Розділ 3

Моделі та технології обробки фінансової інформації

УДК: 336.71.078.3 DOI: http://dx.doi.org/10.18371/fcaptp.v2i19.56924

Сапон Р. В.
студент, Харківський інститут банківської справи Університету банківської справи Національного банку України; Україна;
e-mail: ruler92@bk.ru;
Шамов С. О.
к. т. н., доцент, Харківський інститут банківської справи Університету банківської справи Національного банку України; Україна
e-mail: shamov@khibs.edu.ua

УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЇ КЛІЄНТІВ ПІД ЧАС ДИСТАНЦІЙНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ

Анотація. В статті розглянуто актуальні проблеми, пов'язані з вивченням клієнтів банку, зокрема з процесом їх ідентифікації, під час дистанційного банківського обслуговування Проаналізовано можливості використання банками України досвіду іноземних банків. Запропоновано розширення системи заходів щодо отримання клієнтської інформації та удосконалену модель дистанційного банківського обслуговування.

Ключові слова: ідентифікація, вивчення клієнтів, фінансовий моніторинг, дистанційне банківське обслуговування, Інтернет, інформаційні технології.

Формул: 0; рис.: 2; табл. 0; бібл.:16.

Sapon R. V.
student, Kharkiv Institute of banking of the University of banking of the National bank of Ukraine, Ukraine;
e-mail: ruler92@bk.ru;
Shamov S. O.
PhD of Technical , Associate Professor, Kharkiv Institute of banking of the University of banking of the National bank of Ukraine, Ukraine;
e-mail: shamov@khibs.edu.ua

IMPROVEMENT OF CLIENTS IDENTIFICATION TECHNOLOGIES DURING PROVIDING REMOTE BANKING SERVICES

Abstract. The actual issues related to the study of the bank's clients, including the process of identification during the remote banking are considered in the article. The possibilities of using the foreign banks' experience are analyzed. The extension of measures to obtain customer information and improved model of remote banking are proposed.

The experience of foreign banks indicates the presence of a wide range of opportunities to improve the quality of identification and study of their clients as remote banking service. The proposed system of additional measures to identify and study of clients can be implemented in Ukrainian banks implemented remote banking processes according to the proposed improved model of remote banking service. Regulations that govern the activities of Ukrainian banks regarding customer identification and examination of operations do not include many aspects of remote banking services and need revision, particularly for the possibilities of action under the proposed improved model of remote banking service.

Keywords: identification, studying customers, financial monitoring, remote banking service, Internet, information technology.

Formulas: 2; tabl.: 0, bibl.: 16

JEL Classification: E 58, O 17, L 51.

Сапон Р. В.
студент, Харьковский институт банковского дела Университета банковского дела Национального банка Украины; Украина;
e-mail: ruler92@bk.ru;
Шамов С. А.
к. т. н., доцент, Харьковский институт банковского дела Университета банковского дела Национального банка Украины; Украина;
e-mail: shamov@khibs.edu.ua

СОВЕРШЕНСТВОВАНИЕ ТЕХНОЛОГИЙ ИДЕНТИФИКАЦИИ КЛИЕНТОВ ВО ВРЕМЯ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Аннотация. В статье рассмотрены актуальные проблемы, связанные с изучением клиентов банка, в частности с процессом их идентификации, при дистанционного банковского обслуживания Проанализированы возможности использования банками Украины опыта иностранных банков. Предложено расширение системы мероприятий по получению клиентской информации и усовершенствованную модель дистанционного банковского обслуживания.

Ключевые слова: идентификация, изучение клиентов, финансовый мониторинг, дистанционное банковское обслуживание, Интернет, информационные технологии.

Формул:; рис .: 2; табл. ; библ.: 16.

Вступ. Впродовж останніх років Україна знаходиться серед країн з найбільшою часткою тіньової економіки, обсяги підозрілих банківських операцій постійно зростають [1]. Не дивно, що за даними рейтингових агентств рівень галузевих ризиків в нашій країні дуже високий, що створює бар'єри на шляху інвестицій у вітчизняну економіку [1].

Однією з причин такої ситуації є недостатня увага банків до вивчення своїх клієнтів. Підтвердженням цього є частка проблемних кредитів у вітчизняній банківській системі, яка складає близько 40% [1]. Ризик легалізації через банки коштів, отриманих злочинним шляхом, є дуже високим. Крім того зростає рівень шахрайства, яке спеціалізується на підробці документів необхідних для надання в банк [2].

Тому недостатньо якісне вивчення клієнтів є актуальною проблемою не тільки для українських банків, а й для української економіки в цілому.

Аналіз досліджень та постановка завдання. Вивченню цієї проблеми, пошуку ефективних шляхів її розв'язання присвятили свої праці численні вітчизняні та закордонні вчені: Барановський О. І., Ващенко О. М., Глущенко О. О., Дмитров С. О., Колодовський М. В., Куришко О. О., Медвідь Т. А., Наполеоні Л., Нордвік М., Олсон М., Прошунин М. М., Шотт Поль Алан та інші.

З метою розв'язання проблеми вивчення клієнтів банків, виявлення і відстеження підозрілих операцій та протидії спробам використання банків для легалізації кримінальних доходів та для фінансування терористичної діяльності в Україні створено дворівневу систему фінансового моніторингу. Діяльність суб'єктів фінансового моніторингу постійно вдосконалюються, розробляються нові рекомендації, проте ефективність цього недостатня. Крім того, банківський бізнес поступово переходить у віртуальний інформаційний простір – все більше установ починають обслуговувати клієнтів дистанційно, за допомогою SMS-повідомлень чи мережі Інтернет. Це створює нові загрози шахрайства для банків та їх клієнтів. Хоча віртуалізація банківського обслуговування ще не набула масового характеру, потрібно вже сьогодні розробляти нові методи вивчення клієнтів, засоби захисту від шахраїв та рекомендації щодо дистанційного обслуговування клієнтів банку.

Однак ця потреба ще не набула достатньої уваги з боку наукової спільноти. Вкрай обмежена кількість робіт щодо аналізу цієї потреби, досвіду її задоволення, теоретичного обґрунтування, методичної, технічної та технологічної реалізації відповідних інноваційних механізмів.

Тому метою даного дослідження стали аналіз досвіду і визначення перспективних механізмів забезпечення якості вивчення клієнтів при здійсненні дистанційного банківського обслуговування (ДБО).

Результати дослідження. Згідно нормативних [3-5] вивчення клієнта банку – обов'язковий процес отримання інформації щодо ідентифікації клієнта у випадках, передбачених законодавством, та вивчення його фінансової діяльності в процесі обслуговування для подальшого здійснення аналізу, перевірки, уточнення, узагальнення отриманої інформації (даних) та оцінки, моніторингу ризику клієнта.

Інформація, яка надходить до банку безпосередньо від клієнта, має бути документально підтвердженою [4], щоб мати відповідний рівень достовірності, найбільш повно характеризувати клієнта, мати достатній рівень формалізації. Крім того, банк має допускати поглиблене вивчення клієнта: пошук публічної інформації у ЗМІ, контакти з близькими особами клієнта, представниками керівництва з місця роботи, запити до різних бюро кредитних історій, в т. ч. ЄІС «Реєстр позичальників» НБУ, а також будь-яка можлива інформація з інших банків [5].

Проведення описаних вище дій має на меті отримання інформації:

- про особу клієнта;
- про джерела та обсяги надходження коштів на рахунки;
- про суть діяльності клієнта.

Кожен банк має вести електронні анкети, які повинні містити всю інформацію, отриману банком за результатами ідентифікації, вивчення клієнта, у тому числі результати оцінки фінансового стану клієнта, щоквартального аналізу його фінансових операцій, уточнених даних щодо ідентифікації та вивчення клієнта, а також висновки банку щодо репутації клієнта та оцінки ризику клієнта [5]. Вимагається встановлювати рівень ризику клієнта з урахуванням таких основних складових: ризику за типом клієнта, ризику послуги та географічного ризику [6].

Аналізуючи ці вимоги не важко помітити, що вони розраховані переважно на традиційні форми банківського обслуговування і в умовах ДБО стикаються із складністю або неможливістю забезпечення достовірності отриманої інформації, встановлення місця знаходження клієнта, суті його діяльності і призначення послуги, за якою він звертається.

Поряд з тим банк, що здійснює ДБО, наражається на значні ризики, пов'язані з шахрайством. Для мінімізації їхнього впливу банки використовують різні види захисту: одно- та багаторазові паролі, цифрові підписи, SMS-інформування та ін. [7]. Такі заходи виявляються досить ефективними, якщо застосовуються до клієнтів, які вже були ідентифіковані банком одного разу.

Говорячи про первинну ідентифікацію, на сьогодні такої можливості в рамках дистанційного обслуговування банки не мають. Хоча згідно діючого законодавства мають бути дотримані певні умови: 1) особиста присутність клієнта; 2) надання оригіналів документів; 3) здійснення ідентифікації уповноваженою особою банку; 4) підтвердження її проведення копіюванням відповідних документів [8], – розвиток банківської системи та банківських технологій невдовзі може дійти до повного дистанційного обслуговування, коли відносини між клієнтом і банком будуть здійснюватися лише через мережу Інтернет, а банки матимуть лише одне головне відділення. Такі тенденції вже сьогодні спостерігаються в розвинутих країнах [9], що дає привід говорити про те, що невдовзі українські банки почнуть використовувати дану практику і в нашій країні.

В більшості країн, які є учасницями ФАТФ, вимоги з ідентифікації клієнтів банками [10] закріплені законодавчими актами. Процес ідентифікації проводиться на основі наданих клієнтом чинних документів, які містять повну і всебічну інформацію про клієнта. Порядок ідентифікації своїх клієнтів кожен банк визначає самостійно згідно розроблених внутрішніх програм. Але завжди для ініціації відносин із банком

клієнту потрібно представити офіційний документ, що містить фотографію і підпис. Найчастіше це посвідчення особи, паспорт, водійські права, карта соціального страхування та спеціальні посвідчення іноземців або біженців. Можуть бути представлені і такі документи, як свідоцтво про шлюб, муніципальна карта особистості, військове посвідчення, картка поліцейського або посвідчення, видане банком [11].

Згідно з рекомендаціями Базельського комітету, приймаючи документи від клієнта дистанційно, банки повинні забезпечити виконання наступних вимог [12]:

1) банки мають застосовувати настільки ж ефективну процедуру ідентифікації та постійний моніторинг, як і до клієнтів, з якими можна спілкуватися особисто;

2) мають існувати специфічні та адекватні заходи для зменшення більшого ризику.

Для виконання цих рекомендацій іноземними банками вживається широкий спектр заходів.

У Скандинавських країнах часто запитується *персональний ідентифікаційний номер*, а при відкритті депозитного рахунку в США повинні бути представлені ідентифікаційний номер платника податків або *номер соціального страхування*.

У Данії приймаються тільки ті документи, які важко підробити. Фактично система вимагає, щоб продавці послуг вивчали в обов'язковому порядку *принаймні два документи, а частіше три і більше*.

В Японії поширена практика *відвідування клієнта за вказаною адресою* [11].

У ряді країн проводяться додаткові перевірки.

У Бельгії банки повинні *встановлювати додаткову інформацію* про своїх клієнтів (професія, склад родини, зміна адреси, і т.д.).

У Сінгапурі та Великобританії, по можливості, з клієнтом проводять *особисту співбесіду*.

У Франції передбачається *аналіз поведінки клієнта* – банк, що відкриває рахунок клієнту, який проявляє поспішність, може поцікавитися його заборгованостями [11].

У США для відкриття рахунків на великі суми або при проведенні великих операцій потрібно, щоб клієнт забезпечив ідентифікацію і вказав *номери рахунків у попередньому банку* і, якщо такі є, необхідно підтвердити їх правильність.

З аналізу матеріалів Базельського комітету з банківського нагляду чітко видно, що банки отримують все більше і більше запитів на відкриття рахунків на ім'я клієнтів, з якими не проводиться особистої співбесіди при особистій присутності. Ця практика набуває все більшого поширення з розвитком поштових, телефонних та електронних банківських послуг.

Найбільш яскравим прикладом клієнта, що не присутній особисто при відкритті рахунку, Базельський комітет з банківського нагляду вважає особу, яка виявила бажання відкрити банківський рахунок через Інтернет або аналогічну електронну систему віддаленого телекомунікаційного доступу [12]. При цьому слід зазначити, що досить закритий міжнародний характер електронних банківських послуг у поєднанні зі швидкістю здійснення операцій неминуче створює труднощі в ідентифікації клієнтів.

З урахуванням зазначеної проблематики, Базельський комітет з банківського нагляду пропонує використовувати такі заходи, як: *незалежний контакт банку з клієнтом; рекомендації третіх сторін; запит на проведення першого платежу через рахунок, відкритий на ім'я клієнта в іншому банку, що використовує аналогічні стандарти перевірки клієнтів* [12].

Прикладом іншого підходу до вирішення даної проблеми може послужити досвід Німеччини, в національному законодавстві якої передбачена норма, що допускає як виняток відкриття рахунку без особистої присутності клієнта, за умови, що *клієнт особисто відомий співробітникам банку і вони готові персонально гарантувати його особистість* при укладанні договору банківського рахунку [11]. Проте відкрити рахунок віддалено в Німеччині сьогодні в деяких банках можна також за допомогою

надання необхідних документів у поштовому відділенні або з використанням *паспортів нового зразка з мікро-чіпами*, проте для цього знадобиться певне обладнання [9].

У РФ однією з найбільш поширених схем, використовуваних банками для обходу вимог п. 5 ст. 7 Закону № 115-ФЗ, що забороняє відкривати рахунки (вклади) фізичним особам без особистої присутності особи, яка відкриває рахунок (вклад), або його представника, є використання конструкції, що ґрунтується на *видачі клієнтом доручення на відкриття рахунку спеціальному агенту або співробітнику банку* [11]. Крім того, на сьогоднішній день в Росії розробляються поправки до законодавства, які дозволять відкривати рахунку віддалено, використовуючи *інформацію інших фінансових установ*, які вже здійснили ідентифікацію клієнта [13].

Унікальний механізм ідентифікації особи в інтернеті не так давно з'явився в Америці. Американська компанія «miiCard» підтверджує особу користувача за п'ять хвилин і дозволяє здійснювати в інтернеті операції, що вимагають ідентифікації – наприклад, отримувати кредит в банку, не виходячи з дому [14]. «miiCard» просить користувача *авторизуватися через інтернет-банк свого банку*. По-перше, інформація по банківському рахунку відома тільки самому користувачеві і кредитній організації. А, по-друге, регулярне здійснення операцій в інтернет-банку дозволяє «miiCard» актуалізувати інформацію про користувача.

Таким чином, основними способами дистанційної ідентифікації клієнтів зарубіжних банків є:

використання інформації інших банків;

використання унікального ідентифікатора (чіповані посвідчення);

аутсорсинг – ідентифікацію здійснює третя сторона за допомогою власних баз даних.

Аналізуючи можливості використання цих способів українськими банками, одразу можна відкинути варіант з використанням інформації інших банків – по-перше, ним вирішується проблема первинної ідентифікації, коли має місце перше звернення клієнта до банку, по-друге, у вітчизняній практиці рідко зустрічаються випадки, коли людина користується послугами декількох банків. Використання унікального ідентифікатора та послуг аутсорсингу розглянемо далі. Перед цим слід висвітлити 2 моменти.

По-перше, 18.10.2012 прийнято Закон України Про електронний цифровий підпис [15] (ЕЦП). ЕЦП може отримати як юридична, так і фізична особа. Використовується він для ідентифікації підписанта та підтвердження цілісності даних в електронній формі і прирівнюється до власноручного підпису (печатки). На сьогоднішній день банки України використовують ЕЦП у своїй практиці ДБО. Вони мають право видавати своїм клієнтам особисті ЕЦП згідно Постанови Правління НБУ 17.06.2010 № 284. Під час видачі ЕЦП оформлюється відповідний сертифікат і вносяться відомості до спеціального захищеного довідника ключів. Отримувач документа з ЕЦП може з легкістю звернутися до такого довідника і перевірити особисті дані власника ЕЦП та термін дії сертифікату на нього.

По-друге, в Україні існує Єдина державна інформаційна система (ЄДІС) [16], яка використовується для запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансуванню тероризму. Державною службою фінансового моніторингу України (ДСФМУ), Національною комісією з цінних паперів і фондового ринку, Національною комісією, що здійснює державне регулювання у сфері ринків фінансових послуг, Національним банком України (НБУ), Службою безпеки України, Міністерством внутрішніх справ, Міністерством юстиції, Міністерством економічного розвитку і торгівлі, Міністерство фінансів, Державною фіскальною службою, Державною митною службою, Адміністрацією Державної прикордонної служби, Фондом державного майна, Державною фінансовою інспекцією, Державною службою статистики, Державною реєстраційною службою, Державним

агентством земельних ресурсів.

Два дані аспекти можна використати з метою підвищення рівня надійності клієнтської інформації та зниження ризиків шахрайства.

Удосконалена IDEF0-модель обслуговування клієнта банку, з використанням ЕЦП як унікального ідентифікатора та залучення ЄДІС для ідентифікації клієнтів, має вигляд, що наведено на рис. 1. На рисунку тонкими лініями та звичайним шрифтом відображені складові традиційної моделі ДБО, а складові, які пропонується удосконалити або додати – товстими лініями і напівжирним шрифтом.

По-перше, наведена модель містить удосконалений порядок ідентифікації клієнта, який передбачає (А1):

1) фізична особа, яка планує стати клієнтом банку, має паспорт, ІНН, ЕЦП, а її особисті дані занесені до баз даних ЄДІС (таке занесення може здійснюватись підчас видачі їй паспорту громадянина України, а для іноземних громадян підчас їх реєстрації на території України, або підчас її першого у житті звернення до будь-якого українського банку);

2) фізична особа реєструється на сторінці банка в Інтернеті, формуючи електронний документ-заяву на обслуговування, до якого вносить особисту інформацію;

3) отримані клієнтські дані верифікуються банком шляхом порівняння з даними ЄДІС (такий функціонал застосовується в деяких автоматизованих банківських системах (АБС) під час верифікації документів: дані, введені одним операціоністом, «накладаються» на дані, введені іншим);

4) якщо дані збігаються, то клієнт вважається таким, що пройшов первинну ідентифікацію;

5) в іншому випадку – банк відмовляє клієнту в обслуговуванні.

За встановленим регламентом, співпрацювати з ЄДІС напряму банки не можуть. У зв’язку з цим, виникає необхідність у наявності посередника, роль якого зможе виконувати спеціально створене бюро чи підрозділ ДСФМУ або НБУ. Таким чином, співробітники банку не матимуть доступ до інформації ЄДІС, а лише отримуватимуть повідомлення про збіг чи розбіжність даних.

Після того, як особистість клієнта встановлено (А1) і відбулась його авторизація (А2), на наступному етапі (А3) слід отримати іншу необхідну інформацію, встановлену законодавством: місце роботи та посада, розмір заробітної плати, рухоме та нерухоме майно, рахунки в інших банках та ін. Для підвищення якості такої інформації клієнт, вказуючи її, має також вказати джерела, які можуть підтвердити її. Якщо їх не вказано, банк може звернутися до вказаного роботодавця, іншого банку, надіслати запити до реєстрів майна. Згідно із законодавством, банк має право витребувати інформацію, яка стосується ідентифікації цієї особи та її керівників, до органів державної влади, банків, інших юридичних осіб, а також здійснювати заходи щодо збору такої інформації з інших джерел. Вказані органи державної влади, банки, інші юридичні особи зобов'язані протягом десяти робочих днів з дня отримання запиту безоплатно надати банку таку інформацію [3].

Крім описаних вище заходів, можна запропонувати й інші заходи і засоби, здатні підвищити якість клієнтської інформації. По-перше, це ведення довідників (М8), за якими перевірятимуть отримані від клієнтів дані. Це можуть бути довідники населених пунктів з чітким розмежуванням по областям, районам, селищним радам, районних відділень управління МВС. Якщо вказане клієнтом місце проживання або місце видачі паспорту не буде відповідати вказаній області чи району, йому буде відмовлено в реєстрації. Проте ведення таких довідників є важким завданням. Крім того, що їх потрібно не тільки заповнити, важливо також підтримувати актуальність інформації, що в них міститься.

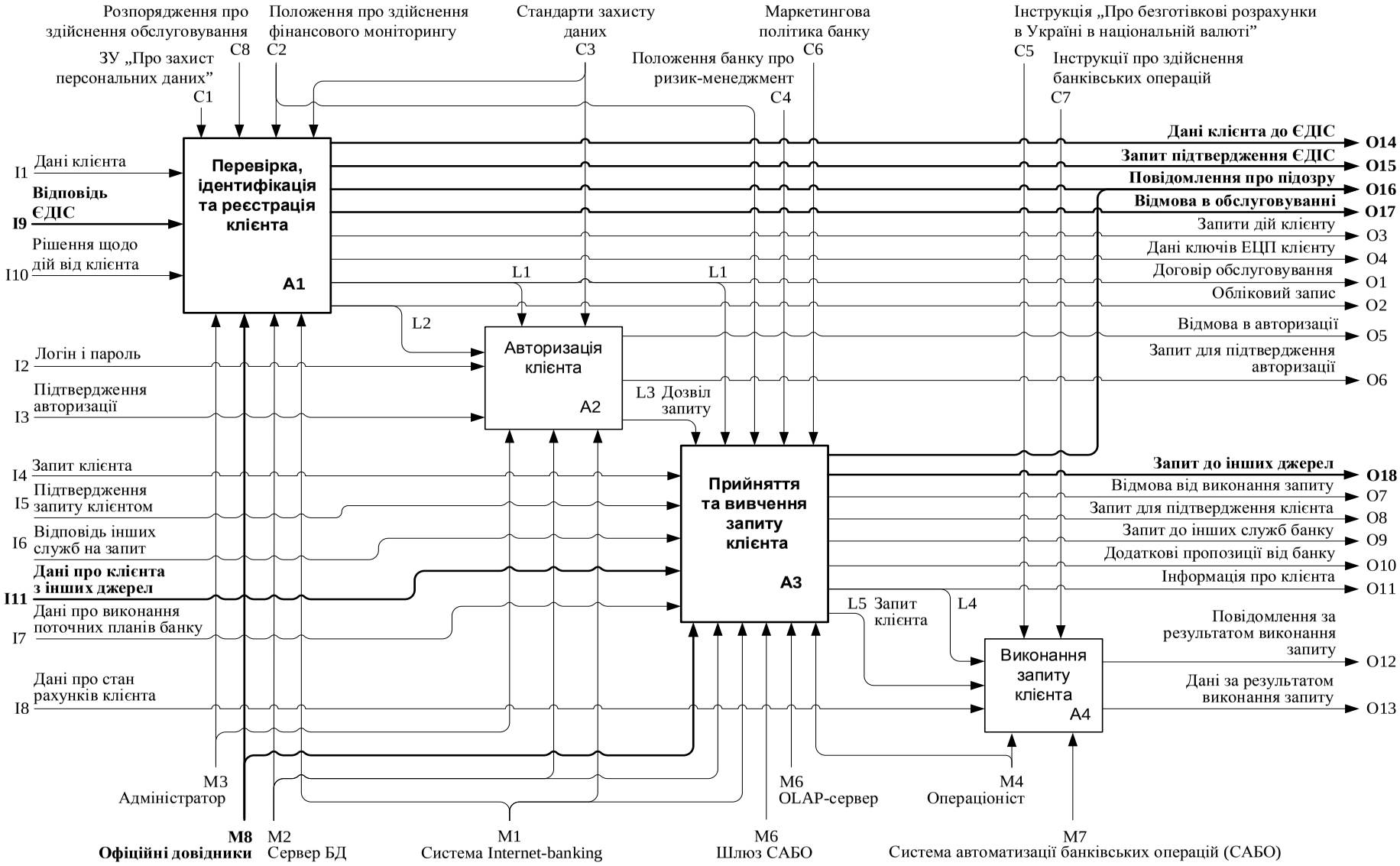

Рис. 1. Модель процесу обслуговування клієнта банку (розробка авторів).

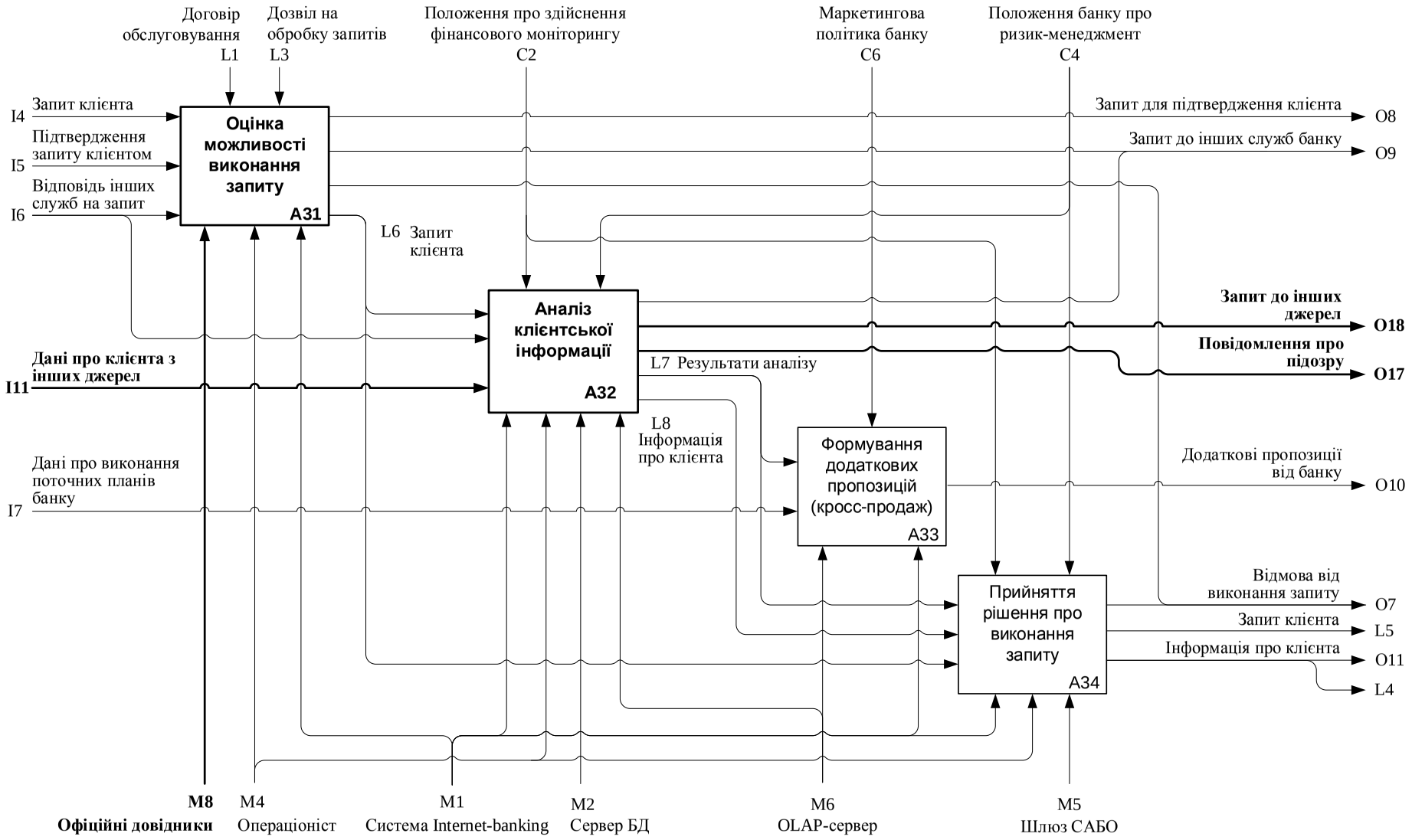

Рис. 2. Модель підпроцесу врахування та вивчення запиту клієнта банка (розробка авторів).

Ще одним обов'язковим заходом (в А1 і А3) має бути *перевірка правильності і відповідності отриманим даним клієнта значень всіх введених клієнтом ідентифікуючих кодів і реквізитів документів.*

Як зазначено вище, варіантом підтвердження достовірності клієнтської інформації є її *порівняння з інформацією державних реєстрів*, ЄДІС. Та, враховуючи обсяги таких реєстрів, ймовірність допущення в них помилки не виключена, а отже для банку існує ризик прийняття стосовно клієнта помилкових рішень. Тому важливо, щоб банк не обмежувався лише державними реєстрами та перевіряв клієнтську інформацію всіма доступними способами. Одним з джерел додаткової інформації для такої перевірки можуть бути *соціальні мережі*. Сьогодні переважна частина економічно активного населення України має в них профілі з вказаною особистою інформацією та світлинами. Крім того, додаткову інформацію про особу можна знайти за допомогою *пошукових запитів в мережі Інтернет*. Проте, важливо звертати увагу, що при залученні такої інформації необхідно враховувати час її появи та її характер, оскільки можливе її навмисне створення для дезінформації.

Як відомо, сучасні технології дозволяють робити миттєві фото та відправляти їх через Інтернет. Тому ще одним способом підтвердження наданої клієнтом інформації може бути запит банком «селфі» клієнта, зробленого за допомогою мобільного телефону, смартфону, планшету чи web-камери комп'ютера. Отримане фото слід проаналізувати з урахуванням додаткової інформації про фото: дата та час зйомки, автор, гео-таргетування.

Врахування наведених пропозицій на етапі прийняття та вивчення запиту клієнта (А3) відображено IDEF0-моделлю, наведеною на рис. 2.

Загалом, побудова удосконаленої моделі ДБО, представленої на рис. 1 і рис. 2, шляхом відображення запропонованих заходів у складові моделі існуючого процесу ДБО та її доповнення, свідчить про можливість впровадження цих заходів у процеси ДБО, здійснювані банками в Україні.

Висновки

1. Досвід іноземних банків свідчить про наявність широкого спектру можливостей для підвищення якості ідентифікації та вивчення їх клієнтів за мов дистанційного банківського обслуговування.
2. Запропонована система додаткових заходів щодо ідентифікації і вивчення клієнтів може бути впроваджена у здійснювані українськими банками процеси дистанційного банківського обслуговування відповідно до запропонованої удосконаленої моделі дистанційного банківського обслуговування.
3. Нормативні документи, які регламентують заходи українських банків щодо ідентифікації клієнтів та вивчення їх операцій, не враховують багатьох аспектів дистанційного банківського обслуговування і потребують доробки, зокрема, для забезпечення можливостей здійснення заходів відповідно до запропонованої удосконаленої моделі дистанційного банківського обслуговування.

Література

1. S&P назвал банки Украины одними из самых слабых в мире [Електронний ресурс]. – Режим доступа: http://finance.liga.net/.
2. МБКИ предупреждает: кредитное мошенничество в Украине растет [Электронный ресурс] : пресс-релиз. – Режим доступа: http://dengi.ua/clauses/125078_MBKI_preduprezhdaet_kreditnoe_moshennichestvo_v_Ukraine_rastet.html.
3. Про банки і банківську діяльність [Електронний ресурс] : закон України від 07.12.2000 р. № 2121-III. – Режим доступу: http://zakon.rada.gov.ua/.
4. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму [Електронний ресурс] : закон України від 14.10.2014 р. № 1702-VII. – Режим доступу: http://zakon.rada.gov.ua/.
5. Про затвердження Положення про здійснення банками фінансового моніторингу [Електронний ресурс] :

постанова правління НБУ від 14.05.2003 р. № 189. – Режим доступу: http://zakon.rada.gov.ua/.
6. Про затвердження Критеріїв ризику легалізації (відмивання) доходів, одержаних злочинним шляхом, або фінансування тероризму [Електронний ресурс] : наказ Державного комітету фінансового моніторингу від 03.08.2010 р. № 126. – Режим доступу: http://zakon.rada.gov.ua/.
7. Страхарчук, А. Я. Інформаційні системи і технології в банках [Текст] : навч. посіб. / А. Я. Страхарчук, В. П. Страхарчук ; Рек. Мін. освіти і науки України. – Київ : Знання, 2010. – 515 с.
8. Щодо ризиків відмивання грошей та запобіжних заходів, які необхідно застосовувати з метою мінімізації таких ризиків [Електронний ресурс] : лист НБУ від 10.01.2006 р. № 48-012/29-192. – Режим доступу: http://zakon.rada.gov.ua/.
9. «Традиционные банкиры только качали головами и крутили пальцами у виска...» : беседа с Маттиасом Кронером, CEO Fidor bank [Электронной ресурс] / Беседу вел А. Арнаутов. – Режим доступа: http://futurebanking.ru/.
10. Про Сорок рекомендацій Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) [Електронний ресурс] : постанова Кабінету Міністрів України і Національного банку України від 28 серпня 2001 р. № 1124. – Режим доступу: http://zakon.rada.gov.ua/.
11. Филимонов, М. И. Проблемы, связные с идентификацией клиента при открытии счета в коммерческом банке [Электронный ресурс] / М. И. Филимонов // Юридическая работа в кредитной организации. - 2005. – № 4. – Режим доступа: http://www.reglament.net/.
12. Належне ставлення банків до клієнтів [Електронний ресурс] : стандарти Базельського комітету банківського нагляду від 01.10.2001р. / Банк міжнародних розрахунків. – Режим доступу: http://zakon.rada.gov.ua/.
13. Кривошапко, Ю. Ничего личного: Счет разрешат открыть без визита в банк [Электронный ресурс] / Ю. Кривошапко // Российская газета. – 2013. – № 6229. – 11 ноября. – Режим доступа: http://www.rg.ru/gazeta/rg/2013/11/11.html.
14. Краснова, А. miiCard – онлайн-паспорт для идентификации в сети [Электронной ресурс] / А. Краснова. – Режим доступа: http://futurebanking.ru/.
15. Про електронний цифровий підпис [Електронний ресурс] : закон України від 22.05.2003 р. № 852-IV. – Режим доступу: http://zakon.rada.gov.ua/.
16. Про Єдину державну інформаційну систему у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансуванню тероризму [Електронний ресурс] : постанова Кабінету Міністрів України від 10.12.2003 р. № 1896. – Режим доступу: http://zakon.rada.gov.ua/.
Стаття надійшла до редакції 13.04.2015

References

1. S&P nazval Banki Ukrainy odni iz samykh slabykh v mire. Available at http:www.//finance.liga.net/
2. MBKI preduprezhdayet: kreditnoye moshennichestvo v Ukraine rastet. Available at http//www.prostobank.ua/
3. Zakon Ukrainy. (2000, hruden). Pro banky I bankivsku diialnist. Available at http://www.zakon1.rada.gov.ua/
4. Zakon Ukrainy. Pro zapobihannia ta protydiiu lehalizatsii (vidvmyvanniu) dokhodiv, oderzhanykh zlochynnym shliakhom, abo finansuvanniu teroryzmu. Available at http://www.zakon1.rada.gov.ua/
5. Postanova pravlinnia NBU. (2003, traven). Pro zatverdzhennia polozhennia pro zdiisnennia bankamy finansovoho monitorynhu. Available at http://www.zakon2.rada.gov.ua/
6. Nakaz Derzhavnoho komitetu finansovoho monitorynhu. (2010, serpen). Pro zatverdzhennia Kryteriiv ryzyku lehalizatsii (vidmyvannia dokhodiv), oderzhanykh zlochynnym shliakhom, abo finansuvannia teroryzmu. Available at http://www.zakon2.rada.gov.ua/
7. Strakharchuk, A. Ya., & Strakharchuk, V. P. (2010). Informatsiini systemy i tekhnolohii v bankakh. Kyiv: UBS NBU: Znannia.
8. Lyst NBU. (2006, sichen). Shchodo ryzykiv vidmyvannia hroshei ta zapobizhnykh zakhodiv, yaki neobkhidno zastosovuvaty z metoiu minimizatsii. Available at http://www.zakon1.rada.gov.ua
9. Arnautov, A. Traditsionnyye bankiry tolko kachali golovami i krutili paltsem u viska. Available at http://www.rebanking.ru/
10. Postanova Kabinetu Ministriv Ukrainy i Natsionalnoho Banku Ukrainy. (2001, serpen). Pro sorok rekomendatsii Hrupy z rozrobky finansovyh zakhodiv borotby z vidmyvanniam hroshei (FATF). Available at http://www.zakon1.rada.gov.ua
11. Filimonov, M. I. (2005). Problemy, sviazannyye s identifikatsiyei kliyenta pri otkrytii scheta v kommercheskom banke. Metodicheskii zhurnal Yuridicheskaia rabota v kreditnoy organizatsii, 4. Available at http://www.reglament.net/
12. Bank mizhnarodnykh rozrakhunkiv «Nalezhne stavlennia bankiv do klientiv (standarty Bazelskoho komitetu bankivskoho nahliadu)». (2001, zhovten). Available at http://www.zakon1.rada.gov.ua/
13. Krivoshapko, Yu. Nichego lichnogo. Rossiiskaia gazeta. Available at http://www.rg.ru/
14. Krasnova, A. MiiCard – onlain passport dlia identifikatsii v seti.
15. Zakon Ukrainy. (2003, traven). Pro elektronnyi tsyfrovyi pidpys. Available at http://www.zakon1.rada.gov.ua/
16. Postanova Kabinetu Ministriv Ukrainy. (2003, hruden). Pro edynu derzhavnu informatsiinu systemu u sferi zapobihannia ta protydii lehalizatsii (vidmyvanniu) dokhodiv,oderzhanykh zlochynnym shliakhom, i finansuvanniu teroryzmu. Available at http://www.zakon1.rada.gov.ua/
Received 13.04.2015