УДК 303.09:336.717.1 JEL Classification C10, G21

АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ ПРОТИДІЇ БАНКІВСЬКИМ КІБЕРШАХРАЙСТВАМ[1]

Кузьменко О.В.,
д.е.н., професорка, професорка кафедри економічної кібернетики,
Сумський державний університет, м. Суми, Україна
o.kuzmenko@biem.sumdu.edu.ua
Яровенко Г.М.,
д.е.н., доцентка, доцентка кафедри економічної кібернетики,
Сумський державний університет, м. Суми, Україна
h.yarovenko@biem.sumdu.edu.ua
Скринька Л.О.,
аспірантка кафедри економічної кібернетики,
Сумський державний університет, м. Суми, Україна
l.skrynka@uabs.sumdu.edu.ua

Статтю присвячено актуальній темі аналізу математичних моделей протидії банківським кібершахрайствам. Дана проблематика обумовлена зростанням ризиків безпеки банківської системи через здійснення шахраями кібератак та реалізації кіберзлочинів. Тому пріоритетним завданням для банківської кібербезпеки є застосування сучасних математичних методів для аналізу джерел кібератак, визначення загроз та збитків ринку банківських послуг, виявлення кібернетичних атак та оцінки сценарії ймовірного кіберризику, тощо. В статті було проаналізовано найбільш розповсюджені види кібершахрайств, серед яких виділяють соціальну інженерію, фішинг, сталкінг, фармінг, DoS-атаки, онлайн-шахрайства, потенційно небажані програми, тощо. Також у дослідженні було розглянуто модель когнітивних обчислень та виявлення підозрілих транзакцій у банківських кіберфізичних системах на основі квантових обчислень у BCPS для постквантової ери. Визначено переваги, недоліки та результати моделі. Для виявлення шахрайства в режимі реального часу шляхом аналізу вхідних банківських транзакцій з платіжними картами запропоновано прогнозне моделювання. В межах даного методу використовуються такі моделі для класифікації виявлення шахрайства, як логістична регресія, дерево рішень та більш вузька техніка – дерево рішень випадкового лісу. Також у дослідженні розглянуто використання алгоритму гармонійного пошуку в нейронних мережах для покращення виявлення шахрайства в банківській системі. З'ясовано, що, хоча дана модель має перевагу у спроможності до навчання на основі минулої поведінки, є труднощі в тривалій обробці великої кількості нейронних мереж. Також наведено етапи реалізації моделі. Крім того, проаналізовано моделювання виявлення шахрайства з кредитними картками на базі використання двох типів моделей: під наглядом і без нагляду. До моделей під наглядом віднесено логістичну регресію, K-найближчі сусіди, екстремальне підвищення градієнта. Серед неконтрольованих генеративних моделей розглянуто однокласну опорну векторну модель, обмежену модель Больцмана, генеративно-змагальну мережу.

Ключові слова: *кібершахрайство, банківська система, модель когнітивних обчислень, прогнозне моделювання, дерево рішень, нейронна мережа.*

DOI:10.21272/1817-9215.2022.2-13

ПОСТАНОВКА ПРОБЛЕМИ

Протягом останніх років у банківській інфраструктурі створюються та впроваджуються новітні сервіси та технології обслуговування клієнтів, в тому числі й різноманітні відділено та дистанційно керовані канали та платформи, схеми, продукти та послуги онлайн-банкінгу для клієнтів банків, що дозволяють скоротити транзакційні витрати, покращити обслуговування та утримання клієнтів. Паралельно з цим зростає і ризик безпеки банківської системи через постійні спроби шахраїв здійснити кібератаки та реалізувати кіберзлочини на ринку фінансів, пов'язані з конфіденційними операціями, доступом до важливої системної інформації. Тобто,

[1] *Робота виконана в рамках держбюджетних науково-дослідних робіт: 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку»; 0121U100467 «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України».*

ризики та загрози шахрайства є критичними проблемами у банківській кіберфізичній системі. Число таких кібернетичних атак в останні роки постійно збільшується та становить реальну загрозу стабільному функціонуванню банківських установ.

Так, для організації безпеки функціонування банківського сектору, з метою збереження довіри, прихильності та впевненості клієнтів, банківські установи запроваджують технічні контрзаходи до кібератак, онлайн-злочинів, кібершахрайств, несанкціонованого втручання та доступу до банківської операційної системи. Однак, традиційні системи аналізу джерел кібератак у банківській системі, моделювання кібершахрайств банківських операцій, засновані на недостатньо адаптованих та дієвих методиках з обмеженими, неповними можливостями та характеристиками, з високою вартістю впровадження, розгортання та обслуговування, зі складною інтеграцією між процесами автентифікації, системами дистанційного обслуговування, онлайн-банкінгу. Тому дедалі загострюються та потребують досконалого вивчення питання практичної реалізації оцінки джерел кібератак ринку банківських послуг, пріоритезації найбільш поширених видів шахрайств, визначення кіберзагроз, виявлення кібернетичних атак, побудови сценаріїв ймовірного кіберризику, тощо. Відповідно, виникає потреба у дослідженні математичних методів та інструментів, які доцільно застосовувати в процесі вирішення поставлених завдань

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Загальнотеоретичні питання – характеристики, особливості, поняття, проблеми кібератак та кібершахрайств, розкриваються у працях сучасних науковців: Надрі Е., Пазукі С., і Асрарі А. [1] визначають схему та засоби дій проти кібератак; Сунь М., Хе Л., Чжан Дж. [2] описують особливості кібератак в електроенергетиці та енергетичних системах; Ачарья С., Міт Р., Константину К., Каррі Р. і Дворккін Ю. [3] трактують особливості кіберстрахування від кібератак; Хоу Л., Лі Ю., Луо В. і Сан Х. [4] показують особливості управління кібер-фізичними системами при кібератаках; Ван В., Харроу Ф., Буєдду Б., Сеноучі С. і Сан Ю. [5] описують комплексний підхід до поняття кібератак у промислових системах, та ін.

Специфічні проблеми кібератак, а також кібершахрайств банківського сектору, досліджують економісти, фінансисти та фахівці ІТ сектору, такі як: Есваран С., Рані В., Даніель Д., Рамакрішнан Дж. і Сельвакумар С. [6] анонсують покращену систему виявлення вторгнень в мережу банківської інфраструктури; Цай Ч. і Су П. [7] пропонують застосування схеми мультисерверної аутентифікації кібершахрайств в транзакційних середовищах інтернет-банкінгу; Чхабра Рой Н. і Прабхакаран С. [8] розкривають побудову стійкої системи реагування на кібершахрайство під керівництвом інсайдерів у банківському секторі; Бтоуш Е., Чжоу, Х., Гурураджан Р., Чан К.С., Тао Х. [9] узагальнюють огляд методів виявлення шахрайства з кредитними картками в банківській сфері для забезпечення кібербезпеки; Акінбоуале О.Е., Клінгельхофер Х.Е. і Зеріхун М.Ф. [10] аналізують вплив кіберзлочинності на банківський сектор за допомогою збалансованої системи показників, та ін.

Особливостям моделювання кібершахрайств та кібератак у різних галузях народного господарства присвячені роботи таких фахівців, як: Енгстрьом В. та Лагерстрьом Р. [11] досліджують різноманітні підходи до моделювання кібератак; Варгас П. та Тьєн І. [12] пропонують використання методології кількісної оцінки впливу сценаріїв ризику кібербезпеки в телекомунікаційних транспортних системах; Ан П., Ван З. і Чжан К. [13] анонсують змішану Гаусівську модель для виявлення кібератак; Джавед А., Лакоджу М., Бернап П. і Рана О. [14] роз'яснюють аналітику безпеки для прогнозування кібератак в реальному часі; Ахмаді А., Набіпур М., Мохаммаді-Іватлу Б. і Вахідінасаб В. [15] застосовують динамічне прогнозування під час кібератак., та ін.

Моделюванню кібершахрайств у банківських установах присвячені трактати таких дослідників, як: Годбол Т., Гочхайт С. і Гош Д. [16] пропонують розроблену платформу для вимірювання кіберстійкості поведінки співробітників на прикладі

індійського банку; Станікзай А.К. і Шах М.А. [**Помилка! Джерело посилання не знайдено.**] висвітлюють оцінку загроз кібербезпеці в банківських системах; Хорна К.Дж., Торо Л. та Регаладо-Пезуа О. [18] описують виявлення та інтерпретацію ризиків кібербезпеки банків, вразливість і ризики під час кібератак банківської установи; Шабір А., Шабір М., Джавед А.Р., Чакраборті К. і Різван М. [19] досліджують виявлення підозрілих транзакцій у банківських кібер-фізичних системах, та ін.

ПОСТАНОВКА ЗАВДАННЯ

Метою даного дослідження є здійснення аналізу математичних моделей протидії банківським кібершахрайствам, які можуть слугувати ефективними інструментами в процесі організації системи кіберзахисту банківської установи.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Узагальнюючи досвід роботи світових та вітчизняних банківських установ, зазначимо, що найпоширенішими видами кібершахрайств у банківських установах є:

- соціальна інженерія (шахрай вступає у безпосередній контакт з особою по телефону або електронною поштою з метою заволодіння необхідної конфіденційної інформації);
- онлайн-шахрайство (надання клієнтам привабливих пропозицій, при переході на посилання за якими на комп'ютер користувача таємно встановлюються шкідливі програми з метою злому комп’ютерної системи та крадіжки конфіденційної інформації);
- атаки інтернет-банкінгу (заволодіння особистими даними та доступів до онлайн-кабінетів, систем дистанційного обслуговування, систем 24/7, Клієнт-Банку для подальшого проведення нелегальних транзакцій, заволодіння коштами юридичних та фізичних осіб);
- потенційно небажані програми (різновид шкідливих програм, що можуть видаляти з системи особи чи банку необхідне програмне забезпечення, перенаправляти на необхідні пошукові системи, встановлювати завантаження певних програм, включати шпигунське програмне забезпечення);
- Android-трояни (представляють собою більш серйозну загрозу, ніж шкідливе програмне забезпечення, віруси-шифрувальники, шкідливі програми, бо він захоплює управління комп’ютерним засобом користувача, і надалі може користуватися всіма існуючими можливостями попереднього користувача для власної вигоди шахрая);
- фішингові листи (надсилання користувачам листів зі шкідливим вкладенням, URL-адресами підроблених сайтів, з метою отримати доступи до особистих облікових записів, комп'ютерів);
- DoS-атаки (використовуються для одночасного направлення на необхідний сайт банку великої кількості запитів із різних джерел, що перевантажує сайт величезним розміром трафіку, в наслідок чого виводить його з роботи, робить недоступним для реальних користувачів Інтернету);
- кібер-сталкінг (онлайн-переслідування, отримання безлічі онлайн-повідомлень, а також електронних листів неприємного змісту з метою залякування та примушення до здійснення фінансових злочинів);
- фармінг (різновид шахрайства, за яким на комп’ютерну техніку жертви завантажується шкідливий код, за допомогою якого замінюються дані за IP-адресами, внаслідок чого користувач автоматично перенаправляється на шахрайські, підроблені сайти);
- фейкові банківські інвестиційні проекти (фальшиві проекти), підроблені платіжні системи (фішингові сторінки, двійники платіжних систем, які схожі на справжні сторінки, при вході на які, користувач передає свої ідентифікаційні та особисті дані, в результаті чого злочинці отримують доступ);

• таргетовані посилання (підроблені сайти відомих банків), крадіжка облікових записів (отримання доступів до персональної інформації користувача);

• ботнети (мережі, що складаються зі зламаної комп'ютерної техніки і систем, що управляються віддаленими хакерами ззовні);

• заборонений чи незаконний контент (злочинці поширюють неприйнятний контент, що вважається вкрай неприємним та образливим з метою залякування чи виведення з психологічної рівноваги особи);

• набори експлойтів (використання шахраями готових інструментів – наборів помилок коду програмного забезпечення з метою отримання контролю над комп'ютерною технікою);

• скімінг (шахраї використовують для здійснення крадіжки грошових коштів спеціальні пристрої скімери - невеликі накладки на отвір, призначений для прийому банківської картки у банкоматі);

• ліванська петля (крадіжка банківської картки під час її відправлення до банкомату за допомогою спеціальних пристроїв, що розміщуються на отворі для прийому карток, які захоплюють пластикову карту, і потім не дають користувачеві дістати її з банкомату);

• інші.

Відповідно до розглянутих видів кібершахрайств, проведемо аналіз наявних моделей їх протидії. На наш погляд, цікавою є модель когнітивних обчислень та виявлення підозрілих транзакцій у банківських кіберфізичних системах на основі квантових обчислень у BCPS для постквантової ери [19]. Перевагами такої моделі є її надійність, ефективність, швидкість. Недоліками – ця методика знаходиться на стадії розробки, і в даний час системи, що базуються на контролі якості, не є доступними у банківській діяльності. Результатами моделі є демонстрація експоненційної пам'яті та обчислювальної потужності. Дана модель реалізується шляхом виконання ряду етапів:

Етап 1: Здійснення когнітивного моніторингу:

- фільтрація сенсорних стимулів;
- сенсорні введення із використанням буферу сенсорної пам'яті для обробки очних стимулів;
- сенсорна трансдукція – введення через рецептори, що спонукає потенціал дії.

Етап 2: Здійснення етапу моніторингу і етапу класифікації:

- перцептивно-асоціативна пам'ять: формула (1) показує перцептивну роздільність сенсорної модальності, тобто різноманітність сенсорних входів, а перцептивна незалежність – статистичний незалежний ефект, представлений формулою (2):

$$P(x|XiYi) = P(x|XiYi) \ldots = P(x|XiY1Y); \quad (1)$$

$$P(x,y|XiYj) = P(x|XiYj)P(y|XiYj), \quad (2)$$

де X, Y - параметри сенсорної модальності.

- посередник-агент, який допомагає зберігати сенсорну інформацію;
- база знань, як консолідоване сховище всіх знань;
- MetaPhor стадія – робоча пам'ять, де на основі когнітивної інтелектуальної поведінки системи відбувається класифікація транзакції як справжньої чи шахрайської. Реакцію метапізнання на запити користувача зображено формулою (3):

$$P(rc|XiYj,\Theta) \sim \eta(fc(XiYj),\Theta), \quad (3)$$

де $XiYi$ - запит користувача;

, - знак, що відноситься до розподілу;

ŋ - заповнювач розподілу ймовірностей.

Також використовується афінне перетворення для нелінійного перетворення; для гібридної мережі виконується стохастичний градієнтний спуск; застосовуються вагові матриці; використовується гомодинний оператор. В результаті отримується багатошарова модель.

Іншим підходом є прогнозне моделювання для виявлення шахрайства з банківськими картами за допомогою аналізу даних [20]. Така система моделювання використовується для виявлення шахрайства в режимі реального часу шляхом аналізу вхідних банківських транзакцій з платіжними картами. Вона передбачає проведення двох етапів для виявлення шахрайства:

1 етап. Розробка платформи для попередньої обробки даних.

2 етап. Розробка аналітичної моделі для прогнозування шахрайства (аналітична модель використовується для перевірки того, чи є вхідна транзакція законною чи ні). Використовуються дві моделі для класифікації виявлення шахрайства:

- логістична регресія є різновидом моделі імовірнісної статистичної класифікації, за якої для виявлення шахрайства використовується формула (4):

$$p = \frac{e^{(c_0 + c_1 x_1)}}{1 + e^{(c_0 + c_1 x_1)}}. \quad (4)$$

Логарифмічна функція може бути застосована до логістичної функції згідно формули (5):

$$loge\left(\frac{p}{1-p}\right), \quad (5)$$

де c_0, c_1 - коефіцієнти, які максимізують ймовірність вхідної транзакції;
p – ймовірність;

- дерево рішень. Використовується метод ID3 для побудови дерева рішень, при цьому враховуючи ентропію набору даних, а ентропія застосовується для вимірювання величини невизначеності в наборі даних. Ентропія різного стану визначається за формулою (6):

$$H(p_1, p_2 \dots p_s) = \sum_{i=1}^{s} \left(pilog\left(\frac{1}{pi}\right)\right), \quad (6)$$

де $p_1, p_2 \dots p_s$ - ймовірності атрибутів набору даних.

Перевагами такої моделі є її простота реалізації, зрозумілість, хороша працездатність. Недоліками – потрібний аналіз окремо кожного сценарію, і при виявленні шахрайства транзакція є сценарієм. Результатами моделі є адаптивність високого рівня, а також простота для розуміння та відображення.

Дерево рішень випадкового лісу - це більш вузька техніка, яка використовується для вирішення регресії та проблем класифікації. Для передбачення шахрайських транзакцій алгоритм випадкового лісу використовує певний псевдокод.

В межах дослідження варто розглянути використання алгоритму гармонійного пошуку в нейронних мережах для покращення виявлення шахрайства в банківській системі [21]. Тобто ця модель передбачає для виявлення шахрайських дій застосування гібридної системи, заснованої на методі штучної нейронної мережі (для виявлення шахрайства), а також алгоритмі пошуку гармонії (для оптимізації параметрів). Перевагами такої моделі є її спроможність до навчання на основі минулої поведінки, здатність виконувати правила, створювати код для використання в додатках реального часу. Недоліками – певні труднощі тривалої обробки великої кількості нейронних мереж, підтвердження структури, тривалого навчання, неадекватних можливостей

уточнення, складності в експлуатації та налаштуванні, великі витрати. Результатами моделі є оперативна швидкість виявлення, портативність, висока точність результатів.

Реалізація цієї моделі передбачає виконання ряду етапів:

1 етап:

- визначення вхідних даних;
- початкове оцінювання параметрів алгоритму пошуку гармонії;
- початкове оцінювання пам'яті гармонії випадковим чином;
- розрахунок пропорції кожної гармонії розв'язання пам'яті з використанням оцінки відповідної нейронної мережі;
- припинення;
- побудова нової гармонії та розрахунок її пропорції з використанням оцінки відповідної нейронної мережі;
- порівняння прецедентності нової гармонії з найгіршої гармонією в пам'яті;
- оновлення пам'яті про гармонію.

2 етап:

- визначення даних дослідження;
- початкове оцінювання параметрів нейронної мережі з використанням значень гармонії;
- дослідження нейронної мережі;
- тестування даних;
- оцінка точності нейронної мережі.

При цьому структуру нейронної мережі, що використовує пам'ять гармоній, можна зобразити у вигляді формули (7).

$$HM = \begin{bmatrix} x_1^1 & x_2^1 \cdots & x_n^1 \\ x_1^2 & x_2^2 \cdots & x_n^2 \\ \vdots & \vdots \cdots & \vdots \\ x_1^k & x_2^k \cdots & x_n^k \end{bmatrix} \begin{matrix} f(x^1) \\ f(x^2) \\ \vdots \\ f(x^k) \end{matrix}. \quad (7)$$

Особливої уваги заслуговує моделювання виявлення шахрайства з кредитними картками на базі використання двох типів моделей: під наглядом і без нагляду [22].

До моделей під наглядом (контрольованих моделей) відносять:

1) логістичну регресію – це регресійна модель, що дозволяє оцінити ймовірність категоричної відповіді на основі однієї або кількох змінних-предикторів. Математично зображується функцією множинної лінійної регресії (формула (8)):

$$Y_i = \beta_0 + \beta_1 x_{i,1} + \beta_2 x_{i,2} + \cdots \beta_p x_{i,p}, \quad (8)$$

де $x_{i,p}$ відноситься до р-ї предикторної змінної для і-го спостереження;

Y_i – результат і-го спостереження.

2) K-найближчі сусіди – у налаштуваннях класифікації алгоритм моделі передбачає формування більшості голосів серед K найбільш схожих екземплярів на таке «невидиме» спостереження, за якого подібність визначається відповідно до метрики відстані між двома точками даних x та x'. Така відстань може бути виражена евклідовою відстанню (формула (9)):

$$d(x, x') = \sqrt{(x_1 - x_1')^2 + (x_2 - x_2')^2 + \cdots + (x_n - x_n')^2}, \quad (9)$$

де x та x' – точки даних.

3) екстремальне підвищення градієнта - це потужний метод для розв’язання завдань регресії, класифікації, ранжування, що передбачає створення моделі прогнозування у формі комбінації менш сильних моделей прогнозування по типу дерева рішень. За цього методу використовується більш упорядкована формалізація моделі для

проведення контролю за досягненням кращої продуктивності заходів. Набір функцій, які використовуються в моделі, характеризуються формулою ():

$$L(\theta) = \sum_i l(y_i, \hat{y}_i) + \Omega(\theta), \quad (10)$$

де θ - вивчений набір параметрів;

l – диференційована опукла функція втрат, що вимірює різницю між передбаченням $\hat{y}_i$ та ціллю y_i;

Ω - член регуляризації.

До моделей без нагляду, неконтрольованих генеративних моделей для виявлення аномалій, відносять:

1) однокласна опорна векторна модель, яка дозволяє вивчати м'який кордон, щоб шляхом навчального набору дослідити нормальні елементи даних, після чого за допомогою тестового елементу даних, він налаштовується на встановлення аномалій, що не входять у межі досліджуваної області. Така модель має математичний вираз задачі оптимізації (формула (11)):

$$Minimize\ \Phi(w) = \frac{1}{2} w^T w + \frac{1}{vn} \sum_{i=1}^{n} \varepsilon_i - p; \quad (11)$$

2) обмежена модель Больцмана – модель, за якої розмежування ймовірностей отримується завдяки вивченню симетричних зв'язних вагів видимих і прихованих шарів. При чому умовна ймовірність описується формулою (12):

$$p(h|x) = \prod_i p(h_i|x), \quad (12)$$

де h - невідоме з використанням вхідних даних x.

А мінімізація негативної логарифмічної ймовірності досліджуваних даних виражається формулою (13):

$$L_{gen} = -\sum logP\big(x\big|(w_{ij}, b_i, c_j)\ \big), \quad (13)$$

де b_i, c_j - зміщення видимих і скритих шарів відповідно;

w_{ij} - ваги між даними видимих і скритих шарів.

3) генеративно-змагальні мережі – генеративна модель, що включає дві диференційовані функції, такі як генератор і дискримінатор, що подаються у вигляді нейронних наборів, одночасно конкурують і підлягають навчанню, і в загальному результаті призводять до того, що згенеровані вибори не можна відрізнити від реальних даних. Така модель виражається функцією оцінки (формулами 14, 15, 16):

$$A(x) = \alpha * L_G(x) + (1 - \alpha) L_D(x), \quad (14)$$

$$L_G(x) = \big\|x - G\big(E(x)\big)\big\|_1, \quad (15)$$

$$L_D(x) = \sigma\big(D\big(x, E(x)\big), 1\big), \quad (16)$$

де G – генератор;

D –дискримінатор;

α - ваговий параметр;

σ - крос-ентропійна втрата від дискримінатора x.

ВИСНОВКИ

Отже, фінансове шахрайство є однією з головних проблем, що підривають довіру клієнтів до банків та фінансових установ. А у двадцять першому столітті саме

кібершахрайство перетворилося у серйозну загрозу для фінансових установ, особливо для банківського сектору. Також важливим є встановлення джерел кібератак у сучасній банківській системі, оскільки це дозволить прогнозувати майбутні кібератаки, а також передчасно виявляти джерела кіберзагроз. Це можливо тільки за умови застосування потужного математичного інструментарію, який дозволить: проводити аналіз джерел кібератак банківської сфери; моделювати пріоритетні напрямки банківських кібершахрайств; в залежності від специфіки та особливостей кібератак ефективно виявляти кібернетичні атаки; оцінювати можливі сценарії потенційного кіберризику; показувати зміни, загрози, збитки на ринку банківських послуг; адаптувати поведінку банківського ринку до умов швидкого реагування на вплив найбільш потужних кібершахрайств; встановити напрямки скорочення кіберризиків банківських операцій. В свою чергу, запропоноване моделювання рейтингів кібершахрайств у банках забезпечить на практиці надійні функції кібербезпеки з низькими витратами на обслуговування платформ онлайн-банкінгу банківських установ, інтерфейси і параметри, що гнучко підлаштовуються, легко інтегруються до існуючих особливостей банківських систем для діючих програмних комплексів банків. В загальному підсумку все це сприятиме покращенню репутації банківської установи, збільшенню її прибутковості та підвищенню економічного зростання.

SUMMARY

Kuzmenko O., Yarovenko H., Skrynka L. ***Analysis of mathematical models for countering cyber fraud in banks.***

The article is devoted to the current topic of analysis of mathematical models for countering cyber fraud in banks. This problem is due to the security risks growth in the banking system, which are formed by fraudsters' cyberattacks and cybercrimes implementation. Therefore, the priority task for cyberbanking security is the application of modern mathematical methods to analyse the sources of cyber attacks, identify threats and losses in the banking services market, identify cyber-attacks and assess the scenario of potential cyber risk, etc. The article analyses the most widespread types of cyber fraud: social engineering, phishing, stalking, farming, DoS attacks, online fraud, potentially unwanted programs, etc. The study also considered a model of cognitive computing and detection of suspicious transactions in banking cyber-physical systems based on quantum computing in BCPS for the post-quantum era. The advantages, disadvantages and results of the model are defined. Predictive modelling is proposed to detect fraud in real-time by analysing incoming bank transactions with payment cards. Within the framework of this method, such models are used for the classification of fraud detection as logistic regression, a decision tree, and a narrower technique - a random forest decision tree. The study also considered using the harmonic search algorithm in neural networks to improve fraud detection in the banking system. It is found that although this model has the advantage of learning ability based on past behaviour, there are difficulties in the long-term processing of many neural networks. The stages of model implementation are also given. In addition, the modelling of credit card fraud detection is based on using two types of models: supervised and unsupervised. Supervised models include logistic regression, K-nearest neighbours, and extreme gradient boosting. The one-class support vector model, restricted Boltzmann model, and generative-competitive network are considered among uncontrolled generative models.

Keywords: *cyber fraud, banking system, cognitive computing model, predictive modelling, decision tree, neural network.*

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Naderi E., Pazouki S., Asrari A. A remedial action scheme against false data injection cyberattacks in smart transmission systems: Application of thyristor-controlled series capacitor (TCSC). *IEEE Transactions on Industrial Informatics.* 2022. Vol. 18, no. 4. P. 2297-2309. DOI: 10.1109/TII.2021.3092341.
2. Sun M., He L., Zhang J. Deep learning-based probabilistic anomaly detection for solar forecasting under cyberattacks. *International Journal of Electrical Power and Energy Systems*. 2022. Vol. 137, no. 107752. DOI: 10.1016/j.ijepes.2021.107752.
3. Acharya S., Mieth R., Konstantinou C., Karri R., Dvorkin Y. Cyber insurance against cyberattacks on electric vehicle charging stations. *IEEE Transactions on Smart Grid.* 2022. Vol. 13, no. 2. P. 1529-1541. DOI: 10.1109/TSG.2021.3133536.
4. Hou L., Li Y., Luo W., Sun H. Adaptive tracking control of switched cyber-physical systems with cyberattacks. *Applied Mathematics and Computation*. 2022. Vol. 415, no. 126721. DOI: 10.1016/j.amc.2021.126721.
5. Wang W., Harrou F., Bouyeddou B., Senouci S., Sun Y. A stacked deep learning approach to cyber-attacks detection in industrial systems: Application to power system and gas pipeline systems. *Cluster Computing.* 2022. Vol. 25, no. 1. P. 561-578. DOI: 10.1007/s10586-021-03426-w.
6. Eswaran S., Rani V., Daniel D., Ramakrishnan J., Selvakumar S. An enhanced network intrusion detection system for malicious crawler detection and security event correlations in ubiquitous banking infrastructure.

International Journal of Pervasive Computing and Communications. 2022. Vol. 18, no. 1. P. 59-78. DOI: 10.1108/IJPCC-04-2021-0102.

7. Tsai C.-H., Su P.-C. The application of multi-server authentication scheme in internet banking transaction environments. *Information Systems and e-Business Management*. 2021. Vol. 19, no. 1. P. 77-105. DOI: 10.1007/s10257-020-00481-5.

8. Chhabra Roy N., Prabhakara, S. Sustainable response system building against insider-led cyber frauds in banking sector: A machine learning approach. *Journal of Financial Crime*. 2022. DOI: 10.1108/JFC-12-2021-0274.

9. Btoush E., Zhou X., Gururajan R., Chan K. C., Tao X. A survey on credit card fraud detection techniques in banking industry for cyber security. Paper presented at the *Proceedings of 2021 8th IEEE International Conference on Behavioural and Social Computing, BESC 2021*. 2021. DOI: 10.1109/BESC53957.2021.9635559.

10. Akinbowale O. E., Klingelhöfer H. E., Zerihun M. F. Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime.* 2020.Vol. 27, no. 3. P. 945-958. DOI: 10.1108/JFC-03-2020-0037.

11. Engström V., Lagerström R. Two decades of cyberattack simulations: A systematic literature review. *Computers and Security*. 2022. Vol. 116, no. 102681. DOI: 10.1016/j.cose.2022.102681.

12. Vargas P., Tien I. Methodology to quantitatively assess impacts of 5G telecommunications cybersecurity risk scenarios on dependent connected urban transportation systems. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*. 2022. Vol. 8, no. 2. DOI: 10.1061/AJRUA6.0001220.

13. An P., Wang Z., Zhang C. Ensemble unsupervised autoencoders and gaussian mixture model for cyberattack detection. *Information Processing and Management*. 2022. Vol. 59, no. 2. DOI: 10.1016/j.ipm.2021.102844.

14. Javed A., Lakoju M., Burnap P., Rana O. Security analytics for real-time forecasting of cyberattacks. *Software - Practice and Experience*. 2022. Vol. 52, no. 3. P. 788-804. DOI: 10.1002/spe.2822.

15. Ahmadi A., Nabipour M., Mohammadi-Ivatloo B., Vahidinasab V. Ensemble learning-based dynamic line rating forecasting under cyberattacks. *IEEE Transactions on Power Delivery*. 2022. Vol. 37, no. 1. P. 230-238. DOI: 10.1109/TPWRD.2021.3056055.

16. Godbole T., Gochhait S., Ghosh D. Developing a framework to measure cyber resilience behaviour of indian bank employees. Paper presented at the *ICT with Intelligent Applications. Proceedings of ICTIS 2021*. 2021. Vol. 1. DOI: 10.1007/978-981-16-4177-0_31.

17. Stanikzai A. Q., Shah M. A. Evaluation of cyber security threats in banking systems. Paper presented at the *2021 IEEE Symposium Series on Computational Intelligence, SSCI 2021 – Proceedings*. 2021. DOI: 10.1109/SSCI50451.2021.9659862.

18. Horna C. J., Toro L., Regalado-Pezua O. Silver bank: Vulnerability and risks during cyberattacks. *Emerald Emerging Markets Case Studies.* 2022. Vol. 12, no. 1. P. 1-33. DOI: 10.1108/EEMCS-02-2021-0034.

19. Shabbir A., Shabir M., Javed A. R., Chakraborty C., Rizwan M. Suspicious transaction detection in banking cyber-physical systems. *Computers and Electrical Engineering*. 2022. Vol. 97. DOI: 10.1016/j.compeleceng.2021.107596.

20. Patil S., Nemade V., Soni P. K. Predictive modelling for credit card fraud detection using data analytics. Paper presented at the *Procedia Computer Science*. 2018. Vol. 132. P. 385-395. DOI: 10.1016/j.procs.2018.05.199.

21. Daliri S. Using harmony search algorithm in neural networks to improve fraud detection in banking system. *Computational Intelligence and Neuroscience*. *2020*. Vol. 2020, no. 6503459. DOI: 10.1155/2020/6503459.

22. Niu X., Wang L., Yang X. A Comparison Study of Credit Card Fraud Detection: Supervised versus Unsupervised. *arXiv preprint arXiv*: 1904.10604 (2019). DOI: 10.48550/arXiv.1904.10604.

REFERENCES

1. Naderi, E., Pazouki, S., & Asrari, A. (2022). A remedial action scheme against false data injection cyberattacks in smart transmission systems: Application of thyristor-controlled series capacitor (TCSC). *IEEE Transactions on Industrial Informatics*, 18(4), pp. 2297-2309. DOI: 10.1109/TII.2021.3092341.

2. Sun, M., He, L., & Zhang, J. (2022). Deep learning-based probabilistic anomaly detection for solar forecasting under cyberattacks. *International Journal of Electrical Power and Energy Systems*, 137, no. 107752. DOI: 10.1016/j.ijepes.2021.107752.

3. Acharya, S., Mieth, R., Konstantinou, C., Karri, R., & Dvorkin, Y. (2022). Cyber insurance against cyberattacks on electric vehicle charging stations. *IEEE Transactions on Smart Grid*, 13(2), pp. 1529-1541. DOI: 10.1109/TSG.2021.3133536.

4. Hou, L., Li, Y., Luo, W., & Sun, H. (2022). Adaptive tracking control of switched cyber-physical systems with cyberattacks. *Applied Mathematics and Computation*, 415, no. 126721. DOI: 10.1016/j.amc.2021.126721.

5. Wang, W., Harrou, F., Bouyeddou, B., Senouci, S., & Sun, Y. (2022). A stacked deep learning approach to cyber-attacks detection in industrial systems: Application to power system and gas pipeline systems. *Cluster Computing*, 25(1), pp. 561-578. DOI: 10.1007/s10586-021-03426-w.

6. Eswaran, S., Rani, V., Daniel, D., Ramakrishnan, J., & Selvakumar, S. (2022). An enhanced network intrusion detection system for malicious crawler detection and security event correlations in ubiquitous banking infrastructure. *International Journal of Pervasive Computing and Communications*, 18(1), pp. 59-78. DOI: 10.1108/IJPCC-04-2021-0102.

7. Tsai, C.-H., & Su, P.-C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. *Information Systems and e-Business Management*, 19(1), pp. 77-105. DOI: 10.1007/s10257-020-00481-5.

8. Chhabra Roy, N., & Prabhakaran, S. (2022). Sustainable response system building against insider-led cyber frauds in banking sector: A machine learning approach. *Journal of Financial Crime*. DOI: 10.1108/JFC-12-2021-0274.

9. Btoush, E., Zhou, X., Gururajan, R., Chan, K. C., & Tao, X. (2021). A survey on credit card fraud detection techniques in banking industry for cyber security. Paper presented at the *Proceedings of 2021 8th IEEE International Conference on Behavioural and Social Computing, BESC 2021*. DOI: 10.1109/BESC53957.2021.9635559.

10. Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime,* 27(3), pp. 945-958. DOI: 10.1108/JFC-03-2020-0037.

11. Engström, V., & Lagerström, R. (2022). Two decades of cyberattack simulations: A systematic literature review. *Computers and Security,* no. 102681. DOI: 10.1016/j.cose.2022.102681.

12. Vargas, P., & Tien, I. (2022). Methodology to quantitatively assess impacts of 5G telecommunications cybersecurity risk scenarios on dependent connected urban transportation systems. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, 8(2). DOI: 10.1061/AJRUA6.0001220.

13. An, P., Wang, Z., & Zhang, C. (2022). Ensemble unsupervised autoencoders and gaussian mixture model for cyberattack detection. *Information Processing and Management,* 59(2). DOI: 10.1016/j.ipm.2021.102844.

14. Javed, A., Lakoju, M., Burnap, P., & Rana, O. (2022). Security analytics for real-time forecasting of cyberattacks. *Software - Practice and Experience*, 52(3), pp. 788-804. DOI: 10.1002/spe.2822.

15. Ahmadi, A., Nabipour, M., Mohammadi-Ivatloo, B., & Vahidinasab, V. (2022). Ensemble learning-based dynamic line rating forecasting under cyberattacks. *IEEE Transactions on Power Delivery*, 37(1), pp. 230-238. DOI: 10.1109/TPWRD.2021.3056055.

16. Godbole, T., Gochhait, S., & Ghosh, D. (2022). Developing a framework to measure cyber resilience behaviour of indian bank employees. Paper presented at the *ICT with Intelligent Applications. Proceedings of ICTIS 2021*. DOI: 10.1007/978-981-16-4177-0_31.

17. Stanikzai, A. Q., & Shah, M. A. (2021). Evaluation of cyber security threats in banking systems. Paper presented at the *2021 IEEE Symposium Series on Computational Intelligence, SSCI 2021 – Proceedings.* DOI: 10.1109/SSCI50451.2021.9659862.

18. Horna, C. J., Toro, L., & Regalado-Pezua, O. (2022). Silver bank: Vulnerability and risks during cyberattacks. *Emerald Emerging Markets Case Studies*, 12(1), pp. 1-33. DOI: 10.1108/EEMCS-02-2021-0034.

19. Shabbir, A., Shabir, M., Javed, A. R., Chakraborty, C., & Rizwan, M. (2022). Suspicious transaction detection in banking cyber-physical systems. *Computers and Electrical Engineering,* 97. DOI: 10.1016/j.compeleceng.2021.107596.

20. Patil, S., Nemade, V., & Soni, P. K. (2018). Predictive modelling for credit card fraud detection using data analytics. Paper presented at the *Procedia Computer Science*, 132, pp. 385-395. DOI: 10.1016/j.procs.2018.05.199.

21. Daliri, S. (2020). Using harmony search algorithm in neural networks to improve fraud detection in banking system. *Computational Intelligence and Neuroscience*, 2020, no. 6503459. DOI: 10.1155/2020/6503459.

22. Niu, X., Wang, L., & Yang, X. (2019). A comparison study of credit card fraud detection: Supervised versus unsupervised. *arXiv preprint arXiv*: 1904.10604. DOI: 10.48550/arXiv.1904.10604.