УДК 004.6:336.7

Г. М. Яровенко,
к. е. н., доцент, доцент кафедри економічної кібернетики, Навчально-науковий інститут бізнес-технологій "УАБС" Сумського державного університету, м. Суми

РОЗРОБКА ІНФОРМАЦІЙНОЇ МОДЕЛІ ВИЯВЛЕННЯ ОЗНАК ШАХРАЙСТВ У БАНКАХ

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

DEVELOPMENT OF THE INFORMATION MODEL FOR DETECTION FRAUD SIGNS IN THE BANKS

Статтю присвячено сучасній та актуальній проблемі боротьби із шахрайствами у банках. Одним із шляхів її вирішення є створення системи моніторингу, інтегрованої з автоматизованою банківською системою. Система повинна виявляти та попереджати ті операції, які мають ознаки шахрайської. Вона будується з урахуванням внутрішніх та зовнішніх інформаційних потоків та з використанням математичного інструментарію Data Mining. Автором пропонується: інформаційна модель виявлення ознак шахрайства для тих операцій, які здійснюють клієнти банку, та інформаційна модель виявлення ознак шахрайства для операцій банківського персоналу. Моделі розроблено у нотації DFD із використанням програмного забезпечення "All Fusion Process Modeller". Вони враховують критерії перевірки: обнуління рахунку, відповідність лімітам, геолокацію, цільове призначення, правильність введення даних, активність, права доступу та інші. У статті запропоновано схеми процесів здійснення операцій клієнтами та банківськими працівниками, які підлягатимуть оперативній перевірці для виявлення ознак шахрайства. Схеми розроблено у нотації BPMN 2.0 у програмному забезпеченні "Bizagi Modeller".

The article is devoted to a modern and actual problem of a struggle against bank fraud. One of the ways to solve it is creating a monitoring system integrated with an automated banking system. The system must detect and alert those operations that have fraudulent features. It is built on the basis of internal and external information flows and using the mathematical tools Data Mining. The author proposes: an information model for fraud detection those operations carried out by bank clients, and an information model for fraud detection transaction of banking staff. The models were developed in the DFD notation with using the "All Fusion Process Modeller" software. They take into the verification criteria: non-zero value verification of an account, compliance with limits, geolocation, destination, data entry, activity, access rights, and others. In the article it was proposed the schemes that shows processes of operations realization by clients and bank staff and which are subject to operative verification for revealing of fraud signs. The schemes are developed in the BPMN 2.0 notation with using the Bizagi Modeller software.

Ключові слова: шахрайство, моніторинг, банк, автоматизована банківська система, інформаційна модель.
Key words: fraud, monitoring, bank, automated banking system, information model.

ПОСТАНОВКА ПРОБЛЕМИ

Одним з важливіших та актуальних питань для банків є вирішення проблеми, пов'язаної із виявленням та попередженням шахрайських, незаконних дій з його фінансовими ресурсами. Шахрайства, об'єктами яких частіше всього стають клієнти банків, сприяють зниженню довіри до банків, як фінансових інститутів, та пошуку альтернативних способів для зберігання коштів. Удосконалення методів шахрайств та збільшення частоти кібератак призводять до збільшення втрат банків та їх клієнтів. Банківська система безпеки часто не встигає за швидкими темпами модернізації способів та інструментів шахраїв. Відповідно рівень протидії загрозам поступається рівню зростаючих загроз.

За оцінками експертів серед галузей, які найбільше потерпають від шахраїв, перше місце займає банківський сектор, друге — енергетичний та добувний сектор, третє — телекомунікаційний. Так, у 2017 році від фішингових атак найбільшої шкоди зазнали 51,7% банків у порівнянні з електронною комерцією та платіжними системами — представниками фінансового сектору. [1]

За статистичними даними ЕМА (Української міжбанківської асоціації членів платіжних систем), сума збитків громадян внаслідок дій шахраїв із платіжними картками у 2017 році досягла 670 млн грн, що значно перевищує збитки за попередні роки — 339,13 млн грн (2016 р.), 181,00 млн грн (2015 р.), 90,00 млн грн (2014 р.). Збільшилася також і середня сума втрат від шахрайства

із використанням методів соціальної інженерії. Так, у 2017 році ця сума склала 2543,00 грн проти 1403,00 грн у 2016 році та 834,00 грн у 2015 році [2].

Боротьба із шахрайством — це глобальна проблема. Для її вирішення створюються спеціальні підрозділи, її намагаються регулювати на законодавчому рівні. На боротьбу із шахрайством впливають:

— розвиток нових способів шахрайства;

— збільшення обсягу інформації, обробка якої потребує нових методів, наприклад, Data Mining;

— обмеження в інформаційних системах, які не дозволяють своєчасно адаптувати їх до ефективної протидії новим за формою і рівнем новизни загрозам;

— проблеми, пов'язані з управлінням даними на фізичному та організаційному рівнях;

— банківські ризики;

— психологія взаємовідносин "клієнт — шахрай — банк", яка дозволяє клієнту у випадках спілкування із шахраєм надавати конфіденційну інформацію.

Одним із головних напрямків боротьби із шахрайством, зазначеним у Постанові НБУ №95 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" від 28 вересня 2017 року, є впровадження банками основних технічних систем [3]:

— виявлення атак;

— моніторингу події управління інцидентами;

— контролю доступу до мережі;

— захисту електронної пошти;

— запобігання атак, спрямованих на відмову в обслуговуванні;

— антивірусного захисту;

— двофакторної автентифікації.

Але роз'яснення щодо їх створення, впровадження, фінансування, тощо, відсутні. Тобто перед банками поставлена задача, а її виконання — це вже прерогатива власників, при цьому спостерігається нехватка спеціалістів у галузі кібербезпеки, що ускладнює виконання задачі.

До вирішення такої складної проблеми треба підходити системно, та ключем її вирішення має бути розвиток та удосконалення автоматизованих інформаційних технологій та систем у поєднанні із математичними методами.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Тема, присвячена пошукам нових методів, технологій виявлення ознак та передумов шахрайств для банківської системи є вкрай актуальною та практично значущою. Нею займалися та займаються вчені та практики різних країн світу. Так, у сфері інтеграції автоматизованих та математичних методів для банківської сфери багато зроблено працівниками американської компанії в галузі бізнес-аналітики "SAS Institute", результатом чого стають програмні розробки для банків [4].

Статистичні дослідження в галузі видів, способів, типів шахрайств для різних сфер економіки здійснює компанія "Kaspersky Lab", яка багато років розробляє програмні рішення для антивірусного захисту та інтернет-безпеки [5].

Сучасні методи моделювання й автоматизації та їх використання для виявлення шахрайств у банках знайшли своє відображення в роботах таких науковців, 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.

МЕТА СТАТТІ

Метою статті є розробка інформаційних моделей виявлення ознак шахрайств з боку клієнтів та персоналу банку як складової частини автоматизованої банківської системи.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Розглянемо банк як складну систему, складовими якої виступають внутрішнє середовище: персонал, менеджмент банку, його власники, автоматизована банківська система (АБС); та зовнішнє середовище: клієнти, кіберзлочинці, пов'язані особи, програмно-технічні пристрої. Тобто банк є системою взаємозв'язаних суб'єктів та об'єктів внутрішнього та зовнішнього середовища. До складу системи будь-якої природи входять елементи різного рівня надійності, або які можуть вторгнутися в певний момент за певних умов, що може призвести до негативних наслідків. По суті, кожен з цих елементів може стати джерелом потенційного шахрайства або ініціатором, або співучасником, або бути опосередковано залученим.

Різні дослідження в сфері банківського шахрайства розглядають в основному зовнішнє середовище, як ініціатора шахрайства, що є не зовсім коректно. 80% від усього обсягу шахрайства пов'язано із персоналом банку. Тому можливості вторгнення повинні враховувати також і внутрішні аспекти загрози.

Отже, при окресленні банківської системи будемо користуватись принципом професійного песимізму, яким керуються аудитори, і який не виключає зловживань на будь-якому робочому місці банку та не виключає ймовірності вторгнення сторонніх осіб задля здійснення шахрайства або шкоди. Тобто шахрайство може бути здійснено будь-ким, будь-де та з використанням будь-яких інструментів та способів. Відповідно система повинна враховувати зміни негативного характеру та реагувати на них.

Виходячи з цього, представляємо архітектуру АБС з урахуванням модулю моніторингу, який є центральною ланкою, що пов'язує інформаційні потоки, які генерують суб'єкти та об'єкти зовнішнього та внутрішнього середовища (рис. 1).

Система повинна передбачати ймовірність шахрайства, виявляти та попереджувати. Тому доцільно, що така система буде мати модуль моніторингу "Monitoring Module", побудований за принципами застосування методів інтелектуального аналізу "Data Mining" та створення бази даних із статистикою шахрайств "Fraud Statistics" й бази правил (критеріїв) для відслідковування ознак шахрайств "Rules Database" (рис. 1). Його головне призначення — виявляти потенціальні шахрайства незалежно від природи ініціатора (зовнішнього — клієнта

банку та його операцій "Transaction Database", чи внутрішнього — персоналу банку та його операцій "Database of Staff Operation"). Операції перевіряються на відповідність певним критеріям, які визначають, чи має операція ознаки шахрайської, які сформовані у базі правил з урахуванням накопичених статичних даних щодо шахрайства.

Відповідно до запропонованої структури АБС побудуємо інформаційну модель виявлення ознак шахрайств для операцій, ініційованих зовнішнім середовищем, яка відображає інформаційні потоки, що будуть функціонувати у середовищі АБС, а саме у модулі моніторингу (рис. 2).

Модель побудовано у нотації DFD (data flow diagrams) [6], яка є одним із інструментів структурного моделювання та проектування інформаційних систем, із використанням програмного забезпечення "All Fusion Process Modeller". DFD-модель дозволяє описати потоки даних.

Побудована на рисунку 2 модель відображає інформаційні потоки, які будуть задіяні в модулі моніторингу для виявлення ознак шахрайств та їх попередження. Це відбувається шляхом перевірки банківської транзакції ("Transaction"), яку здійснює клієнт (сутність "Bank Customer"), із використанням функцій "Data Monitoring". Перевіряються:

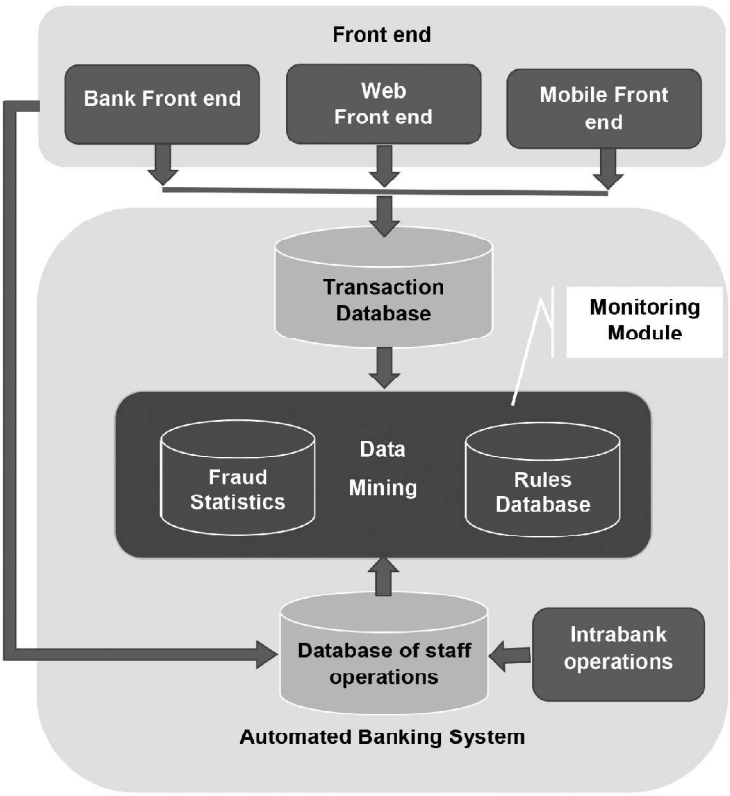

Рис. 1. Архітектура автоматизованої банківської системи з урахуванням модулю моніторингу

— суми транзакцій ("Transaction Amount") на предмет обнуління рахунку ("A non-zero value verification"). Частіше всього шахрай у процесі шахрайської операції знімає усі кошти з рахунку, що ймовірніше за все не є типовим для власника рахунку. В результаті отримується інформація про те, що на рахунку нульовий баланс "Zero Balance";

— суми транзакцій ("Transaction Amount") на перевищення встановлених лімітів ("Limit Verification"). У процесі шахрайства операції можуть перевищувати встановлені банком або клієнтом ліміти "Overlimit", що дозволить сигналізувати про спробу здійснення незаконної операції;

— локації клієнта ("Customer Location Verification"), оскільки операція може здійснюватися з будь-якої країни, міста та може не відповідати фактичній геолокації клієнта;

— рахунку цільового призначення ("Verification of a special purpose account"). Рахунок може бути в "чорному списку" клієнтів ("Suspicious accounts") або може бути перевищення лімітів по сумі транзакції ("Overlimit"), якщо цільовий рахунок відкрито в іншому банку;

— номера та аккаунти клієнта ("Number or Account verification") в залежності від типу пристрою ("Device Type"), з якого ініціюється операція. У випадку, коли операцію намагаються здійснити з номера та аккаунта, які не належать клієнту ("Non-client account" та "Non-client number");

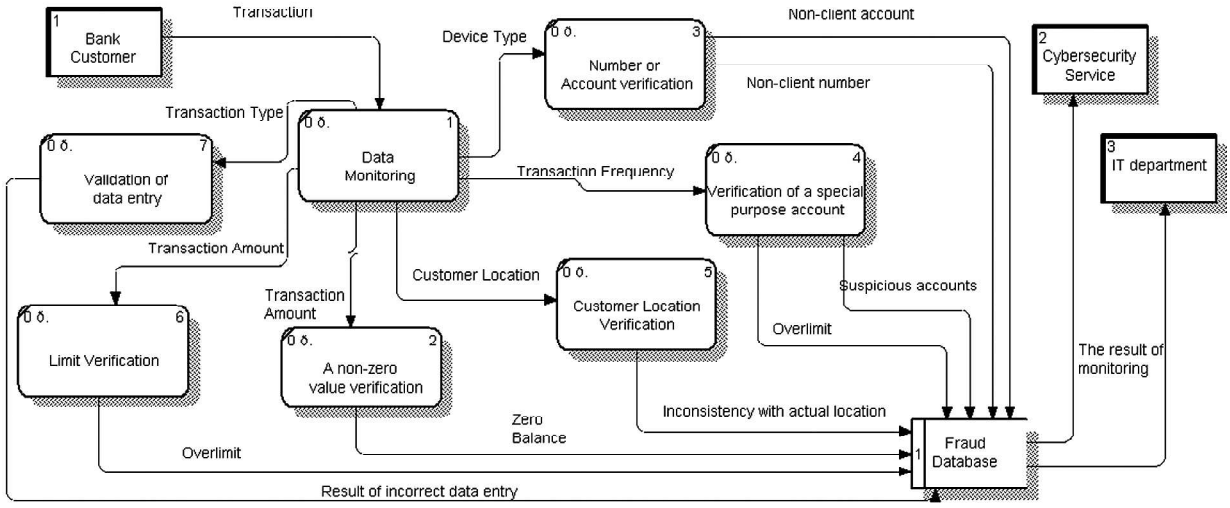

Рис. 2. Інформаційна модель виявлення ознак шахрайств клієнтів

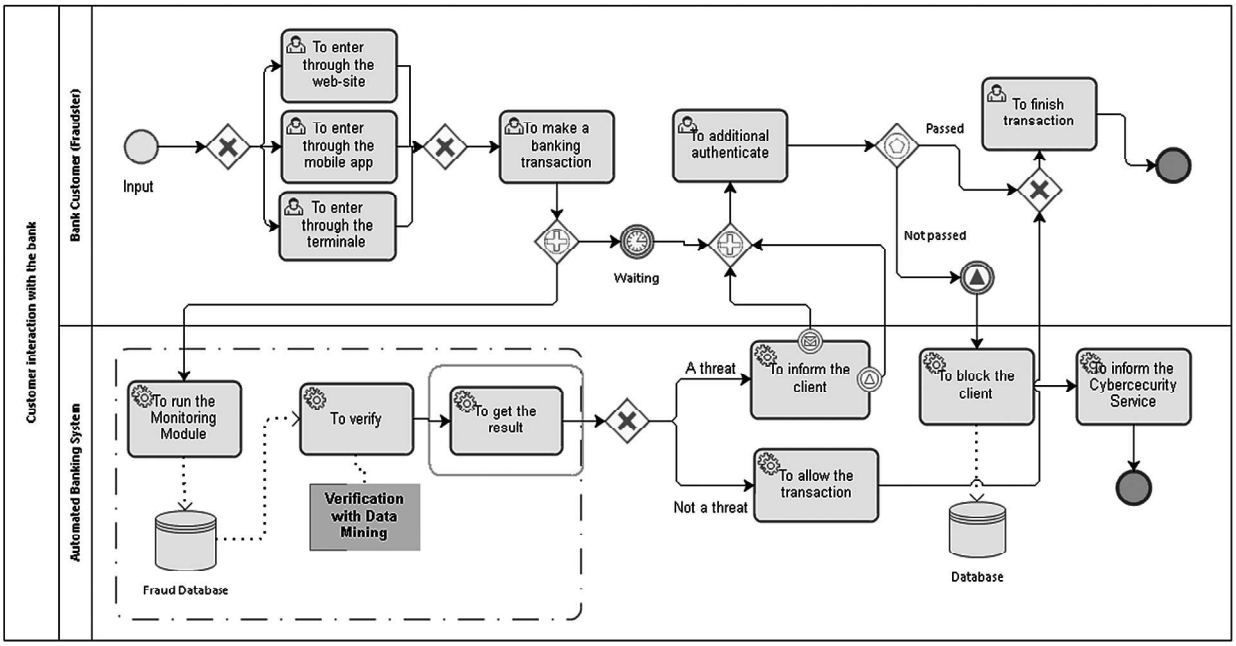

Рис. 3. Схема процесу здійснення операції клієнтом банку

— правильності введених даних ("Validation of data entry") в залежності від типу транзакції ("Transaction Type"). Результати неправильних спроб ("Result of incorrect data entry") можуть сигналізувати про ймовірне зламування акаунту клієнта.

Інформація щодо ймовірні порушення, шахрайства, зламування надходить до бази даних шахрайств ("Fraud Database"), обробляється. Результати моніторингу ("The Result of Monitoring") передаються відділам IT ("IT Department") та кібербезпеки банку ("Cybersecurity Service").

У відповідністю із запропонованою інформаційною моделлю (рис. 2) розроблено схему процесу здійснення операції клієнтом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (Business Process Model and Notation) [7] із використанням програмного забезпечення "Bizagi Modeller" (рис. 3).

Процес виглядатиме так (рис. 3):

1) клієнт банку або потенційний шахрай ("Bank Customer (Fraudster)") здійснює вхід до системи або з використанням веб-сайту, або мобільного пристрою, або терміналу;

2) клієнт банку або потенційний шахрай здійснює операцію ("To make a banking transaction");

3) АБС ("Automated Banking System") перевіряє операцію на наявність ознак шахрайства із застосуванням модулю моніторингу, в якому реалізовано методи інтелектуального аналізу ("Verification with Data Mining"). Перевірка проводитиметься за тими критеріями, які представлені на рисунку 2, та які сформовані у базі даних ("Fraud Database");

4) якщо результат перевірки не виявляє ознак потенційного шахрайства, то система дозволяє здійснити операцію ("To allow the transaction") та клієнт її завершує ("To finish the transaction");

5) якщо результат перевірки виявляє ознаки шахрайства, система робить запит на підтвердження операції шляхом sms-повідомлення або дзвінка, або іншим способом ("To inform the client");

6) клієнт здійснює додаткову аутентифікацію ("To additional authenticate");

7) якщо операція була ініційована клієнтом, то її успішно буде завершено;

8) у випадку, якщо клієнт виявиться шахраєм, тобто він не зможе пройти додаткову аутентифікацію, то його буде заблоковано ("To block the client") та проінформовано систему безпеки ("To inform the Cybersecurity Service").

Що стосується випадків внутрішніх шахрайств, то було розроблено інформаційну модель виявлення шахрайства, якщо шахраєм виступає персонал банку, у нотації DFD (рис. 4).

Модель, представлена на рисунку 4, відображає інформаційні потоки, які циркулюють в процесі перевірки модулем моніторингу ("Data Monitoring") операцій ("Bank operation"), що здійснюються персоналом банку ("Staff") на предмет виявлення ознак шахрайства. Перевіряються:

— активності рахунку ("Activity Verification") у випадку, коли персонал у власних цілях використовує "сплячі рахунки" ("Sleeping Account");

— власники рахунку ("Owner Verification"), якщо власник присутній у "чорному списку" або є іноземцем, померлим тощо ("Owner from "The black list"");

— ліміти по операціям, що здійснюються у відповідності із вимогами НБУ, політикою банку, посадовими інструкціями тощо ("Limit Verification"), в результаті чого виявляються надлишки по лімітам ("Excess of transaction limits");

— активності банківських співробітників ("Frequency of operations") на предмет дотримання банківських нормативів, які співробітник може перевищувати чи недовиконувати ("Discrepancy or excess");

— операції працівників на відповідність належним їм правам доступу ("Verification of access rights"). Це може бути випадок, коли працівники перевищують свої права ("Excess of access rights") і, наприклад, проводять операції, які не відповідають їх функціональним обов'язкам та посадовим інструкціям;

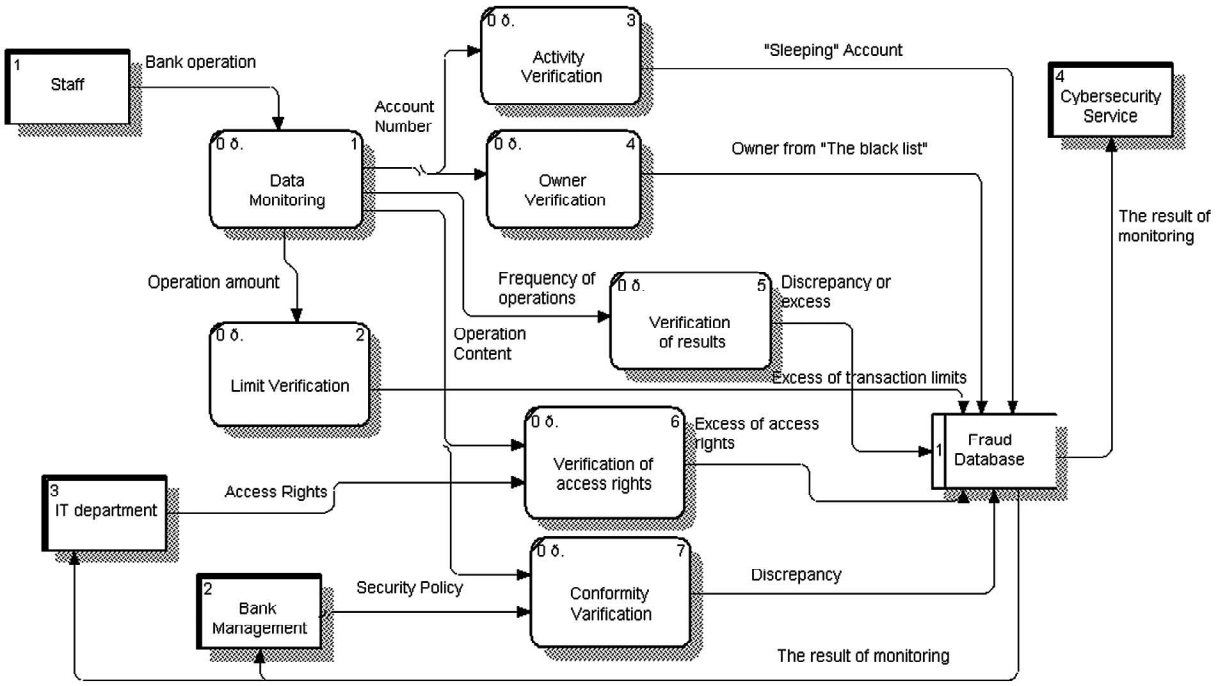

Рис. 4. Інформаційна модель виявлення ознак шахрайств персоналу банку

— операції працівників на відповідність політиці безпеці банку ("Conformity Verification"). Це можуть бути випадки копіювання бази даних, користування некорпоративною поштою, перегляду рахунків клієнтів, особливо VIP-клієнтів тощо.

Результати накопичуються у базі даних шахрайств, обробляються та надсилаються відділу кібербезпеки банку ("Cybersecurity Service"), IT-відділу ("IT Department) та менеджменту банку ("Bank Management").

У відповідністю із запропонованою інформаційною моделлю (рис. 4) розроблено схему процесу здійснення операції персоналом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (рис. 5).

Процес виглядатиме так:

1) банківський співробітник, який може бути потенційним шахраєм, ("Bank clerk (Fraudster)") авторизується в банківській системі ("To authorize in the banking system") та здійснює банківську операцію ("To make the banking operation");

2) АБС ("Automated Banking System") перевіряє операцію на предмет шахрайства ("Verification with Data Mining") із використанням критеріїв ("Fraud Database"), представлених в інформаційні моделі на рисунку 4;

3) якщо операція відповідає всім критеріям та не містить ознаки шахрайства з боку персоналу, то система дозволяє здійснення операції ("To allow the operation") та працівник її завершує ("To finish the operation");

4) якщо система виявляє ознаки шахрайства, то вона повідомляє керівника відповідного департаменту ("Head of department"), де було здійснено операцію, який аналізує інформацію ("To analyse") та приймає рішення ("To make a decision");

5) якщо операція допустима, то працівник отримує дозвіл ("Resolution") та завершує операцію;

6) в протилежному випадку операція блокується ("To block the operation") та інформація надходить до служби безпеки ("To inform the Cybersecurity Service").

ВИСНОВКИ

Реалізація запропонованих моделей дозволить виявити передумови та ознаки, наслідком яких може бути здійснення шахрайства або протиправної дії, або дії, яка призведе до негативних наслідків як для банка, так і для клієнта. Їх побудова із використанням системного підходу дозволить поєднати всіх учасників незалежно від належності до їх зовнішнього чи внутрішнього середовища. Розроблені моделі слугують передумовою для створення автоматизованого модулю моніторингу для перевірки банківських операцій та транзакцій на предмет наявності ознак шахрайства. Це продиктовано необхідністю у інструментах, які системно вирішують проблеми виявлення та попередження шахрайств у банках. В результаті цей підхід сприятиме комплексній інтеграції всіх бізнес-процесів банку в єдину автоматизовану банківську систему. Врешті-решт впровадження автоматизованої системи моніторингу підвищить ефективність системи управління за рахунок своєчасного попередження та оперативного прийняття рішення.

НАПРЯМИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У подальшому планується: розробити прототип автоматизованого модулю моніторингу для виявлення шахрайських операцій з можливістю його подальшої інтеграції в автоматизовану банківську систему; розробити проект нормативних внутрішньобанківських інструкцій щодо організації автоматизованої банківської системи як складової кібербезпеки в банках.

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".

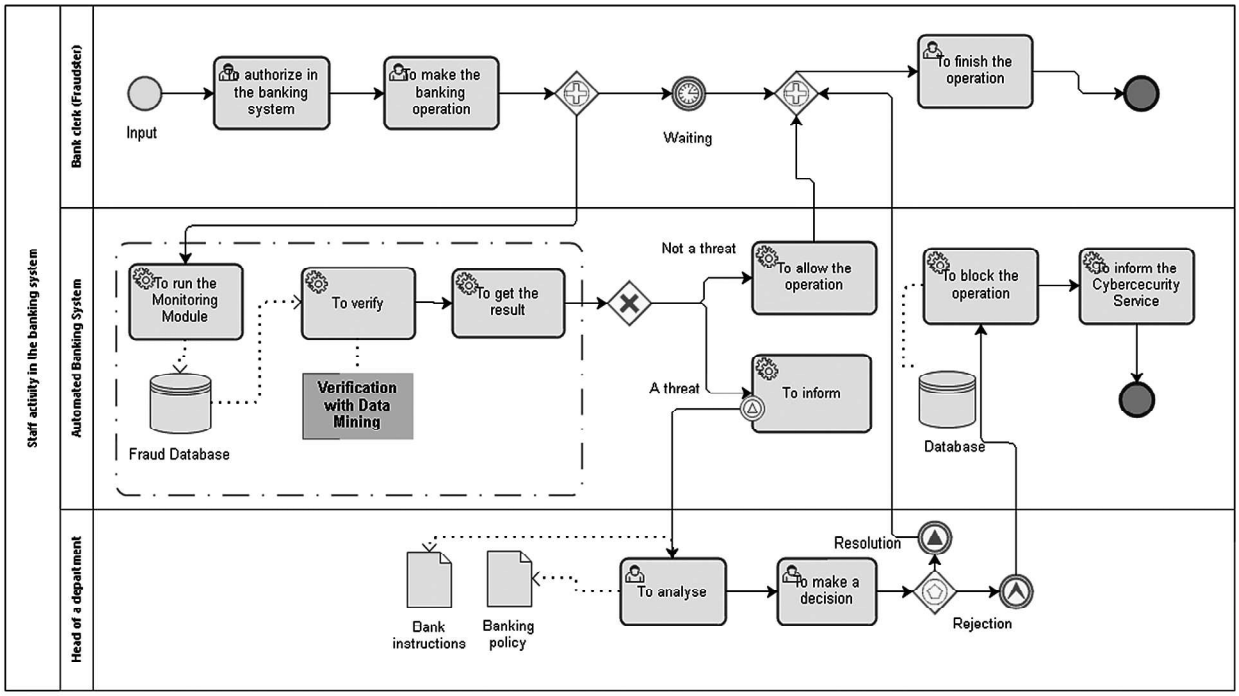

Рис. 5. Схема процесу здійснення операцій персоналом банку

Література:

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

2. Статистика платежного мошенничества — итоги 2017-го года (ИНФОГРАФИКА) [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем ЕМА. — 2018. — Режим доступу: https://ema.com.ua/cyberfraud-ema-statistics-results-2017/

3. Постанова НБУ № 95 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" від 28.09.2017 [Електронний ресурс] // Офіційний вебпортал Верховної Ради України. — 2017. — Режим доступу: http://zakon3.rada.gov.ua/laws/show/v0095500-17

4. SAS Fraud Management [Електронний ресурс] // The official site of the company "SAS". — Режим доступу: https://www.sas.com/en_us/software/fraud-management.html

5. IT threat evolution Q3 2017. Statistics [Електронний ресурс] / R.Unuchek, F. Sinitsyn, D. Parinov, A. Liskin // The official site of the company "AO Kaspersky Lab". — 2017. — Режим доступу: https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/

6. AllFusion® Process Modeler Data Flow Diagramming. Design Guide r7.2 [Електронний ресурс] / / The official site of the company "CA". — 2006. — Режим доступу: https://supportcontent.ca.com/cadocs/0/e002761e.pdf

7. Business Process Model and Notation (BPMN) Version 2.0 [Електронний ресурс] // The official site of the company "Object Management Group". — 2011. — Режим доступу: http://www.omg.org/spec/BPMN/2.0

References:

1. 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 18 June 2018).

2. The official site of the Ukrainian Interbank Association of Payment System Members EMA (2018), "The statistics of payment fraud — the results of 2017 (INFOGRAFIKA)", available at: https://ema.com.ua/cyberfraud-ema-statistics-results-2017/ (Accessed 18 June 2018).

3. The Verkhovna Rada of Ukraine (2017), The Resolution of the NBU "On Approval of the Provision on the Organization of Measures to Ensure Information Security in the Banking System of Ukraine", available at: http://zakon3.rada.gov.ua/laws/show/v0095500-17 (Accessed 18 June 2018).

4. The official site of the company "SAS" (2018), "SAS Fraud Management", available at: https://www.sas.com/en_us/software/fraud-management.html (Accessed 18 June 2018).

5. The official site of the company "AO Kaspersky Lab" (2017), "IT threat evolution Q3 2017. Statistics", available at: https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/ (Accessed 18 June 2018).

6. The official site of the company "CA" (2006), "AllFusion® Process Modeler Data Flow Diagramming. Design Guide r7.2", available at: https://supportcontent.ca.com/cadocs/0/e002761e.pdf (Accessed 18 June 2018).

7. The official site of the company "Object Management Group" (2011), "Business Process Model and Notation (BPMN) Version 2.0", available at: http://www.omg.org/spec/BPMN/2.0 (Accessed 18 June 2018).

Стаття надійшла до редакції 26.06.2018 р.