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 | № 10, 2018 | 31.10.2018 р.

УДК 004.6:336.7

Г. М. Яровенко,
к. е. н., доцент, доцент кафедри економічно кібернетики,
Навчально-науковий інститут бізнес-технологій «УАБС»
Сумського державного університету, м. Суми
В.О. Ковач,
магістрант кафедри економічно кібернетики,
Навчально-науковий інститут бізнес-технологій «УАБС»
Сумського державного університету, м. Суми

МОДЕЛЮВАННЯ ПОРТРЕТІВ ПОТЕНЦІЙНИХ ШАХРАЯ ТА ЖЕРТВИ БАНКІВСЬКИХ ШАХРАЙСТВ

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
V. Kovach
graduate student of the Economic Cybernetics Department, Educational and Scientific Institute of Business Technologies "UAB" of Sumy State University, Sumy

MODELING OF POTENTIAL FRAUDSTER'S PORTRAIT AND BANKING FRAUD VICTIM'S PORTRAIT

Статтю присвячено актуальній проблемі боротьби із шахрайствами у банках, яка набула глобального характеру за рахунок збільшення збитків банків та їх клієнтів у різних країнах. На це вплинула поява нових можливостей здійснення фінансових операцій за допомогою різних технологій – Інтернет, мобільних, безконтактних пристроїв, спеціальних програмних додатків, тощо. Для дослідження використано статистичні дані по шахрайствам в Великій Британії за 2015-2018 роки за різними видами фінансових продуктів, які було надано агентством звітності споживчого кредитування "Experian". В статті запропоновано узагальнений підхід до моделювання портретів потенційного шахрая та жертви, який можна застосовувати для формування таких портретів в банківських установах різних країн.
Авторами проаналізовано шахрайства, які здійснюються від першої сторони та від третьої. До шахраїв першої сторони відносяться клієнти банку, які цілеспрямовано здійснюють протизаконні дії з банківськими кредитними, ощадними, платіжними рахунками, картками, іпотекою. Шахраями від третьої сторони вважаються сторонні особи, жертвою яких становиться саме клієнт банку. За останні роки спостерігається збільшення випадків шахрайств, які здійснюють сторонні особи.
Авторами було побудовано дві моделі у вигляді дерева рішень, які являють собою змодельовані портрети потенційного шахрая від першої сторони та потенційної жертви шахрайств з боку третіх сторін. Для побудови дерева було розподілено клієнтів з урахуванням ознак статі, віку та соціальної групи або становища та визначено ймовірності гілок. В результаті отримано дерево із 300 можливими варіантами розвитку подій, що дозволило виділити ймовірних шахраїв та жертв. При впровадженні даних моделей у практичну діяльність аналітичний

відділ банку може самостійно відслідковувати різні групи та ознаки, за якими може виникати шахрайство. Це допоможе вирізнити тих клієнтів, для яких потрібно вжити додаткових заходів безпеки за всіма видами банківських продуктів, особливо поточних, кредитних, ощадних та карткових рахунків. Використання подібних портретів сприятиме більш ефективному прийняттю рішення з боку банківського персоналу та попередженню шахрайства у різних випадках.

The article is devoted to the actual problem of a struggle against bank fraud, which has become global in the context of increasing bank losses and their clients in different countries. The problem was influenced by the emergence of new opportunities for financial transactions through various technologies - the Internet, mobile, contactless devices, special software applications, etc. For the research, the authors used fraud statistics for different types of financial products in the UK during 2015-2018, which was provided by the Consumer Credit Reporting Agency "Experian ". The article proposes a generalized approach to modeling the portraits of a potential fraudster and victim that can be used to create such portraits in banking institutions of different countries. The authors analyzed the frauds that are carried out from the first person and the third. The first person of fraudster includes bank clients, which deliberately makes illegal actions with bank credits, savings, payment accounts, cards, mortgages. The fraudsters of the third person are considered outsiders, whose victims are exactly bank clients. In recent years, there has been the cases of fraud increase that have carried out by outsiders. Authors constructed two models in the form of a decision tree that represent simulated portraits of a potential fraudster from the first person and a potential victim of fraud by third persons. For the construction of the tree, clients were distributed, taking into account gender, age and social group or status, and the probability of branches was also determined. As a result, the tree with 300 possible variants of the development of events has been obtained, which has made it possible to identify probable fraudsters and victims. An analytical bank department can independently track the various groups and signs, which may lead to fraud, with using these models in the practical activities. It will help to identify those bank clients whom need to take additional security measures for all kinds of banking products, especially current, credit, savings and card accounts for. The use of such portraits will contribute to more effective decision-making by bank staff and fraud prevention in different causes.

Ключові слова: *шахрайство; банк; портрет шахрая; портрет жертви; фінансова операція; дерево рішень; модель; моніторинг.*

Keywords: *fraud; bank; fraudster’s portrait; victim's portrait; financial transaction; tree decision; model; monitoring.*

Постановка проблеми. Сьогодні все більших обертів набувають електронні фінансові операції, стрімко зростає кількість карткових транзакцій та активне використання цифрових грошей. Сучасні інноваційні технології зробили можливими платежі через спеціальні програмні додатки, встановленими на мобільні пристрої, або взагалі використання безконтактних технологій. Збільшенню обсягів електронних транзакцій сприяють також й популяризація інтернет-магазинів. Інформаційні технології зробили здійснення платіжних та фінансових операцій зручним та швидким процесом не залежно від місця знаходження платника або отримувача коштів, наявності коштів на рахунку, виду платіжної операції тощо.

Але поряд з вищезгаданими тенденціями набирає обертів й банківське шахрайство, яке на сьогоднішній день є проблемою глобального характеру для банків, їх клієнтів та тих суб’єктів, які мають право здійснювати фінансові операції. За останні роки збитки від фінансових шахрайств зросли кардинально. Це має негативні наслідки для клієнтів фінансово-економічних агентів, які стають основним об’єктом шахрайств та втрачають кошти. Банкам шахрайство наносить також значну шкоду, що проявляється у втраті клієнтів, необхідності відшкодовувати вкрадені кошти, збільшенні коштів на модернізацію служби кібербезпеки та посилення захисних заходів. Поширеними є: шахрайства з банківськими картками, як найбільш простий, доступний та масовий спосіб платежу, що робить його можливим для підробки карток, пристроїв, що зчитують інформацію, викрадання даних з карт; Інтернет-шахрайства, коли Інтернет, який є платформою для клієнтів банку, через яку здійснюють онлайн-платежі, використовується шахраями як інструмент для крадіжки особистих фінансових даних клієнтів; соціальна інженерія, коли шахрай від імені банку дізнається у клієнта всю його інформацію та викрадає кошти з його

рахунку. В арсеналі шахраїв досить багато способів шахрайства із залученням психологічних інструментів, комп'ютерних програм, різних технічних пристроїв, баз даних з інформацією про клієнтів тощо.

Банки та фінансові установи виявляють шахрайства тільки тоді, коли їхні клієнти повідомляють про вже здійснений факт. Крім того, у більшості випадків шахрайств банки не можуть виявити факт шахрайства в процесі його здійснення, тим більше встановити особу шахрая. Банк може працювати тільки з наслідками шахрайства. Як правило, у таких випадках залучають правоохоронні органи та у неможливості знаходження шахрая банк сплачує компенсацію своїм ошуканим клієнтам, які потім звертаються до послуг іншого банку. Такий сценарій не є ефективним, оскільки дозволяє попереджувати тільки наслідки, а не факти самого процесу шахрайства.

Враховуючи останні тенденції, банки зобов'язані інвестувати значною мірою в модернізацію системи кіберзахисту шляхом придбання або створення сучасних систем виявлення та попередження шахрайств, які врешті-решт також можуть виявитися неефективними. Тому для боротьби із шахрайствами банки повинні підходити послідовно та системно. По-перше, необхідна чітка регламентація дій персоналу щодо доступу до даних, що дозволить уникнути фактів його доступу до персональної інформації клієнтів та відповідно викрадення її. По-друге, вводити стратегії, які включають проведення тренінгів з обізнаності про шахрайство, роз'яснення серед населення через засоби масової інформації та Інтернет, оцінку ризиків шахрайства та безперервний моніторинг. По-третє, удосконалити програмне та інформаційне забезпечення автоматизованої банківської системи з урахуванням інтелектуальних алгоритмів обробки, що дозволить на етапі здійснення шахрайства ідентифікувати шахрая та жертву, попередити здійснення такої операції та виявити злочинця. Тому тема, присвячена процесу моделювання портрету потенційного шахрая та потенційної жертви є актуальною й для банків та для їх клієнтів.

Аналіз останніх досліджень і публікацій. Проблемою боротьби із шахрайствами у банках активно почали займатися останні 10 років. Статистичними дослідженнями в галузі банківського шахрайства займаються відомі компанії в галузі аналітики, як "SAS Institute", "Experian", "ElevenPath", "Українська міжбанківська асоціація членів платіжних систем ЕМА" та інші.

Загальною проблематикою визначення шахрайства в банківській сфері, його суб'єктів, способів займалися такі науковці, як: А. Єпіфанов, М. Зацеркляний, Д. Козлов, О. Кришевич, В. Левін, С. Ніколаюк, С. Поперешняк, І. Сало, О. Саяпін, С. Шапочка, А.М. Шевченко та інші., що знайшло відображення у низці наукових публікацій.

Аспекти сучасних методів моделювання й автоматизації для використання в процесі виявлення шахрайств у банках знайшли своє відображення в роботах вітчизняних науковців та вчених з різних країн, як Н. Паклін та В. Орешков (2009 р.), J. Stanton (2013), M.J. Zaki and W. Meira (2014 р.), Jared Dean (2014), А. Шипунов, Е. Балдін, П. Волкова, А. Коробєйніков та інші (2014 р.), С. Мастицький, В. Шитіков (2014 р.), A.S. Muller, S. Guido (2016 р.) та інші. [1]

На нашу думку, суттєвим недоліком відображення проблеми шахрайства у наукових досліджень є практично повна відсутність прикладних розробок, які можна впроваджувати в діяльність банків для попередження шахрайських операцій, що робить дану проблему цінною для подальшого вивчення.

Метою статті є моделювання портрету потенційного шахрая та потенційної жертви банківських шахрайств з урахуванням статі, віку та фінансових можливостей з використанням дерева рішень, що дозволить в процесі здійснення банківських операцій виявляти потенційних шахраїв та їх жертв, та попереджати факт проведення такої операції.

Виклад основного матеріалу дослідження. Для дослідження даної проблематики було взято статистичні дані по шахрайствам в Великій Британії за 2015-2018 роки за різними видами фінансових продуктів. Статистика була надана агентством звітності споживчого кредитування "Experian", яке збирає та обробляє інформацію про понад мільярд людей та підприємств по всьому світу та входить в трійку найбільших кредитних бюро США. На жаль аналітичні агентства та банки України не публікують подібного роду статистику в періодиці або в офіційних виданнях. Тому в даному досліджені буде представлений узагальнений підхід до моделювання портретів потенційного шахрая та жертви, виконаний на прикладі даних Великої Британії, який можна застосовувати для формування таких портретів в різних країнах та з урахуванням їх умов.

Для дослідження було використано статистику за двома основними групами шахраїв. Перша група включає в себе осіб, які є споживачами послуг банків чи фінансово-кредитних компаній, тобто шахраї від першої сторони – безпосередні учасники. Шахрайство починається тоді, коли клієнт не має наміру в подальшому погасити виплати за фінансовим продуктом. Саме в цьому намірі й полягає найбільша різниця між кредитним ризиком та ризиком не повернення коштів в результаті шахрайства. Кредитний ризик включає клієнтів, які отримали товари чи послуги з наміром їх погасити, але просто не мають ресурсів для виконання своїх зобов'язань в зв'язку з непередбачуваними для них самих обставинами. За другим варіантом людина цілеспрямовано не віддає кошти. Такий вид шахрайства може включати широкий спектр тактик. Наприклад, коли одна особа передає відповідальність за виплату коштів на іншу особу. Тобто шахрай дуже гарно знає особу, на яку оформлює кредит, за виплату якого буде відповідати жертва, а не шахрай. Найуспішними шахрайствами є випадки, коли шахраї поєднуються з хорошими клієнтами, які мають гарну кредитну історію, що створює підґрунтя для довгострокових масштабних шахрайств. [2]

Другу групу складають шахрайства від третьої сторони, тобто від осіб, які не пов'язані ні з провайдером фінансово-кредитних послуг, ні з їх клієнтами. Таке шахрайство здійснюється сторонніми особами шляхом використання фальшивих ідентифікаційних документів, без відома особи, чия особа використовується для здійснення шахрайства. Сюди ж відноситься шахрайська діяльність, пов'язана з незаконним отриманням

конфіденційних даних клієнтів банків, ПІН-кодів та CVV2-кодів банківських карток, логінів та паролів від інтернет-банкінгу, заволодівання мобільними фінансовими номерами клієнтів, за якими здійснюється аутентифікація, тощо. У випадку шахрайства від третьої сторони вкрай складно визначити особу самого шахрая, відслідкувати його місцезнаходження. Тому такі види шахрайств є найбільш популярними, оскільки зловмисники часто залишаються не спійманими. [3]

Так, розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки представлений на рисунку 1.

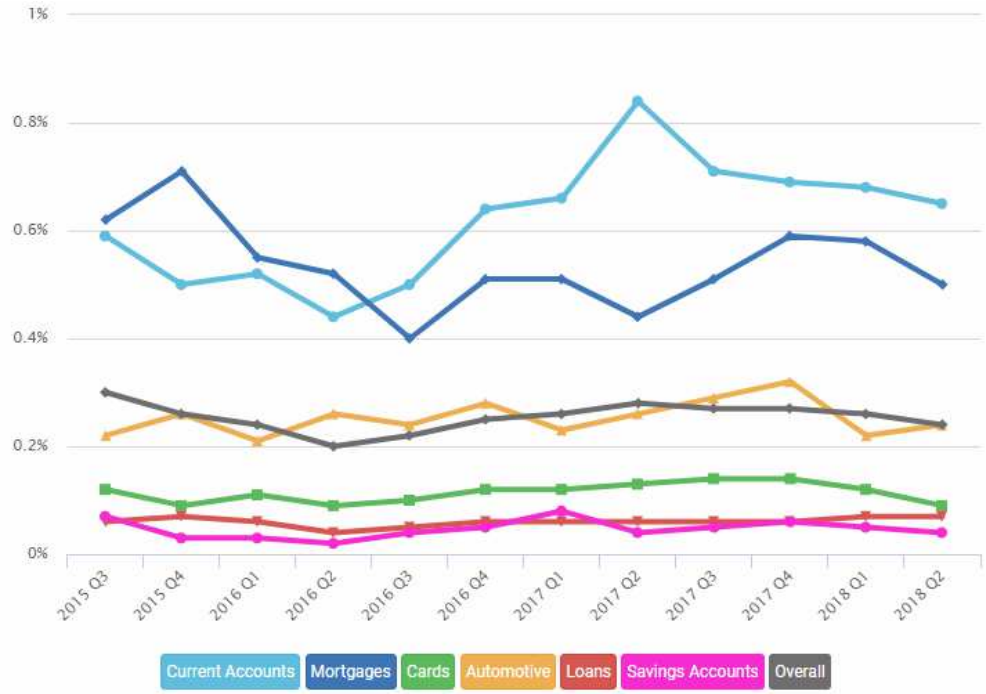

Рис. 1. Розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки

(дані взято з офіційного сайту британського філіалу агентства "Experian" [4])

Шахрайства від першої сторони найбільш ймовірно припадають на шахрайства з поточними банківськими рахунками (Current Accounts) та іпотеку (Mortgages) (див. рис. 1). В даному випадку розглядається традиційне іпотечне шахрайство, яке включає в себе заходи, спрямовані на те, щоб обдурити кредитора, наприклад, намагання шахраєм отримати кредит, на який він не може законно претендувати, коли позичальники хибно представляють свою фінансову інформацію. [5]

Що стосується шахрайств від третьої сторони, то вони здійснюються переважно над поточними рахунками клієнтів (Current Accounts). Також популярними є шахрайства з банківськими картками (Cards) та ощадними рахунками (Saving Accounts) (див. рис. 2). Тобто шахраї можуть отримати доступ до рахунку клієнта шляхом застосування методів соціальної інженерії, що є найбільш популярним способом шахрайства. Також можливі випадки, коли ідентифікаційні дані клієнта викрадаються з бази даних банку. Відомі випадки, коли банківські працівники продавали бази даних стороннім особам, за рахунок чого шахраї отримували доступ до даних клієнтів. Тут певну роль відіграє нехтування клієнтами елементарних правил безпеки власних конфіденційних даних, їх необережність при здійсненні розрахункових операцій та довірливість.

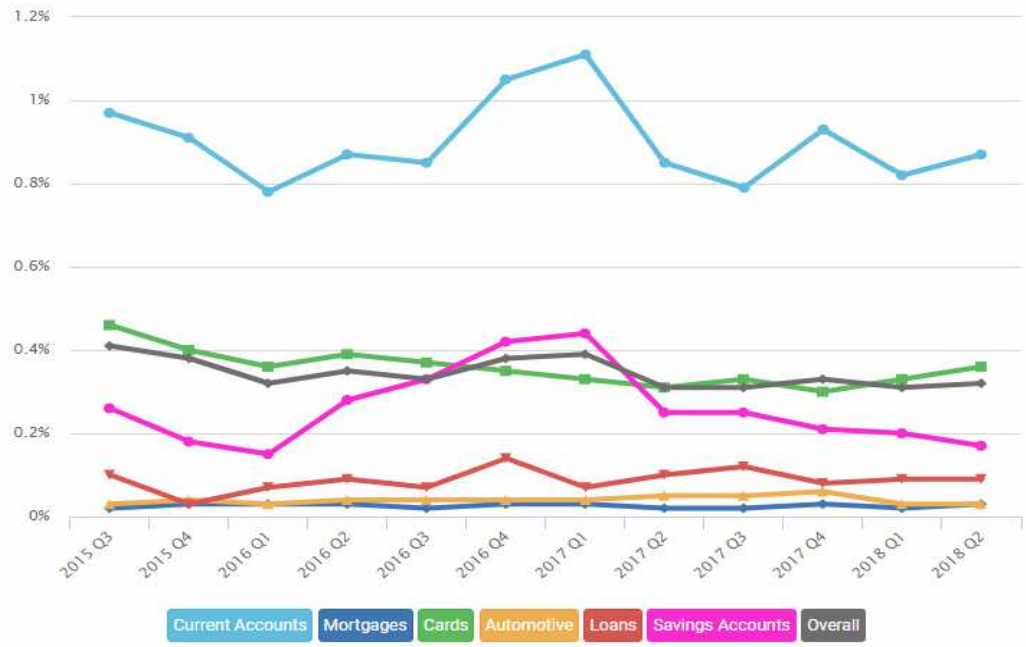

Рис. 2. Розподіл шахрайств від третьої сторони за видами фінансових продуктів у Великій Британії за 2015-2018 роки

(дані взято з офіційного сайту британського філіалу агентства "Experian" [4])

За останні три роки шахрайства від третьої сторони переважають над шахрайствами від першої. У 2017 році співвідношення шахрайств від першої сторони до шахрайств від третьої складає 44%, а шахрайств від третьої сторони до шахрайств від першої – 56%, тоді як ще в 2014 році ситуація була протилежною. Можна припустити, що це пов'язано з більш масовим використанням Інтернет-технологій для здійснення банківських операцій, оскільки в просторах Інтернету набагато складніше забезпечити максимальну конфіденційність даних.

Використовуючи статистику по розподілу шахраїв від першої сторони на групи за віком, статтю та соціальним статусом, а також статистику по жертвах шахрайств з боку третьої сторони за такими ж параметрами, авторами побудовано два ймовірнісні дерева, які являють собою змодельовані портрети потенційного шахрая від першої сторони та потенційної жертви шахрайств з боку третіх сторін.

Дерево ймовірностей це модель, яка широко застосовується для прийняття рішення, та складається з вузлів, які відповідають моменту настання події, в нашому випадку – здійснення шахрайства з фінансовими продуктами. Гілки дерева це можливі варіанти розвитку події, кожна зі своєю ймовірністю.

На першому етапі побудови дерева розподіляємо клієнтів (потенційних шахраїв) за статтю. Ймовірності для гілок будуть дорівнювати: 68,9 % ймовірність першого варіанту розвитку подій, при якому шахрай виявиться чоловіком (Male); 31,1 % – ймовірність того, що шахраєм буде жінка (Female).

На наступному етапі враховуємо розподіл шахраїв за віковими групами (Age). Ймовірність кожної наступної гілки отримуємо, як добуток ймовірностей фактору статі до ймовірності кожної з вікових груп. На другому етапі отримуємо з двох гілок двадцять, за різними варіантами розвитку подій. На третьому етапі аналогічним чином уточнюємо модель, включивши фактор приналежності до однієї з 15 соціальних груп. В результаті отримали дерево, в якому буде 300 гілок, тобто ми змоделювали 300 можливих варіантів розвитку подій і розрахували їх ймовірності.

Побудоване дерево рішень, тобто модель потенційного шахрая від першої сторони за ознаками статі, віку та соціальної групи, представлено на рисунку 3. В матриці результатів моделі її елементи мають різні кольори у відповідності із рівнем ймовірності: зелений колір найменша ймовірність шахрайства, жовтий середня, червоний найвищий рівень ймовірності шахрайства.

В результаті побудованої моделі шахрая (див. рис. 3) отримано, що найбільш схильною до шахрайства групою клієнтів є чоловіки у віці від 25 до 29 років, які мешкають в мультикультурних кварталах міста. Ця група складає 2,14% від усіх шахраїв і є найбільш ризикованою групою клієнтів для банків та інших фінансово-кредитних організацій. Також до великої схильності шахрайства можна віднести чоловіків у віці від 30 до 34 років, що також мешкають у містах, чоловіків у віці 25-29 років, які наймають помешкання.

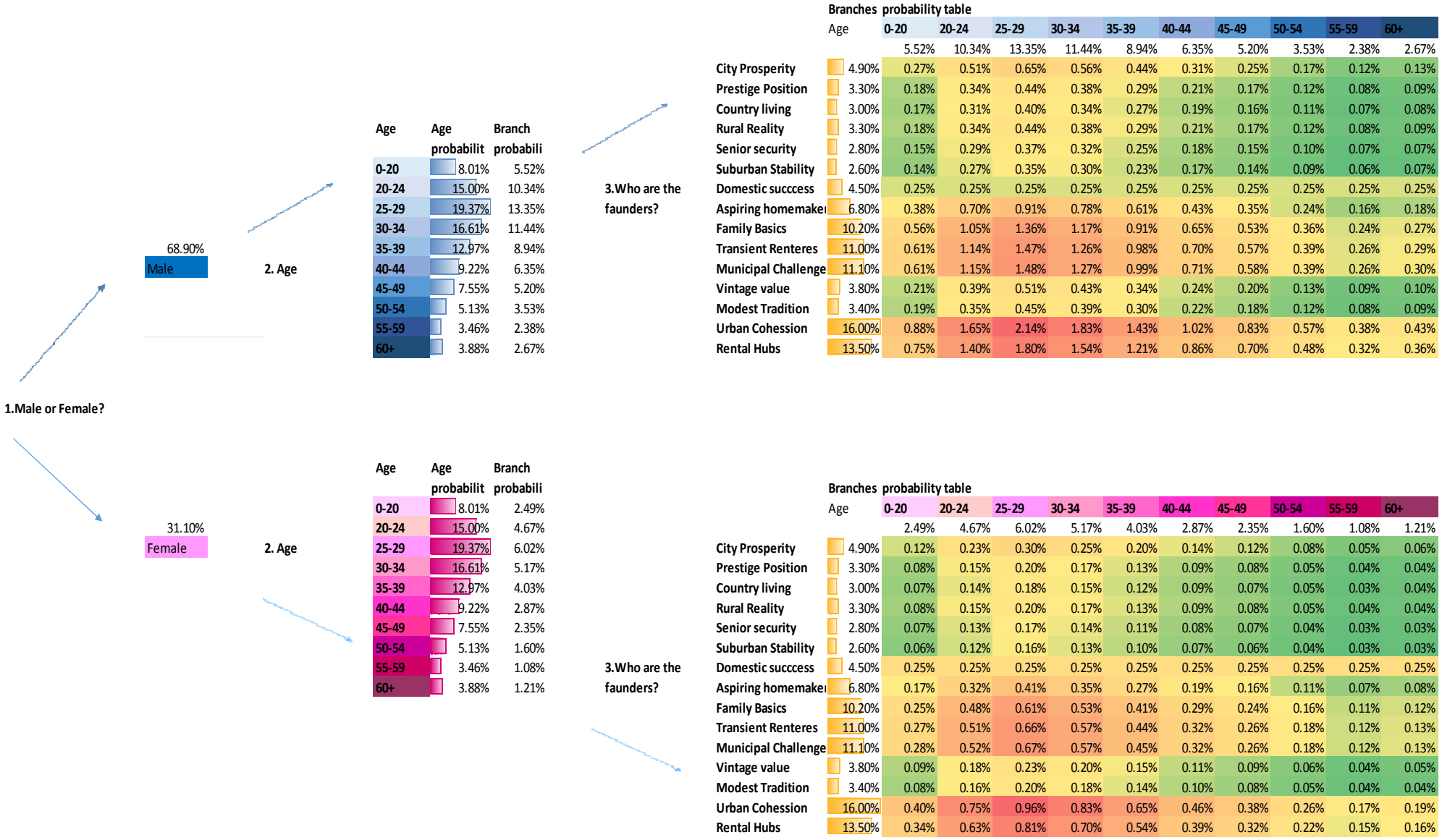

Рис. 3. Модель портрету потенційного шахрая від першої сторони за ознаками статі, віку та соціальної групи
(авторська розробка)

Серед жінок можна виділити групи у віці 25-29 років та 30-34 років, що також мешкають в мультикультурних кварталах міста або наймають житло. Це можливо пояснити за рахунок того, що люди у віці 25-34 ще можливо не мають стабільного кар'єрного зросту, постійного місця проживання, тому й стикаються з певними фінансовими труднощами, які схиляють їх до шахрайств.

Найменша ймовірність того, що шахраєм виявиться жінка або чоловік у віці від 50 років, які відносяться до соціальної групи «Senior security», тобто подружні жінки та чоловіки, які живуть окремо від своїх дітей у власних зручних приватних будинках і мають достатній рівень фінансової забезпеченості для спокійного та розміреного життя. Лише 0,03% шахрайських випадків з боку клієнтів фінансових установ здійснюються представниками цієї групи. Такий же відсоток шахрайств припадає на жінок та чоловіків, що класифікуються як «Country living» (доброзичливі домовласники, які живуть в сільській місцевості, часто фермери), «Suburban Stability» (домовласники, що мають заміську нерухомість), «Sity Prosperity» (міські жителі із стабільним середнім доходом); «Prestige Position» (міські жителі із високим доходом).

Отримана модель дає можливість швидко визначити рівень ймовірності шахрайства для тієї чи іншої особи-клієнта враховуючи три основні фактори: стать, вік та соціальну групу. Вона може бути корисною при прийнятті рішення про видачу позики, реалізації будь-яких ризикованих фінансових операцій, для забезпечення яких може використовуватися нерухомість, тощо. При впровадженні даної моделі у практичну діяльність банк може самостійно відслідковувати різні групи та ознаки, за якими може бути виникати шахрайство.

Результат побудованої моделі потенційного жертви шахрайства від третьої сторони за ознаками статі, віку та соціальної групи, представлено на рисунку 4. Отримана модель вказує на те, що найбільше від сторонніх шахраїв потерпають чоловіки в віці 25 - 44 років, які відносяться до соціальної групи «Rental Hubs» □ переважно молоді, одинокі люди, та люди середнього віку, які живуть у міських поселеннях та орендують свої будинки, перебуваючи на ранній або середній стадіях своєї кар'єри або продовжують навчання.

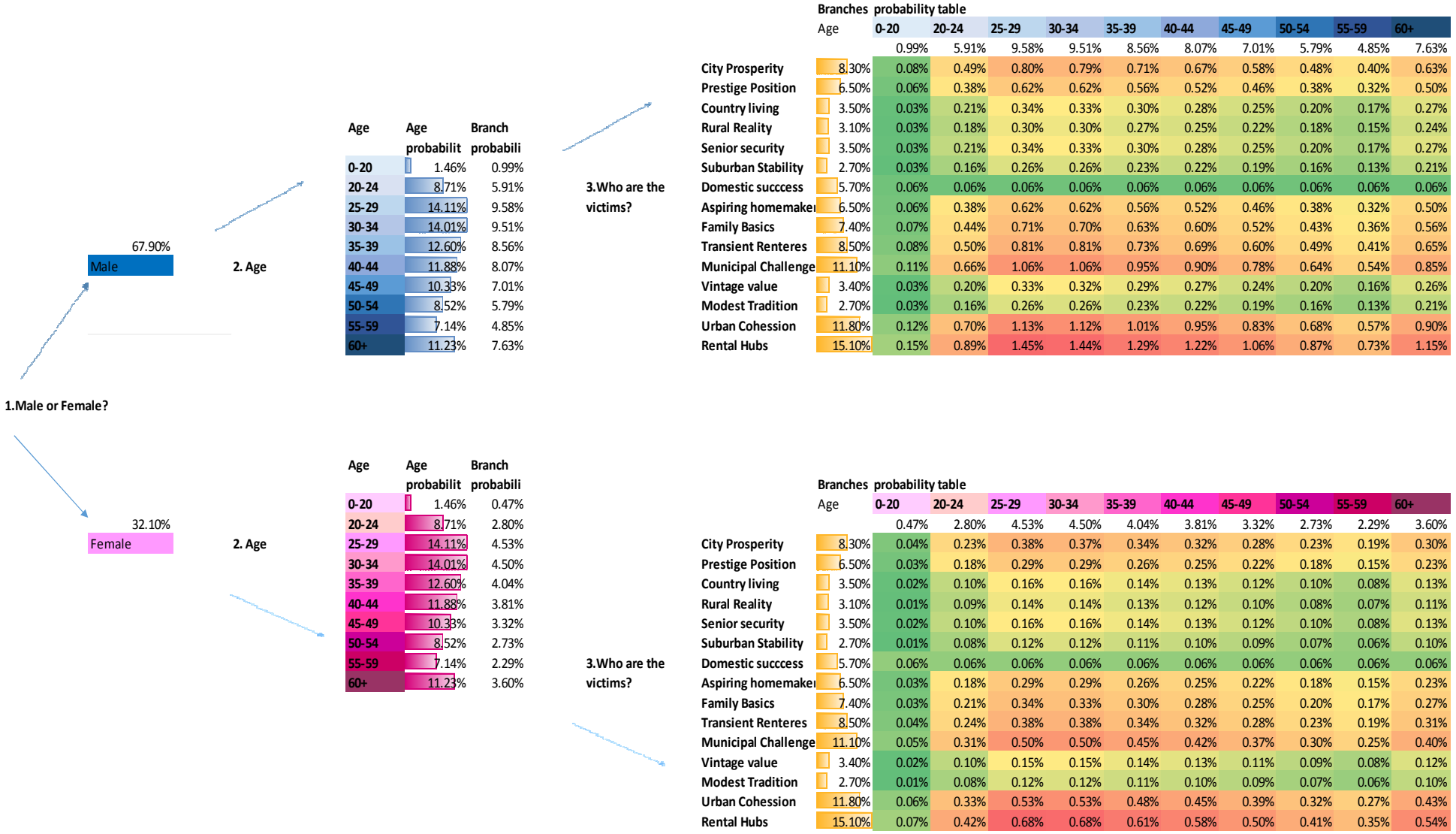

Рис. 4. Модель портрету потенційної жертви шахрайства від третьої сторони за ознаками статі, віку та соціальної групи
(авторська розробка)

Схожі результати й для жінок, які знаходяться у віці 25 - 39 років та також орендують житло. Це можна пояснити більшою фінансовою активністю даної групи людей, які частіше здійснюють будь-які фінансові операції через Інтернет або мобільні пристрої, частіше користуються послугами фінансово-кредитних організацій, онлайн-сервісами, програмними додатками.

Найменша ймовірність бути жертвою шахрая є у чоловіків та жінок у віці до 20 років за різними соціальними групами. Це пов'язано з тим, що ця група – це молоді люди, які ще навчаються у навчальних закладах, коледжах та не мають самостійності у фінансах. Найменша ймовірність з даної групи бути жертвою шахрая, це жінки з соціальної групи «Modest Tradition», які живуть в приватних недорогих будинках, в скромних сім'ях, та вже давно прижились на певній території.

Розроблена модель допомагає вирізнити тих клієнтів, для яких потрібно посилити систему безпеки за всіма видами банківських продукті, особливо банківських карт, поточних та ощадних рахунків, щоб уникнути небажані збитки. Можливе також введення додаткових заходів для інформування клієнтів про найпоширеніші актуальні схеми банківських шахрайств.

Дану методику побудови портретів шахраїв можна використати й в роботі українських банків. Ймовірно, що портрети будуть відрізнятися, оскільки співвідношення віку, статі та фінансової стабільності клієнта є різними для громадян з розвинутої країни та країни, що розвивається. Але застосування цієї методики дозволить вже на етапі здійснення операції визначити потенційного шахрая чи жертву. Це призведе до коригування інструкцій в банках та зменшить навантаження на людину в процесі прийняття рішення.

Висновки. Таким чином, для ефективної взаємодії фінансово-кредитних установ та їх клієнтів, та для зменшення ймовірності отримати збитки від шахрайських операцій, необхідно застосовувати нові інструменти. В якості такого інструменту може виступати побудова моделей потенційних шахраїв та жертв банківських шахрайств. Портрети представляють собою моделі дерева рішень, які дозволяють визначити ймовірність шахрайства у відповідності з рядом ознак. Методика є вкрай простою та може враховувати не тільки вік, стать, соціальне становище, але й способи здійснення операцій (Інтернет, мобільний телефон, тощо), історію клієнта, місце здійснення операції, та інше. Оскільки шахраї вдосконалюють свої інструменти, відповідно банківські підрозділи кіберзахисту повинні швидко реагувати на ці зміни. Це можливо, якщо банки будуть використовувати математичні методи для розробки алгоритмів моніторингу, перевірки клієнтів та операцій на предмет виникнення ймовірності шахрайства. Отримані результати повинні накопичуватися та формувати банк даних, використання якого надасть можливість оперативно оновлювати інформацію щодо шахрайств та модернізовувати портрети. В свою чергу, це сприятиме більш ефективному прийняттю рішення з боку банківського персоналу та попередженню шахрайства.

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».

Література.

1. Яровенко Г. М. Розробка інформаційної моделі виявлення ознак шахрайств у банках / Г. М. Яровенко // Інвестиції: практика та досвід. – 2018. – №14. – С. 23-28.

2. Ryan C. Hybrid Risk: The truth behind first party fraud [Електронний ресурс] / Chris Ryan // The official site of the company "Experian". – 2015. – Режим доступу до ресурсу: http://www.experian.com/blogs/insights/2015/10/hybrid-risk-the-truth-behind-first-party-fraud/.

3. Third Party Fraud [Електронний ресурс] // Open Risk Manual. – 2017. – Режим доступу до ресурсу: https://www.openriskmanual.org/wiki/Third_Party_Fraud.

4. #FraudStats [Електронний ресурс] // The official site of the company "Experian". – 2018. – Режим доступу до ресурсу: https://www.experian.co.uk/identity-and-fraud/fraud-statistics/.

5. What is Mortgage Fraud? [Електронний ресурс] // MortgageLoan.com. – 2015. – Режим доступу до ресурсу: https://www.mortgageloan.com/.

References.

1. Yarovenko, H.M. (2018), "Development of the information model for detection fraud signs in the banks", *Investytsii: praktyka ta dosvid*, vol. 14, pp. 23–28.

2. Ryan, C. (2015), "Hybrid Risk: The truth behind first party fraud", *The official site of the company "Experian"*, [Online], available at: http://www.experian.com/blogs/insights/2015/10/hybrid-risk-the-truth-behind-first-party-fraud/ (Accessed 19 Oktober 2018).

3. The official site "Open Risk Manual" (2017), "Third Party Fraud", available at: https://www.openriskmanual.org/wiki/Third_Party_Fraud (19 Oktober 2018).

4. The official site of the company "Experian" (2018), "#FraudStats", available at: https://www.experian.co.uk/identity-and-fraud/fraud-statistics/ (19 Oktober 2018).

5. The official site "MortgageLoan.com" (2015), "What is Mortgage Fraud?", available at: https://www.mortgageloan.com/ (19 Oktober 2018).

Стаття надійшла до редакції 20.10.2018 р.