є створення гнучкої системи виявлення шахрайств у сфері платіжних карток на базі засобів машинного навчання, з дотриманням вимог інформаційної безпеки сучасного бізнесу та з мінімальними витратами на технічне забезпечення такої системи.

Вирішення поставленого завдання відбуватиметься за наступними етапами: визначення класу задач, до якого відноситься проблема виявлення фінансових шахрайств; вибір найефективнішого алгоритму машинного навчання; створення технічної архітектури системи виявлення шахрайств у сфері платіжних карток.

Перш за все, є доцільним пояснити використовувану в роботі термінологію.

Теорія навчання машин (Machine Learning – ML, машинне навчання) – математична та інженерна дисципліна, що вивчає методи побудови алгоритмів, здатних навчатися. Дана наукова дисципліна знаходиться на стику прикладної статистики, чисельних методів оптимізації та дискретного аналізу. Однак, це не тільки математична, а й практична, інженерна дисципліна. Теорія, як правило, не призводить відразу до методів і алгоритмів, які можуть застосовуватися на практиці. Для їх належної роботи необхідні додаткові евристики, що компенсують невідповідність зроблених в теорії припущень умовам реальних завдань.

У будь-якій задачі машинного навчання існує задана множина об'єктів X, множина допустимих відповідей Y та цільова функція y^*: $X \to Y$, значення якої $y_i = y^*(x_i)$ відомі тільки на скінченній множині об'єктів $\{x_1, \ldots, x_\ell\} \subset X$. Пари «об'єкт – відповідь» (x_i, y_i) називаються прецедентами. Сукупність пар $X^\ell = (x_i, y_i)^\ell{}_{i=1}$ називається навчальною вибіркою.

Задача навчання полягає у тому, щоб за вибіркою X^ℓ відновити залежність y^*, тобто побудувати вирішуючу функцію a: $X \to Y$, яка б наближала цільову функцію $y^*(x)$, причому не тільки на об'єктах навчальної вибірки, а і на всій множині X.

Вирішуюча функція a повинна допускати ефективну комп'ютерну реалізацію; з цієї причини вона називається алгоритмом.

Ознака f об'єкта x – це результат вимірювання деякої характеристики об'єкта. Формально ознакою називається відображення $f : X \to D_f$, де D_f – це множина допустимих значень ознаки.

Метод навчання або навчальний алгоритм – це відображення $\mu: (X \times Y)^\ell \to A$, яке довільній скінченній вибірці $X^\ell = (x_i, y_i)^\ell{}_{i=1}$ ставить у відповідність деякий алгоритм $a \in A$. Також можна сказати, що метод μ будує алгоритм a за вибіркою X^ℓ. Метод навчання повинен допускати ефективну програмну реалізацію.

Таким чином, в задачах машинного навчання розрізняють два етапи.

На етапі навчання метод μ за вибіркою X^ℓ будує алгоритм $a = \mu(X^\ell)$.

На етапі застосування алгоритм a для нових об'єктів x видає відповіді $y = a(x)$.

Етап навчання є найбільш складним. Як правило, він зводиться до пошуку параметрів моделі, які надають оптимальні значення за прийнятим критерієм ефективності [4 с. 4–14].

Вирішення поставленого завдання

Для побудови системи виявлення фінансових шахрайств необхідно спочатку визначити, до якого класу задач машинного навчання належить дана проблема.

Почати доцільно із розглядання вхідних даних, за якими модель буде навчатися. Цими даними є ретроспектива транзакцій з рахунку одного користувача. Це означає, що установі, відповідальній за обслуговування такого рахунку відома різниця між нормальними операціями та несанкціонованими операціями (через повідомлення банку, іншої фінансової установи про шахрайство, несподіване списування коштів тощо). Говорячи термінами машинного навчання, пари «об'єкт – відповідь» відомі, невідомою є лише залежність між ними.

Система виявлення фінансових шахрайств повинна дати відповідь на питання «чи є дана транзакція шахрайською або нормальною?». Таким чином, $Y = \{0,1\}$ та алгоритм навчання повинен розділити множину транзакцій на два класи – шахрайські або нормальні. Виходячи з цього, виявлення фінансових шахрайств є задачею бінарної класифікації.

При розробці моделей виявлення шахрайства з кредитними картками, спочатку доступний тільки сирий набір даних, що включає в себе інформацію щодо індивідуальних транзакцій. Типовими атрибутами полів транзакції є: Transaction ID (Унікальний ідентифікатор транзакції); Date (Дата і час транзакції); Debet / Credit (Дебет / Кредит); Account number (Ідентифікатор рахунку відправника / одержувача); Transaction type (Тип транзакції: оплата у POS-терміналі; прямий дебет; зняття готівки в банкоматах; комісія, що стягується банком; переведення з поточного рахунку на власний ощадний рахунок; переведення третій стороні за допомогою інтернет-банкінгу тощо); Amount (Сума транзакції); Comments (Коментарі).

Кожне поле транзакції містить важливу інформацію, яку можна використати для побудови моделі виявлення фінансових шахрайств. Однак, така інформація у своєму початковому вигляді не може бути використана для побудови ефективної моделі.

Не всі атрибути транзакції є достатньо інформативними для її успішної класифікації. Інформативність означає, що хоча всі атрибути є предикатами транзакції, тобто описують її, не всі вони є закономірностями, тобто здатними виділяти достатньо багато транзакцій одного класу.

Поле «Transaction ID» не є необхідним для побудови моделі, так як унікальність ідентифікатора транзакції перевіряється та забезпечується безпосередньо банківською установою, а також зберігання та обробка цих даних є забороненою у ряді міжнародних стандартів.

Поле «Date» необхідне для побудови моделі тому що, як правило, витрати фізичних осіб є циклічними та повторюються щотижня, щомісяця, щороку тощо. Використовуючи дані із цього поля можливо відслідкувати поведінкові закономірності особи у транзакціях.

Поле «Debet / Credit» буде використовуватися для побудови моделі тільки зі значенням «Debet», так як це означає втрати для власника рахунку. В свою чергу значення «Credit», означає надходження коштів на рахунок, і не несе збитків власнику рахунку.

Поля «Account number» також виключено, так як модель виявлення фінансових шахрайств буде застосовуватися до кожного окремого рахунку. Це обумовлено тим, що для одного рахунку транзакція може бути підозрілою, а для іншого цілком нормальною, враховуючи поведінкові закономірності власника рахунку.

Значення поля «Transaction type» є необхідним, так як відображає типові типи транзакцій для конкретного рахунку.

Поле «Amount», тобто сума здійсненої транзакції, є обов'язковим для використання і найважливішим з усіх атрибутів транзакції. Це випливає із призначення моделі, яка пропонується.

Поле «Коментарі» виключено, так як воно може містити довгий неструктурований текст, який може ускладнити та погіршити роботу моделі виявлення шахрайств.

Таким чином, на вході алгоритму виявлення фінансових шахрайств буде задано множину транзакцій X, де кожен об'єкт цієї множини описується m предикатами (ознаками). Виходячи із зазначених вище положень, множина транзакцій буде описуватися трьома ознаками: «Date», «Transaction type» та «Amount».

Серед усіх алгоритмів машинного навчання, які вирішують проблеми бінарної класифікації, найкращим за співвідношенням критеріїв точність – ресурсозатратність є алгоритм C4.5, що є доведеним багатьма дослідженнями в даній області [5 С. 180-185].

Алгоритм C4.5 є різновидом відомого із теорії графів дерева рішень. Процес побудови ієрархічної класифікаційної моделі у вигляді дерева із множини транзакцій X відбувається згори до низу. Спочатку створюється корінь, а потім інші вершини дерева.

На першому кроці маємо порожнє дерево (тільки корінь) і вихідну множину транзакцій X (асоційовану з коренем). Необхідно розбити вихідну множину на підмножини. Це можна зробити, вибравши одну з ознак в якості перевірки. Тоді в результаті розбиття вийде n (за кількістю значень ознаки) підмножин і, відповідно, створиться n вершин дерева (нащадків кореня), кожній з яких буде поставлена у відповідність своя підмножина, отримана при розбитті множини транзакцій X. Потім ця процедура рекурсивно застосовується до всіх підмножин (нащадків кореня).

Розглянемо критерій вибору ознаки, за якою має відбутися розгалуження дерева. Маємо m (за кількістю ознак) можливих варіантів, з яких необхідно вибрати найбільш підходящий.

Нехай маємо перевірку T (в якості перевірки може бути обрана будь-яка ознака), яка приймає n значень A_1, A_2...A_n. Тоді розбиття K з перевірки T дасть нам підмножини K_1, K_2... K_n, при T дорівнює відповідно A_1, A_2...A_n.

Тоді, критерій вибору ознаки відбуватиметься наступним чином.

Нехай freq (C_j, S) – кількість транзакцій з деякої множини S, що відносяться до одного і того ж класу C_j. Тоді ймовірність того, що випадково обрана транзакція з множини S буде належати до класу C_j:

$$P=\frac{\text{freq}\,(C_j,S)}{|S|}, \qquad (1)$$

де P – ймовірність того, що випадково обрана транзакція буде належати до класу C_j; freq (C_j, S) – кількість транзакцій з деякої множини S, що відносяться до одного і того ж класу C_j; C_j – клас, з яким може бути асоційована транзакція; S – множина транзакцій, що є частиною загальної множини усіх транзакцій X.

Згідно із теорією інформації, кількість інформації, що міститься в повідомленні, залежить від її ймовірності:

$$\text{B}=\log_2\left(\frac{1}{P}\right), \qquad (2)$$

де B – кількість інформації, що міститься в повідомленні; P – ймовірність.

Оскільки було використано логарифм з двійковою основою, то вираз (2) надає кількісну оцінку в бітах.

Далі, є доцільним визначення кількості інформації, необхідної для віднесення транзакції із множини X до відповідного класу:

$$\text{Info}(X)=-\sum_{j=1}^{k}\frac{\text{freq}\,(C_j,S)}{|X|}\times\log_2\frac{\text{freq}\,(C_j,S)}{|X|}, \qquad (3)$$

де Info (X) – ентропія множини транзакцій X, відповідно до термінології теорії інформації.

Таке ж визначення кількості інформації, але після розбиття множини X за T, дає наступний вираз:

$$\text{Info}_T(X)=\sum_{i=1}^{n}\frac{|X_i|}{|X|}\times\text{Info}(X_i). \qquad (4)$$

Тоді критерієм для вибору ознаки буде наступна формула:

$$\text{Gain}(T)=\text{Info}(X)-\text{Info}_T(X). \qquad (5)$$

Критерій (5) розраховується для всіх ознак. Обирається ознака, яка максимізує даний вираз. Ця ознака буде перевіркою в поточній вершині дерева, а потім із цієї ознаки проводитиметься подальша побудова дерева. Тобто, у вершині буде перевірятися значення із цієї ознаки і подальший рух по дереву буде проводитися в залежності від отриманої відповіді.

Такі ж міркування можна застосувати до отриманих підмножин K_1, K_2... K_n і продовжити рекурсивно процес побудови дерева, до тих пір, поки у вершині не опиняться транзакції з одного класу.

Обґрунтуємо причину максимізації критерію (5). Із властивостей ентропії відомо, що максимально можливе значення ентропії досягається у тому випадку, коли всі його повідомлення рівновірогідні. У даному випадку, ентропія (4) досягає свого максимуму коли частота появи класів в транзакціях множини X рівноймовірна. Задача ж полягає у виборі такої ознаки, щоб при розбитті по ній один із класів мав найбільшу ймовірність появи. Це можливо в тому випадку, коли ентропія (4) матиме мінімальне значення і, відповідно, критерій (5) досягне свого максимуму.

Описані вище положення дозволяють сформувати дерево рішень. Для застосування даного алгоритму до поставленого практичного завдання, обхід дерева рішень починається із кореня дерева. На кожній внутрішній вершині перевіряється значення транзакції x за ознакою, яка відповідає перевірці в даній вершині, і, в залежності від отриманої відповіді, знаходиться відповідне розгалуження, яке опускає обхід дерева на рівень нижче. Обхід дерева закінчується як тільки зустрінеться вершина рішення, яка і дає назву класу транзакції x.

Для технічної реалізації системи виявлення шахрайських транзакцій пропонуємо створення високодоступного та масштабуємого сервісу, який складається з декількох додатків, працюючих в хмарних службах Microsoft Azure (Azure Cloud Services).

Причинами вибору хмарних служб Azure для реалізації системи виявлення шахрайських транзакцій є, по-перше те, що дані служби є системами зберігання даних із високою надмірністю та відповідають більшості міжнародних стандартів із інформаційної безпеки та безпеки операцій із кредитними картками, таких як ISO 27001/27002 та PCI DSS 3.2. Крім цього, система виявлення шахрайств на базі хмарних служб Azure буде відповідати і вимогам українського законодавства. Адже, інформація про операції не буде зберігатися в хмарному сховищі, туди потраплятимуть тільки вибрані атрибути транзакцій, які є дозволеними для зберігання Положенням про організацію операційної діяльності в Україні. Таким чином, використання хмарних служб Azure і не порушує законодавство і дозволяє повністю уникнути витрат на утримання серверного та мережевого господарства.

Хмарні служби Azure є прикладом концепції платформи як послуги (Platform as a Service – PaaS).

PaaS – модель надання хмарних обчислень, при якій підписник отримує доступ до використання інформаційно-технологічних платформ: операційних систем, систем управління базами даних, сполучного програмного забезпечення, засобів розробки і тестування, розміщеними у хмарного провайдера.

Технологія Azure Cloud Services призначена для підтримки масштабованих, надійних і недорогих в експлуатації додатків. Хмарні служби Azure розміщуються на віртуальних машинах. На віртуальних машинах, що використовують хмарні служби Azure, можна встановити власне програмне забезпечення, а потім отримати віддалений доступ до нього.

Пропонуємо створити систему виявлення шахрайських транзакцій у вигляді REST-сервісу (Representational State Transfer – передача репрезентативного стану) [6].

REST – це архітектурний стиль взаємодії компонентів розподіленого додатку в мережі. Компоненти REST взаємодіють на кшталт клієнту та серверу, за допомогою HTTPS запитів. Тобто, користувач системи буде відправляти запит на перевірку транзакції, використовуючи веб-браузер, на програмний інтерфейс додатку (Application Programming Interface – API) для отримання відповіді.

Архітектура системи виявлення шахрайств наведена на рисунку 1.

Пропонована система виявлення шахрайських операцій складається з наступних компонентів.

API сервісу виявлення шахрайств (з) – це REST-сервіс, який надає API для взаємодії із Сервісом виявлення шахрайств.

Сервіс виявлення шахрайств (а) – ядро системи, яке працює на базі хмарної служби Azure Machine Learning Studio (г). Дана служба надає широкий інструментарій для створення, тестування та впровадження алгоритмів машинного навчання.

Журнал транзакцій (б) – це сховище даних про транзакції, яке працює на базі хмарної служби Azure Tables (г), яка призначена для зберігання великих напівструктурованих наборів даних.

Служба аналітики (в) – призначена для аналізу та візуалізації даних, побудови панелей моніторингу, звітів, графіків, які слугують допоміжним матеріалом для особи, що приймає рішення. Працює на базі хмарної служби Azure Power BI (д).

Процес взаємодії користувача із системою виявлення шахрайських транзакцій може бути описано наступними кроками.

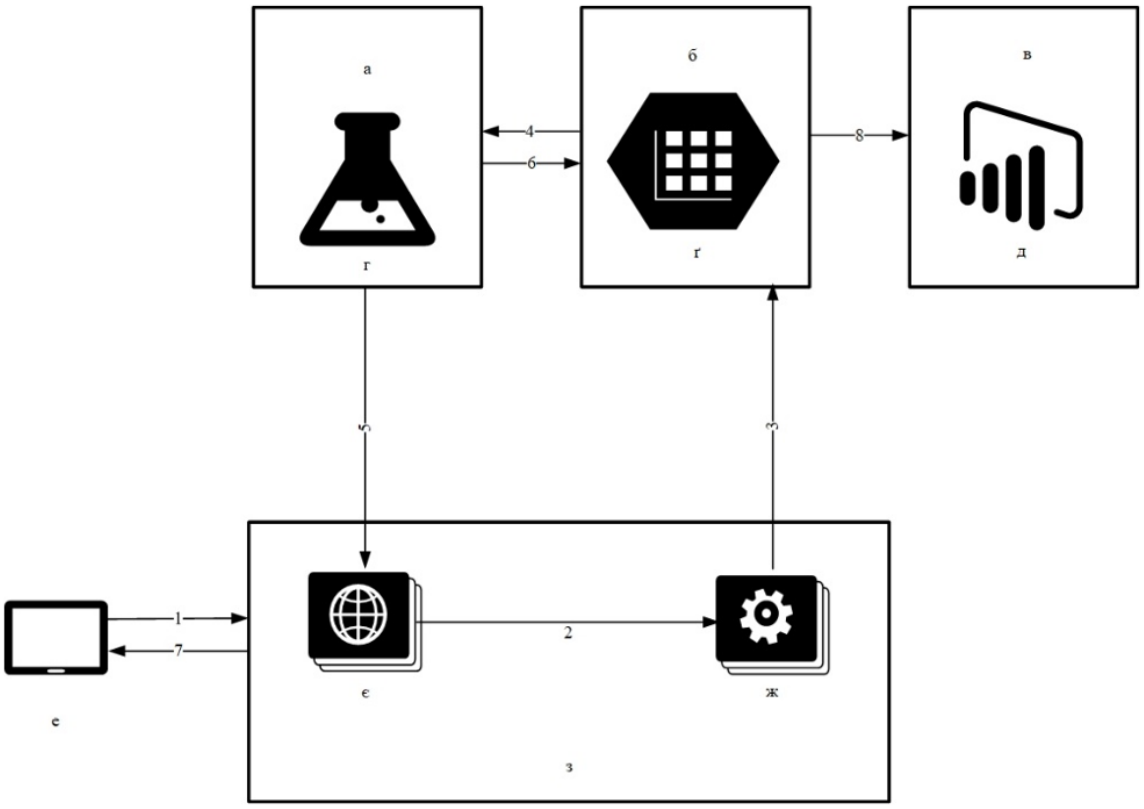

Рис. 1. Архітектура системи виявлення шахрайств

Крок 1 – користувач, використовуючи веб-браузер (е), надсилає HTTPS запит для перевірки транзакції на API сервісу виявлення шахрайств.

Крок 2 – API сервісу виявлення шахрайств працює в кластері із веб-ролі (є) та робочої ролі (ж) хмарної служби Azure. Веб-роль хмарної служби передає дані про транзакції, введені користувачем до робочої ролі.

Крок 3 – робоча роль передає дані про транзакцію до Журналу транзакцій, де дані зберігаються.

Крок 4 – із Журналу транзакцій дані передаються до Сервісу виявлення шахрайств, де обробляються алгоритмом машинного навчання.

Крок 5 – після розрахування відповіді Сервіс виявлення шахрайств повертає рішення про класифікацію транзакції до API сервісу виявлення шахрайств.

Крок 6 – після розрахування відповіді Сервіс виявлення шахрайств повертає рішення про класифікацію транзакції до Журналу транзакцій.

Крок 7 – API сервіс виявлення шахрайств повертає відповідь користувачу.

Крок 8 – із Журналу транзакцій відповідь переходить до Служби аналітики для подальшого аналізу даних.

Оцінку ефективності роботи запропонованої системи виявлення шахрайських транзакцій було проведено на тестовій вибірці історії транзакцій прямих дебетів за міжнародною системою SEPA за три роки [7]. У досліджуваному наборі із 2430 транзакцій 5 були шахрайськими. Після проходження кожної транзакції через алгоритм C4.5 створеної системи виявлення шахрайських фінансових операцій, було виявлено 4 шахрайські операції і всі 2425 нормальних операцій.

Критерієм ефективності було обрано загальноприйняті показники у теорії машинного навчання чутливість та специфічність.

Чутливість алгоритму класифікації (*Sensivity*) – це відношення загальної кількості транзакцій, які містять необхідну ознаку (є шахрайськими) до вірно класифікованих системою транзакцій.

$$Sensivity = \frac{TP}{TP+FN} = \frac{4}{4+1} = 0{,}8, \qquad (6)$$

де *TP* – істинно-позитивне значення (true-positive), якщо результат класифікації позитивний і справжнє значення також є позитивним;

FN – хибно-негативне значення (false-negative), якщо результат класифікації негативний, але справжнє значення позитивне.

Специфічність алгоритму класифікації (*Specificity*) – це відношення загальної кількості транзакцій, які не містять необхідної ознаки (не є шахрайськими) до помилково класифікованих системою транзакцій.

$$Specificity = \frac{TN}{TN+FP} = \frac{2425}{2425+0} = 1, \qquad (7)$$

де *TN* – істинно-негативне значення (true-negative), якщо результат класифікації негативний і справжнє значення теж негативне; *FP* – хибно-позитивне значення (false-positive), якщо результат класифікації позитивний, але справжнє значення негативне.

Таким чином, значення показника чутливості (6) алгоритму становить 0.8, а показник специфічності (7) прямує до одиниці, адже система не класифікувала жодну із нормальних операцій, як шахрайську і відповідно *FP* дорівнює нулю. Зрозуміло, що ці результати є попередніми і потребують перевірки на інших тестових вибірках транзакцій.

Висновки

У даному дослідженні було окреслено цикл побудови системи виявлення шахрайств із платіжними картками засобами машинного навчання. Пропонована система, завдяки своїй технічній архітектурі, є гнучкою і піддається модифікації, у разі появи нових більш досконалих алгоритмів машинного навчання. Розміщення всієї системи на віртуальних машинах робить архітектуру масштабованою, а використання обчислювальних ресурсів керованим.

Пропонований метод створення такої системи є дорожньою картою, що може включати додаткові дослідження ефективності алгоритмів, механізми доопрацювання та економічну доцільність.

ЛІТЕРАТУРА

[1]. Національний банк України. Огляд ринку платіжних карток та платіжної інфраструктури України за 2018 рік. [Електронний ресурс]. Режим доступу: https://bank.gov.ua/doccatalog/document?id=88661687.

[2]. Департамент кіберполіції. Підсумки 2018 року в цифрах. [Електронний ресурс]. Режим доступу до ресурсу: https://cyberpolice.gov.ua/results/2018/.

[3]. П. Равенков, А. Пухов, Л. Лямин, *Мошенничество в платежной сфере. Бизнес-энциклопедия*. М.: Интеллектуальная Литература, 2015, 345 с.

[4]. К. Воронцов, *Математические методы обучения по прецедентам (теория обучения машин)*. [Електронний ресурс]. Режим доступу до ресурсу: http://www.machinelearning.ru/wiki/images/6/6d/Voron-ML-1.pdf.

[5]. B. Baesens, V. Van Vlasselaer, W. Verbeke*, Fraud analytics using descriptive, predictive, and social network techniques : a guide to data science for fraud detection*. Canada: Wiley & SAS business series, 2015, 400 p.

[6]. A. Tselykh, D. Petukhov, "Web service for detecting credit card fraud in near real-time", *SIN '15 Proceedings of the 8th International Conference on Security of Information and Networks*, pp. 114-117, 2015.

[7]. A. Shrivastava, T. Deshpande, Hadoop-Blueprints [Електронний ресурс]. Режим доступу: https://github.com/PacktPublishing/Hadoop-Blueprints/tree/master/Chapter%2003.

ОБНАРУЖЕНИЕ ФИНАНСОВОГО МОШЕННИЧЕСТВА СРЕДСТВАМИ МАШИННОГО ОБУЧЕНИЯ

Система обнаружения финансовых махинаций средствами машинного обучения - современный инструмент обеспечения информационной безопасности в финансовых учреждениях и коммерческих организациях. В данной работе формализована задача обнаружение финансовых махинаций с платежными картами в терминологии машинного обучения. Обоснован выбор математического аппарата для функционирования модели обнаружения финансовых махинаций с платежными карточками. Также было адаптировано математические алгоритмы к решению задачи классификации транзакций и приведен пошаговый алгоритм реализации данной задачи машинного обучения. Разработана и обоснована техническая реализация системы обнаружения финансовых мошенничеств с платежными картами на базе облачных сервисов Microsoft Azure. Проведена оценка эффективности работы предложенной системы обнаружения мошеннических транзакций, где критериями эффективности были выбрана общепринятые показатели в теории машинного обучения - чувствительность и специфичность.

Ключевые слова: системы обнаружения финансовых махинаций, машинное обучение, облачные сервисы, система поддержки принятия решений, безопасность операций.

THE FINANCIAL FRAUD DETECTION USING MACHINE LEARNING

The financial fraud detection system using machine learning is a modern tool for ensuring information security in financial institutions and commercial organizations. The relevance of this work is due to an increase in trends in the development of the use of cashless transactions, together with an increase in criminal offenses related to payment card fraud. An analysis of the research of scientists on this topic is provided and it shows that they cover the individual components of building a financial fraud detection system, but do not describe the complete cycle of the development and implementation of such a system. The two fundamentally different approaches to identifying financial fraud are considered – based on rules and based on machine learning tools. The advantage of using machine learning tools is substantiated in the context of improving the usability of the system, increasing the accuracy of fraud detection and possible integration with behavioral analytics systems. In this paper, the problem of detecting financial fraud with payment cards is formalized in machine learning terminology. The choice of the mathematical apparatus for the functioning of the model of detecting financial fraud with payment cards is substantiated. Mathematical algorithms are adapted to solve the problem of transaction clas-

sification and a step-by-step algorithm for the implementation of this machine learning task is given. The technical implementation of the system for detecting financial fraud with payment cards based on Microsoft Azure cloud services is developed and substantiated. The effectiveness of the proposed system for detecting fraudulent transactions is assessed, where sensitivity and specificity are selected as the criteria for efficiency being generally accepted indicators in machine learning theory.
Keywords: financial fraud detection systems, machine learning, cloud services, decision support systems, security of operations.

Фесенко Андрій Олексійович, кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій КНУ імені Тараса Шевченка.
E-mail: aafesenko88@gmail.com.
Orcid ID: 0000-0001-5154-5324.
Фесенко Андрей Алексеевич, кандидат технических наук, асистент кафедры кибербезопасности и защиты информации факультета информационных технологий КНУ имени Тараса Шевченко.
Fesenko Andrii, PhD, assistant of the Cybersecurity and Information Security Department of the Information Technology Faculty, Taras Shevchenko National University of Kyiv.

Папірна Ганна Костянтинівна, студентка кафедри кібербезпеки та захисту інформації факультету інформаційних технологій КНУ імені Тараса Шевченка
E-mail: mhiaofy@gmail.com.
Orcid ID: 0000-0001-9989-9412.
Папирна Анна Константиновна, студентка кафедры кафедры кибербезопасности и защиты информации факультета нформационных технологий КНУ имени Тараса Шевченко.
Papirna Hanna, student of the Cybersecurity and Information Security Department of the Information Technology Faculty of Taras Shevchenko National University of Kyiv.

Бауиржан Мадіна Бауиржанівна, докторант PhD, Казахський національний дослідницький технічний університет ім. К.І. Сатпаєва, Алмати, Республіка Казахстан.
E-mail: madina890218@gmail.com.
Orcid ID: 000-0002-8287-4283.
Бауыржан Мадина Бауыржановна, докторант PhD, Казахский национальный исследовательский технический университет им. К.И. Сатпаева, Алматы, Республика Казахстан.
Bauyrzhan Madina, PhD Student, Satbayev University, Almaty, Republic of Kazakhstan.

DOI: 10.18372/2410-7840.21.13768
УДК 004.274:004.056

ПОБУДОВА СКІНЧЕННИХ АВТОМАТІВ РЕКОНФІГУРОВНИМИ ЗАСОБАМИ ДЛЯ ВИРІШЕННЯ ЗАДАЧ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сергій Гільгурт

Протидія загрозам інформаційної безпеки потребує вживання заходів різного плану – організаційних, технічних, криптографічних тощо. Мережеві системи виявлення вторгнень, антивіруси, та інші засоби технічного захисту, робота яких заснована на використанні сигнатур, мають вирішувати в реальному часі обчислювально складну задачу множинного розпізнавання рядків, яка на відміну від одиночного розпізнавання має метою одночасний пошук у вхідних даних великої кількості зразків. Програмні рішення вже не впорюються з цією проблемою через сталий зріст об'єму мережевого трафіку, кількості та складності атак. Тому все більшого поширення набувають апаратні рішення з використанням реконфігуровних пристроїв на базі ПЛІС типу FPGA, які поєднують в собі близьку до апаратної продуктивність із гнучкістю програмного забезпечення. На сьогодні найбільш поширеними є три підходи щодо побудови апаратних схем множинного розпізнавання, робота яких заснована на використанні: асоціативної пам'яті, фільтра Блума та скінченних автоматів. Кожен с підходів має свої власні переваги та вади. Ефективна побудова все більш складних сигнатурних засобів технічного захисту інформації, яки б відповідали вимогам оптимального функціонування в залежності від зовнішніх умов, неможлива без всебічному аналізу властивостей та специфічних рис кожного з підходів. У цьому дослідженні з метою підвищення ефективності створюваних на базі ПЛІС засобів захисту інформації проаналізовані переваги та недоліки третього з перелічених підходів. На основі аналізу світового досвіду використання скінченних автоматів також досліджені особливості їх реалізації на ПЛІС, проблеми, що виникають, та шляхи їх вирішення.
Ключові слова: *захист інформації, сигнатурний аналіз, ПЛІС, скінченний автомат, алгоритм Ахо-Корасік, ефективність.*