Електронне наукове фахове видання "**Ефективна економіка**" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)
www. economy.nayka.com. ua | № 7, 2018

УДК 303.09:336.717.1

*Г. М. Яровенко,*
*к. е. н., доцент, доцент кафедри економічної кібернетики,*
*Навчально-науковий інститут бізнес-технологій «УАБС»*
*Сумського державного університету*
*А. І. Сковронська,*
*магістр економічної кібернетики,*
*Навчально-науковий інститут бізнес-технологій «УАБС»*
*Сумського державного університету*
*М. М. Бояджян,*
*магістрант кафедри економічної кібернетики,*
*Навчально-науковий інститут бізнес-технологій «УАБС»*
*Сумського державного університету*

# МОДЕЛЮВАННЯ ВИЯВЛЕННЯ ОЗНАК КІБЕРЗАГРОЗ В БАНКАХ ІЗ ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ

*H. Yarovenko*
*Ph.D., Associate Professor, Associate Professor of the Economic Cybernetics Department,*
*Educational and Scientific Institute of Business Technologies "UAB" of*
*Sumy State University, Sumy*
*A. Skovronska*
*master of Economic Cybernetics,*
*Educational and Scientific Institute of Business Technologies "UAB" of*
*Sumy State University, Sumy*
*M. Boiadzhian*
*graduate student of the Economic Cybernetics Department,*
*Educational and Scientific Institute of Business Technologies "UAB" of*
*Sumy State University, Sumy*

## MODELING THE DETECT SIGNS OF THE CYBER THREATS IN THE BANKS WITH USING DATA MINING

*Стаття присвячена актуальній проблемі боротьби із кіберзагрозами в банківській сфері. Автори пропонують використовувати методи інтелектуального аналізу для оперативного виявлення операцій, які мають ознаки кіберзагрози. Найбільш поширеними є загрози, які класифікують, як соціальну інженерію. Авторами було висунуто ряд гіпотез стосовно вірогідності виникнення ознак кіберзагроз саме такого напрямку. На ймовірність того, що операція має ознаки загрози, впливає факт: обнуління сум рахунків в результаті транзакцій; тип транзакції; тип пристрою – мобільний банкінг або Інтернет банкінг; місцеположення клієнта, який здійснює операцію. Використовуючи сформовані гіпотези, було обрано вхідні показники для моделювання: сума транзакції, тип пристрою, місцеположення в процесі транзакції, місцеположення при реєстрації, баланс після транзакції, баланс до здійснення транзакції, тип транзакції. Набір даних*

*сформовано на основі 2.000.000 спостережень Сумського банку. Для побудови моделі було використано логіт-регресію, нейронну мережу і дерево рішень. Модель реалізовано із використанням аналітичного пакету «SAS Enterprice Miner». Результатом дослідження є математична модель для визначення ймовірності ознаки кіберзагрози під час проведення транзакцій користувачами мобільного та інтернет-банкінгу.*

*The article is devoted to the actual problem of the fight against cyber threats in the banking sector. The authors suggest using the methods of data mining for the rapid detection of operations that have signs of cyber threats. The most common are threats that are classified as social engineering. The authors put forward several hypotheses about the potential signs of cyber threats in this area. If an operation has signs of cyber treats, such facts affected on the probability: zeroing of account amounts as a result of transactions; transaction type; type of device - mobile banking or Internet banking; the location of the client who carries out the transaction. The input parameters for modeling were selected using the formed hypothesis: transaction amount, device type, transaction location, registration location, post-transaction balance, balance before the transaction, transaction type. The data set is based on the 2.000.000 observations of one Sumy Bank. Logistic regression, neural network and decision tree were used to construct the model. The model is implemented by using an analytical package «SAS Enterprise Miner». The result of the research is the mathematical model for determining the probability of cyber threats signs during transactions by users of mobile and Internet banking.*

***Ключові слова:*** *кіберзагроза, моделювання, інтелектуальний аналіз, логістична регресія, нейрона мережа, дерево рішень, «SAS Enterprice Miner», банк.*

***Keywords:*** *cyber threats, modeling, Data Mining, logistic regression, neural network, decision tree, «SAS Enterprice Miner», bank.*

**Постановка проблеми.** Сьогодні досить актуальною проблемою, яка призводить до негативних економічних та соціальних наслідків, є проблема боротьби із кіберзагрозами. З кожним роком результати їх впливу набирають значного масштабу, завдаючи шкоди банківській системі країни, окремим громадянам, економіці країни в цілому. Зростання рівня інформаційних технологій впливає на те, що банківська система частіше всього не встигає за модернізацією системи кібербезпеки, що впливає на появу вразливих місць. Це призводить до збільшення фінансових втрати банків та їх клієнтів від кібератак.

Що ж таке кіберзагрози? Їх визначають, як наявні або потенційно можливі явища та чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних систем [1].

Серед найпоширеніших кіберзагроз в банках виділяють:

а) соціальну інженерію, яка представляє собою здійснення фішингових та вішингових атак та яка найбільш поширеною на сьогодні.

Фішинг – це шахрайство через Інтернет шляхом отримання клієнтом підроблених електронних листів, які використовуються для отримання доступу до їх рахунків або отримання особистої інформації. Станом на кінець першого кварталу 2017 року найбільшої шкоди від фішингових атак зазнали 51,70% банків. До країн з найвищим відсотком нападу на користувачів відносяться: Китай (20,87%), Бразилія (19,16%), Макао (11,94%), Російська Федерація (11,29%) , Австралія (10,73%), Аргентина (10,42%), Нова Зеландія (10,18%), Катар (9,87%), Казахстан (9,61%), Тайвань (9,27%) [2].

Вішинг – телефонне шахрайство, пов'язане з виманюванням реквізитів банківських карток або іншої конфіденційної інформації, примушуванням до переказу коштів на картку злодіїв. У 2017 році за часткою атакованих користувачів до найбільш атакованих країн відносяться: Росія (1,2%), Україна (0,4%), Узбекистан (0,40%), Казахстан (0,36%), Таджикистан (0,35%), Туреччина (0,34%), Молдова (0,31%), Україна (0,29%), Киргизстан (0,27%), Білорусь (0,26%) та Латвія (0,23%) [2].

б) атаки мережевого та прикладного рівнів: DoS – хакерська атака на обчислювальну систему з метою довести її до відмови; DDoS – широкомасштабна координована атака на надання послуг системи жертви або мережевих ресурсів; розрив або призупинення серверів та мережевих ресурсів, підключених до Інтернету;

в) розвинені стійкі загрози (APT - AdvancedPersistentThreats): «Backdoor» – вразливість в програмі, що дозволяє хакерам зламати систему або здійснити будь-яку недружелюбну дію; шкідливий код, за допомогою якого нападники залишаються непоміченими в системі;

г) організовану кіберзлочинність: розкрадання інтелектуальної власності, конфіскація банківських рахунків та втрата споживачів внаслідок бізнес-збоїв; продаж особистої інформації на чорному ринку;

д) порушення основних даних: викрадання даних клієнтів та їх продаж; розкриття конфіденційної інформації про банківські установи та їх клієнтів. [3]

Проблема боротьби з кіберзагрозами в банківській сфері – це не тільки проблема в Україні, але вона носить світовий характер. Особливо це актуально в частині боротьби із соціальною інженерією. Через те, що банки не можуть гарантувати захист своїм клієнтам, рівень їх довіри до банків, як до фінансових інститутів, зменшується. Тому банкам потрібні нові методи боротьби з цим явищем, які б дозволяли оперативно відслідковувати та визначати, чи має дана операція ознаки кіберзагрози чи ні. Для швидкого відстеження та попередження кіберзагроз банкам необхідно використовувати математичний інструментарій, особливо інтелектуальний аналіз (Data Mining), у поєднанні з інформаційними технологіями. Тільки така комбінація заходів дозволить системі налаштовуватися до зміни умов та реагувати на відхилення. Тому дана стаття й присвячена розробці математичного інструментарію для виявлення ознак кіберзагроз.

**Аналіз останніх досліджень і публікацій.** Питанню моделювання в банківській сфері приділено багато уваги в працях зарубіжних та вітчизняних вчених. Але проблема, пов'язана із використанням математичних методів для виявлення ознак кіберзагроз для банківських операцій, висвітлена недостатньо.

В таблиці 1 систематизовано підходи до математичного моделювання, які використовувалися у наукових працях вітчизняних та закордонних науковців для вирішення проблем у банках.

**Таблиця 1.**
**Підходи до моделювання у банківській сфері**

| № за/п | П.І.П. науковців | Підходи до моделювання |
|---|---|---|
| Українські дослідники та науковці | | |
| 1 | Вітлінський В.В., Великоіваненко Г. І. | Мікроекономічне моделювання |
| 2 | Козак О.Ю. | Динамічне моделювання |
| 3 | Костіна Н.І., Антонов В.М., Ганах Н.І. | Ймовірнісна-автоматна модель |
| 4 | Нікітін А.В. | Ситуаційне моделювання |
| 5 | Примостка Л.О. | Банківський аналіз |
| Закордонні дослідники та науковці | | |
| 6 | J. Poveda Poveda and J. Turmo Borras;<br>B. Klemens;<br>J. Stanton;<br>M. J. Zaki and W. Meira | Фундаментальні концепції та алгоритми інтелектуального аналізу |
| 7 | А. Барсегян;<br>М. Купріянов, В. Степаненко, І. Холод;<br>Н. Паклін, В. Орешков | Методи та моделі аналізу даних, базові алгоритми Data Mining |
| 8 | Грибов А.Ф. | Оптимізаційні, виробничо-організаційні, стохастичні, динамічні моделі |
| 9 | Муханов Л.Е. | Нейронні мережі, методи кластеризації, оптимізації, теорія графів |
| 10 | Селянин В.Е. | Нечіткі нейронні мережі, байесівський аналіз |

Інтелектуальний аналіз є найбільш поширеним методом дослідження у випадках аналізу великих масивів даних. Так, на його застосування в галузі виявлення шахрайств та кіберзагроз припадає 21,8%, що робить його досить популярним засобом знаходження помилок, незаконних операцій, маніпуляцій з інформацією [4]. Його ефективність є достатньо високою, тому для моделювання виявлення ознак кіберзагроз доцільно обрати саме цей метод.

**Мета статті** полягає у побудові математичних моделей для виявлення ознак кіберзагроз під час проведення транзакцій банківськими клієнтами та її практичній реалізації із використанням методів інтелектуального аналізу за допомогою аналітичного пакету SAS EnterpriseMiner.

**Виклад основного матеріалу дослідження.** Для побудови моделі було висунуто ряд гіпотез стосовно вірогідності виникнення ознак кіберзагроз під час проведення транзакцій користувачами мобільного та інтернет-банкінгу. Виходячи з аналізу статистичних даних виділимо показники, що можуть вказувати на можливе виникнення кіберзагрози в процесі виконання банківської операції [5]:

1) транзакція має ознаки кіберзагрози, якщо її ініційовано на території іншої країни. В більшості банків прийнята практика необхідності повідомлення банка клієнтом про його виїзд за кордон та зазначення країн, які будуть відвідані. В іншому випадку служба безпеки банку може заблокувати карту, якщо по ній будуть ініційовано транзакції з іншої країні. Це пов'язано з тим, що хакери, зламуючи доступ до мобільного або інтернет-банкінгу та привласнюючи чужі кошти, застосовують спеціальні програми для шифрування їх місцеположення;

2) на ймовірність виникнення кіберзагрози впливає тип пристрою, з якого виконувалась транзакція. Існують різні способи злому мобільних пристроїв та комп'ютерів, завдяки яким зловмисники з

легкістю отримують доступ до мобільного та інтернет-банкінгу користувачів банківських послуг. Також банк не в змозі контролювати, хто є користувачем та де він користується пристроєм. Частіше за все такі операції можуть містити ознаки кіберзагроз;

3) тип проведеної транзакції впливає на ймовірність виникнення ознак кіберзагрози. Широке коло типів банківських транзакцій сприяє впровадженню нових заходів з боку зловмисників, направлених на заволодіння чужими коштами та порушення безпеки інформації в банку;

4) обнуління рахунків клієнтів банку вказує на ймовірні ознаки кіберзагроз. Сьогодні досить розповсюдженими є безготівкові розрахунки, коли платежі відбуваються без використання готівкових коштів. Тому, в більшості випадків на банківському рахунку людини завжди присутня певна сума коштів. Якщо під час транзакції зі зняття всієї суми можливо має місце ознака порушення користування рахунком або несанкціоноване зняття коштів.

З урахуванням означених гіпотез обрано вхідні та вихідні показники для моделювання, опис яких представлено в таблиці 2. Набір вхідних та вихідних змінних сформовано на основі 2.000.000 спостережень Сумського банку «А», назва якого не зазначається з урахуванням принципів комерційної таємниці.

**Таблиця 2.**
**Опис вхідних та вихідних змінних**

| Ім'я змінної | Економічний зміст | Роль | Тип | Допустимі значення |
|---|---|---|---|---|
| isfraud (*Y*) | Випадки виникнення кіберзагроз | цільова | binary | 1 – виявлено ознаки кіберзагроз<br>0 – ознак кіберзагроз не виявлено |
| amount ($X_1$) | Загальна сума, що проходила в транзакціях | вхідна | interval | >=0 |
| devicetype ($X_2$) | Тип пристрою, з якого виконувалась транзакція | вхідна | nominal | M – мобільний банкінг<br>I – інтернет банкінг |
| factlocation ($X_3$) | Ініційоване місцеположення пристрою, з якого проводилась транзакція | вхідна | nominal | UA – Україна<br>Other – інша країна |
| location ($X_4$) | Місцеположення, вказане при реєстрації клієнта банкінгу | вхідна | nominal | UA – Україна |
| newbalance ($X_5$) | Баланс клієнта після проведення транзакції | вхідна | interval | >=0 |
| oldbalance ($X_6$) | Баланс клієнта до проведення транзакції | вхідна | interval | >=0 |
| type ($X_7$) | Тип виконаної транзакції | вхідна | nominal | CASH_IN – поповнення коштів<br>CASH_OUT – зняття коштів<br>DEBIT – списання коштів з рахунку<br>PAYMENT – проведення оплати<br>TRANSFER – переведення коштів |

Враховуючи обрані змінні, дані та висунуті гіпотези було розроблено концептуальну модель виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу (рис. 1).


**Рис. 1. Концептуальна модель виявлення ознак кіберзагроз в банківських транзакціях**

На першому кроці реалізації концептуальної моделі було проведено первинний аналіз, де було зроблено перевірку інтервальних вхідних змінних на відповідність нормальному закону розподілу. Оскільки гіпотеза не підтвердилася, було проведено трансформацію вхідних змінних шляхом їх логарифмування.

На наступному кроці було обрано такі методи інтелектуального аналізу, як логіт-регресія, дерево рішень та нейронна мережа. Даний вибір обумовлено тим, що дані методи є досить ефективними для оцінки ймовірності. Побудову моделей було виконано за допомогою аналітичного пакету "SAS Enterprise Miner" [6].

В результаті побудови логіт-регресії отримано результати оцінки, представлені на рисунку 2.

Output

Analysis of Maximum Likelihood Estimates

| Parameter | | DF | Estimate | Standard Error | Wald Chi-Square | Pr > ChiSq | Standardized Estimate | Exp(Est) |
|---|---|---|---|---|---|---|---|---|
| Intercept | | 1 | -3.4043 | 0.3518 | 93.65 | <.0001 | | 0.033 |
| LOG_newbalance | | 1 | -0.8950 | 0.0910 | 96.66 | <.0001 | -3.1280 | 0.409 |
| LOG_oldbalance | | 1 | 0.8738 | 0.0846 | 106.81 | <.0001 | 2.7445 | 2.396 |
| factlocation | Other | 1 | 5.1102 | 0.2700 | 358.11 | <.0001 | | 165.707 |

**Рис. 2. Результати оцінки параметрів логіт-регресії**

У результаті покрокового відбору було обрано 3 значущі фактори:

1) ініційоване місцеположення пристрою, з якого проводилась транзакція (інша країна) ($X_{3.2}$);
2) баланс клієнта після проведення транзакції ($X_5$);
3) баланс клієнта до проведення транзакції ($X_6$).

Розраховані значення ймовірності < 0,0001, що свідчить про високу статистичну значущість параметрів регресії. Використовуючи отримані значення, побудовано математичну модель логіт-регресії для оцінки вірогідності виникнення ознак кіберзагроз під час проведення транзакцій користувачами мобільного та інтернет-банкінгу (формула 1):

$$1 + E^{-(-3{,}4+5{,}11X_{3.2}-0{,}89X_5+0{,}87X_6)}) \quad (1)$$

Отже, ймовірність того, що банківська транзакція буде мати ознаки кіберзагрози, зростає із присутністю зафіксованого факту проведення транзакції в іншій країні, з великим значенням балансу до проведення транзакції та зменшується із великим значенням балансу після проведення транзакції.

На наступному кроці побудовано трирівневе дерево рішення (рис. 3).

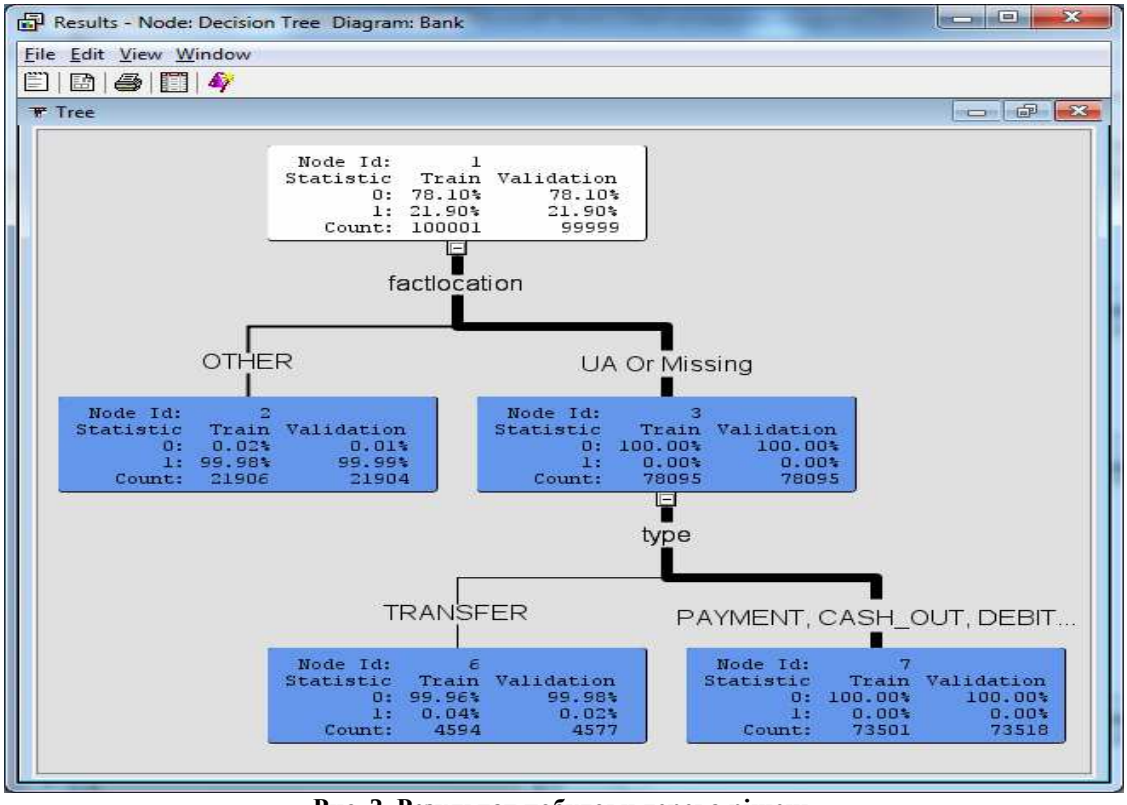


**Рис. 3. Результат побудови дерева рішень**

З побудованої діаграми дерева рішень (рис. 3) видно, що найбільш вагомий фактор – це ініційоване місцеположення пристрою, з якого виконувалась транзакція. Після нього за важливістю є тип операції, який здійснював клієнт банку.

Таким чином, найімовірніше виконана транзакція не містить ознак кіберзагроз, якщо фіксоване місцеположення виконання транзакції клієнтом банкінгу – Україна. А також з'ясовано, що безпечними для користувачів на випадок наявності ознак кіберзагрози є наступні типи операцій: поповнення та зняття коштів, списання коштів з рахунку та проведення оплати.

На наступному кроці побудовано нейронну мережу. Результатом є мережа, яка складається з 1-го прихованого шару з двома нейронами (рис. 4).

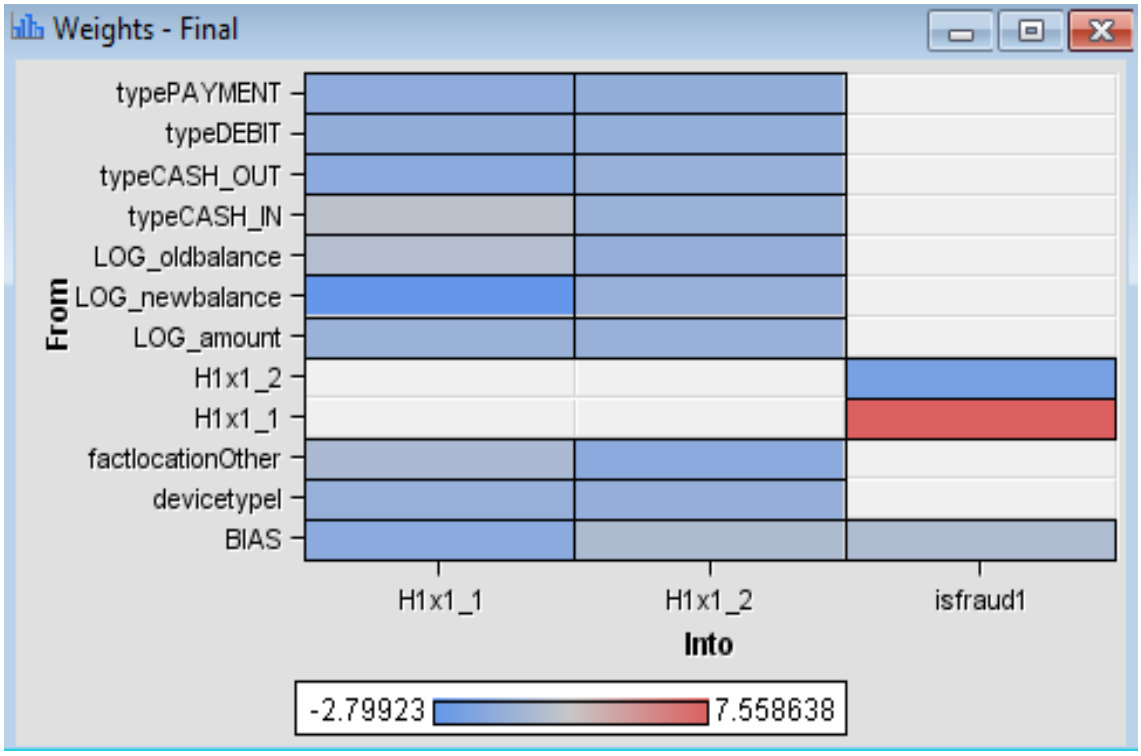


**Рис. 4. Архітектура побудованої нейронної мережі**

Отримані вагові коефіцієнти нейронної мережі представлено на рисунку 5.

Table: Weights - Final

| Label | From | Into | Weight |
|---|---|---|---|
| LOG_amount -> H1x1_1 | LOG_amount | H1x1_1 | 0.044417 |
| LOG_newbalance -> H1x1_1 | LOG_newbalance | H1x1_1 | -2.79923 |
| LOG_oldbalance -> H1x1_1 | LOG_oldbalance | H1x1_1 | 1.360785 |
| LOG_amount -> H1x1_2 | LOG_amount | H1x1_2 | -0.05355 |
| LOG_newbalance -> H1x1_2 | LOG_newbalance | H1x1_2 | -0.11025 |
| LOG_oldbalance -> H1x1_2 | LOG_oldbalance | H1x1_2 | -0.25139 |
| devicetypeI -> H1x1_1 | devicetypeI | H1x1_1 | -0.13465 |
| factlocationOther -> H1x1_1 | factlocationOther | H1x1_1 | 0.867504 |
| typeCASH_IN -> H1x1_1 | typeCASH_IN | H1x1_1 | 1.775061 |
| typeCASH_OUT -> H1x1_1 | typeCASH_OUT | H1x1_1 | -0.75885 |
| typeDEBIT -> H1x1_1 | typeDEBIT | H1x1_1 | -0.34715 |
| typePAYMENT -> H1x1_1 | typePAYMENT | H1x1_1 | -0.57974 |
| devicetypeI -> H1x1_2 | devicetypeI | H1x1_2 | -0.23464 |
| factlocationOther -> H1x1_2 | factlocationOther | H1x1_2 | -0.78262 |
| typeCASH_IN -> H1x1_2 | typeCASH_IN | H1x1_2 | 0.048199 |
| typeCASH_OUT -> H1x1_2 | typeCASH_OUT | H1x1_2 | -0.0721 |
| typeDEBIT -> H1x1_2 | typeDEBIT | H1x1_2 | -0.30449 |
| typePAYMENT -> H1x1_2 | typePAYMENT | H1x1_2 | -0.39577 |
| BIAS -> H1x1_1 | BIAS | H1x1_1 | -0.77711 |
| BIAS -> H1x1_2 | BIAS | H1x1_2 | 0.991864 |
| H1x1_1 -> isfraud1 | H1x1_1 | isfraud1 | 7.558638 |
| H1x1_2 -> isfraud1 | H1x1_2 | isfraud1 | -1.75976 |
| BIAS -> isfraud1 | BIAS | isfraud1 | 1.022777 |

**Рис. 5. Вагові коефіцієнти нейронної мережі**

Математичну інтерпретацію отриманої нейронної мережі наведено у формулах 2-4:

$$Y = 1{,}02 + 7{,}56 \cdot H_1 x_1 - 1{,}76 \cdot H_2 x_2; \quad (2)$$

$$H_1 = \tanh(-0{,}78 + 0{,}04 \cdot LOGX_1 - 0{,}13 \cdot X_{2.2} + 0{,}87 \cdot X_{3.2} - 2{,}8 \cdot LOGX_5 + 1{,}36 \cdot LOGX_6 + 1{,}78 \cdot X_{7.1} - 0{,}76 \cdot X_{7.2} - 0{,}35 \cdot X_{7.3} - 0{,}58 \cdot X_{7.4}); \quad (3)$$

$$H_2 = \tanh(0{,}99 - 0{,}05 \cdot LOGX_1 - 0{,}23 \cdot X_{2.2} - 0{,}78 \cdot X_{3.2} - 0{,}11 \cdot LOGX_5 - 0{,}25 \cdot LOGX_6 + 0{,}05 \cdot X_{7.1} - 0{,}07 \cdot X_{7.2} - 0{,}3 \cdot X_{7.3} - 0{,}4 \cdot X_{7.4}). \quad (4)$$

Отримана нейронна мережа показує, що на ймовірність того, що банківська транзакція буде мати ознаки кіберзагрози, впливає: місцеположення пристрою, з якого проводилась транзакція – інша країна ($X_{3.2}$); баланс клієнта після проведення транзакції ($X_5$) та до проведення ($X_6$); загальна сума транзакції ($X_1$); тип пристрою – Інтернет-банкінг ($X_{2.2}$); типи транзакцій – поповнення коштів ($X_{7.1}$), зняття коштів ($X_{7.2}$), списання коштів з рахунку ($X_{7.3}$), проведення оплати ($X_{7.4}$).

Для вибору найбільш точної моделі використано частку неправильної класифікації та середньоквадратичної похибки (табл. 3).

**Таблиця 3.**
**Порівняльна характеристика моделей**

| № з/п | Модель | Частка неправильної класифікації (Misclassification Rate, MISC) | | Середньоквадратична похибка (Mean Square Error, MSE) | |
|---|---|---|---|---|---|
| | | Валідаційна | Навчальна | Валідаційна | Навчальна |
| 1 | Нейронна мережа | 0,00002 | 0,00005 | 0,001094 | 0,001105 |
| 2 | Дерево рішень | 0,00003 | 0,00009 | 0,001097 | 0,001112 |
| 3 | Логіт-регресія | 0,00003 | 0,0001 | 0,001091 | 0,001119 |

Моделі, представлені в таблиці 3, розташовані від найкращої до найгіршої за кількісними оцінками частки неправильної класифікації та середньоквадратичної похибки. Модель тим краще описує набір даних, чим менші значення цих показників. Найточнішою моделлю виявилась нейронна мережа, оскільки її

представлені показники мають найнижчі значення. Інші моделі є також досить точними – їх значення наближаються до 0.

Результат розрахованих значень коефіцієнтів підкріплюється графіками ROC-кривих. На рисунку 6 відображено ROC-криві для навчального та валідаційного наборів даних. Синьою лінією зображено криву дерева рішень, червоною – регресії, а зеленою – нейронної мережі. Чим більше крива віддаляється від базової лінії, тим краще модель класифікує дані, тобто прогнозує ймовірність виникнення ознаки кіберзагрози. Представлені на рисунку ROC-криві моделей накладаються одна на одну, що свідчить про приблизно однакову якість класифікації моделей.

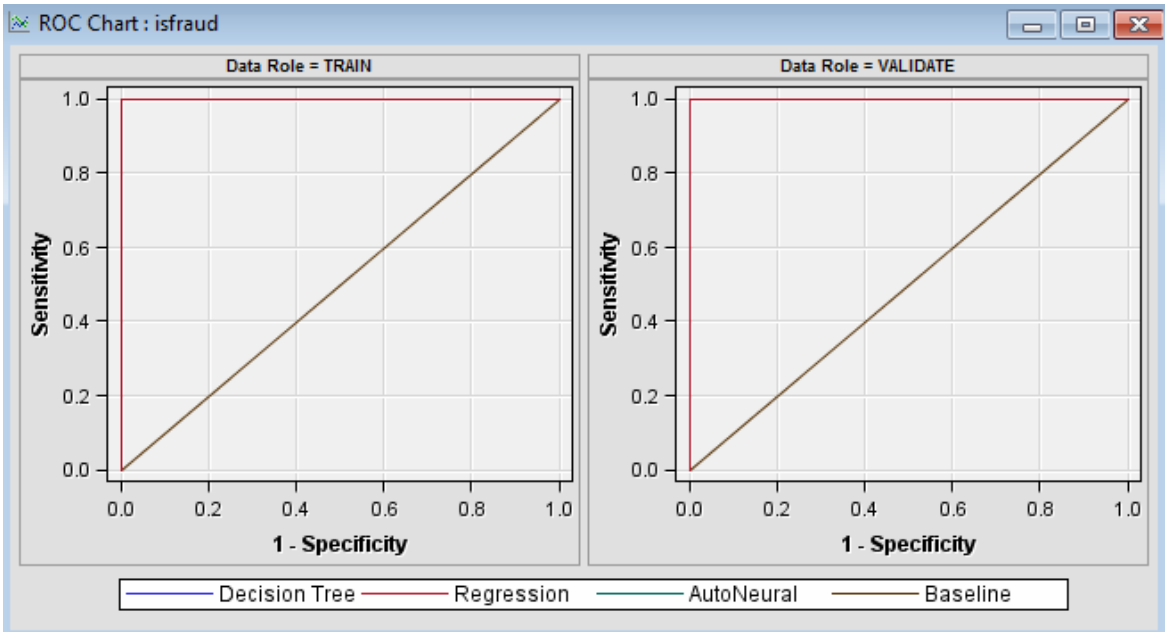


**Рис. 6. ROC-криві дерева рішень, регресії та нейронної мережі**

Оскільки нейронна модель є більш точнішою та враховуючи властивість адаптивності нейронних мереж до змін, оберемо її для перевірки на адекватність. З цією метою на новому наборі вхідних даних проведемо розрахунки та порівняємо характеристики класифікаційних властивостей нейронної мережі (табл. 4).

**Таблиця 4.**
**Характеристика класифікаційних властивостей нейронної мережі**

| Цільова змінна | Результат | Цільова змінна, % | Результат, % | Частота випадків | Загальна класифікація, % |
|---|---|---|---|---|---|
| Навчальна вибірка | | | | | |
| 0 | 0 | 99,9949 | 99,9987 | 78096 | 78,0952 |
| 1 | 0 | 0,0051 | 0,0183 | 4 | 0,0040 |
| 0 | 1 | 0,0046 | 0,0013 | 1 | 0,0010 |
| 1 | 1 | 99,9954 | 99,9817 | 21900 | 21,8998 |
| Валідаційна вибірка | | | | | |
| 0 | 0 | 99,9987 | 99,9987 | 78095 | 78,0958 |
| 1 | 0 | 0,0013 | 0,0046 | 1 | 0,0010 |
| 0 | 1 | 0,0046 | 0,0013 | 1 | 0,0010 |
| 1 | 1 | 99,9954 | 99,9954 | 21902 | 21,9022 |

Результати в таблиці 4 показують, що модель на навчальній вибірці вірно класифікує 99,99% транзакцій, які не мають ознаки кіберзагрози, та 99,98% транзакцій, які мають ці ознаки. Однак, модель класифікувала 0,018% транзакцій, що мали ознаки кіберзагрози, як ті, що не мають таких ознак, і 0,001% транзакцій, які не виявились кіберзагрозами, було класифіковано, як ті, що є кіберзагрозами. Щодо абсолютних величин, то модель правильно класифікувала 78096 транзакцій, як ті, що не мають ознак кіберзагрози, та 21900, як ті, що мають. Неправильно класифіковано всього 5 транзакцій. Тобто, частка неправильної класифікації не перевищує 5%.

**Висновки з проведеного дослідження.** У результаті проведеного дослідження було побудовано логіт-регресію, нейронну мережу і дерево рішень. Проаналізовано їх результати та встановлено, що усі побудовані моделі майже однаково точно описують вхідні дані, проте найбільш точною виявилась модель нейронної мережі, яка пройшла перевірку на адекватність.

Нейронна мережа, як і будь-яка інша модель, потребує постійного оновлення та удосконалення у зв'язку з появою нових ознак загроз для банківських клієнтів. Тому необхідно постійно доповнювати вибірку даних актуальною інформацією про виконані користувачами транзакції.

Застосування отриманої моделі на практиці допоможе працівникам банківського сектору виявляти в транзакціях ознаки кібернетичних загроз, тим самим попереджаючи користувачів мобільного та інтернет-банкінгу від можливих збитків, завданих злочинними діями. Інтеграція моделі в існуючу систему кіберзахисту банку дозволить проводити регулярний моніторинг транзакцій на предмет наявності ознак кіберзагроз, сприятиме підвищенню рівня довіри клієнтів до банків через підвищення захищеності та надійності.

**Робота виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України».**

**Список літератури:**

1. Проект Стратегії забезпечення кібернетичної безпеки України [Електронний ресурс] // Офіційний сайт Національного інституту стратегічних досліджень. – 2013. – Режим доступу до ресурсу: http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf.

2. Trend Report «Financial Cyber Threats Q1 2017» [Електронний ресурс] // The official site of the company "ElevenPaths". – 2017. – Режим доступу до ресурсу: https://www.elevenpaths.com/wp-content/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf.

3. The Top Five Security Threats to Your Banking Institution [Електронний ресурс] // The official site of the company "SentutyLink". – 2017. –Режим доступу до ресурсу: http://www.level3.com/-/media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regionalbanks.pdf.

4. Левкович-Маслюк Л. Великие раскопки и великие вызовы. Компьютерный поиск знаний становится все более ценным / Л. Левкович-Маслюк // Компьютерра. – 2007. – №11(679). – С. 48-51.

5. Яровенко Г.М. Концептуальна модель виявлення ознак кібершахрайств в банках / Г.М. Яровенко, М.М. Бояджян // Сучасні міжнародні економічні відносини: становлення та шляхи перспективного розвитку: збірник тез наукових робіт учасників Всеукраїнської науково-практичної конференції (м. Одеса, 9-10 лютого 2018 р.). – О. : ЦЕДР, 2018. – С. 98-100.

6. SAS Enterprice Miner. Обзор решения [Електронний ресурс] // Офіційний сайт компанії "SAS". – 2016. – Режим доступу до ресурсу: https://www.sas.com/content/dam/SAS/ru_ru/doc/factsheet/sas-enterprise-miner-04-04-2016.pdf.

**References.**

1. The official site of the National Institute for Strategic Studies (2013), "The Project of the Strategy of providing cybernetic security of Ukraine", available at: http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf (Accessed 7 July 2018).

2. The official site of the company "ElevenPaths" (2017), "Trend Report «Financial Cyber Threats Q1 2017»", available at: https://www.elevenpaths.com/wp-content/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf (Accessed 7 July 2018).

3. The official site of the company "SentutyLink" (2017), "The Top Five Security Threats to Your Banking Institution", available at:: http://www.level3.com/-/media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regionalbanks.pdf (Accessed 7 July 2018).

4. Levkovich-Masljuk, L. (2007), "Great excavations and great challenges. A computer search of knowledge is becoming more valuable", *Komp'juterra*, vol. 11(679), pp. 48-51.

5. Yarovenko, H.M. and Boiadzhian, M.M. (2018), "The conceptual model for detecting signs of cybercrime in banks", *Suchasni mizhnarodni ekonomichni vidnosyny: stanovlennia ta shliakhy perspektyvnoho rozvytku: zbirnyk tez naukovykh robit uchasnykiv Vseukrains'koi naukovo-praktychnoi konferentsii* [Modern international economic relations: formation and ways of perspective development: the abstracts collection of scientific works of participants by the All-Ukrainian scientific-practical conference], Vseukrains'ka naukovo-praktychna konferentsiia [All-Ukrainian Scientific and Practical Conference], Center of Economic Research and Development, Odessa, Ukraine, pp. 98-100.

6. The official site of the company "SAS" (2016), "SAS Enterprice Miner. Solution Overview", available at: https://www.sas.com/content/dam/SAS/ru_ru/doc/factsheet/sas-enterprise-miner-04-04-2016.pdf (Accessed 7 July 2018).

*Стаття надійшла до редакції 12.07.2018 р.*