

FINANCE AND CREDIT

Дистанційний банкінг в Україні

Аврамчук Лідія Андріївна¹, Ясковець Ірина Василівна²

¹ доцент кафедри банківської справи та страхування;
Національний університет біоресурсів і природокористування України; Україна

² здобувач вищої освіти за спеціальністю «Фінанси, банківська справа та страхування»;
Національний університет біоресурсів і природокористування України; Україна

Анотація. Дистанційний банкінг є одним з найбільш популярних сервісів, який дозволяє клієнтам банків здійснювати фінансові операції за допомогою Інтернету. Цей сервіс надає зручний та швидкий спосіб контролювати свої фінанси, без необхідності відвідувати банк особисто. У дистанційному банкінгу клієнти можуть переглядати свої баланси, оплачувати рахунки, переказувати гроші, здійснювати інвестиції та багато іншого, користуючись комп'ютером або мобільним пристроєм. Він є надійним та безпечним, забезпечуючи захист персональної інформації та грошових операцій. Дистанційний банкінг надає клієнтам більш гнучкі умови для управління своїми фінансами та дозволяє їм ефективно використовувати свій час. Тому цей сервіс є дуже популярним у сучасному світі та має великий потенціал для подальшого розвитку.

Ключові слова: Дистанційний банкінг, банківські установи, фінансові послуги, управління, технології.

В останні роки фінансові технології (FinTech) набули все більшої популярності в банківській галузі. FinTech – це використання новітніх технологій для надання фінансових послуг, що дозволяє банкам оптимізувати свою діяльність та забезпечити більш ефективне обслуговування клієнтів. Одним з головних напрямків використання FinTech є дистанційний банкінг, який дозволяє клієнтам банків здійснювати фінансові операції в будь-який час та з будь-якого місця, не відходячи від комп'ютера або смартфона. Для забезпечення дистанційного банкінгу необхідно мати надійний та безпечний канал зв'язку між клієнтом та банком, а також забезпечити захист персональних даних клієнтів.

Дистанційний банкінг стає все більш актуальним у зв'язку з швидким розвитком технологій та збільшенням використання інтернету та мобільних пристроїв. Він забезпечує зручний та швидкий доступ до банківських послуг, які можна отримати з будь-якого місця та в будь-який час. Він також дозволяє клієнтам економити час та зменшувати витрати на візити до банківських відділень. Крім того, дистанційний банкінг забезпечує більш високий рівень безпеки, оскільки

FINANCE AND CREDIT

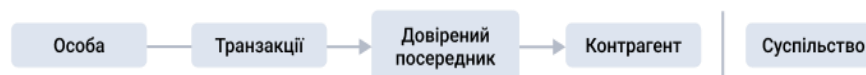
використовується сучасне шифрування та методи автентифікації користувачів. Проте, разом із зростанням популярності дистанційного банкінгу зростає й кількість ризиків, пов'язаних з цими послугами. Клієнти мають ризик бути атакованими хакерами, які можуть отримати доступ до їхніх фінансових даних. Також, існує ризик технічних помилок та збоїв, що можуть привести до втрати грошей або недоступності банківських послуг.

FinTech-підприємства надають рішення для дистанційного банкінгу, що дозволяє банкам надавати більш ефективні та зручні фінансові послуги своїм клієнтам.

Telebanking сьогодні – це банківський сервіс, заснований на використанні можливостей телефонів із тоновим набором номера. Цю форму банківського обслуговування називають ще "phonebanking". Система дозволяє клієнтові за допомогою кнопок телефонного апарата віддавати розпорядження на здійснення фінансових операцій, замовити та одержати потрібну інформацію про рух коштів на рахунку або про послугу [4]. Штучний інтелект та машинне навчання вже знайшли широке застосування у банківській галузі, де їх використовують для підвищення ефективності рішень та покращення обслуговування клієнтів. Одним з основних застосувань штучного інтелекту та машинного навчання є аналіз даних клієнтів. За допомогою цих технологій банки можуть аналізувати інформацію про попередні транзакції клієнта, його поведінку та інші дані. Окрім того, штучний інтелект та машинне навчання можуть використовуватись для запобігання шахрайства.

Blockchain-технології є децентралізованою технологією, яка дозволяє забезпечувати безпеку та конфіденційність фінансових операцій. Ці технології використовуються для створення безпечних та надійних платіжних систем, які дозволяють забезпечувати конфіденційність операцій та зменшувати ризики шахрайства. Модель конфіденційності наведена на рисунку 1. [5].

Традиційна модель конфіденційності



Нова модель конфіденційності

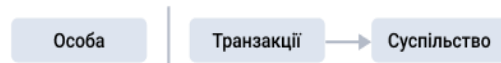


Рисунок 1

Модель конфіденційності фінансових операцій [5]

FINANCE AND CREDIT

Одним з основних принципів blockchain-технологій є децентралізація. Це означає, що дані про операції зберігаються на кожному вузлі мережі, а не в одному централізованому центрі. Це забезпечує надійність та безпеку даних, оскільки для того, щоб змінити дані, необхідно змінити їх на кожному вузлі мережі, що робить такі дії надзвичайно складними.

Також, blockchain-технології можуть забезпечувати конфіденційність фінансових операцій, оскільки вони дозволяють використовувати публічні та приватні ключі для здійснення транзакцій. При цьому приватний ключ забезпечує конфіденційність операції, оскільки тільки власник ключа може здійснити транзакцію.

Основу технології блокчейн складають декілька основоположних принципів, які можна віднести до головних переваг блокчейну (табл.1.):

Таблиця 1

Переваги блокчейн-технологій
Переваги блокчейну
1. Блокчейн є розподіленим реєстром та буде функціонувати до останнього активного мережевого вузла.
2. Доступ до історії транзакцій блокчейну мають всі учасники мережі, а повного контролю над ним не має ніхто.
3. У мережі блокчейн відсутня ієрархія, тобто серед безлічі мережевих вузлів немає головного.
4. За своєю природою блокчейн здатний забезпечити унікальне поєднання відкритості та захищеності даних користувачів. Високий ступінь надійності досягається за допомогою прогресивних методів шифрування.
5. Дані в мережі блокчейн неможливо видалити або замінити, бо вони підтверджуються безліччю мережевих вузлів.

Дані сформовано з[5]

Цифровий ідентифікатор – це унікальний код, що ідентифікує конкретну особу в мережі. Він може бути представлений у формі номера паспорта, документа, що підтверджує особу, або у формі біометричних даних, наприклад відбитків пальців чи скану обличчя. Одним з головних переваг використання цифрових ідентифікаторів є забезпечення безпеки та конфіденційності фінансових операцій.

Основними законодавчими актами, які регулюють дистанційний банкінг в Україні, є:

1. Закон України "Про банки та банківську діяльність" [1]. Цей закон містить загальні вимоги до банківської

FINANCE AND CREDIT

діяльності, які стосуються і дистанційного банкінгу. Наприклад, вимоги до зберігання інформації про клієнтів, їх транзакції та інші вимоги до організації банківської діяльності.

2. Закон України "Про захист персональних даних" [2]. Цей закон містить вимоги до зберігання, обробки та передачі персональних даних, що стосуються не лише дистанційного банкінгу, але і будь-яких інших видів обробки персональних даних.

3. Постанова Національного банку України "Про затвердження Положення про здійснення банками фінансового моніторингу" [3]. Це Положення визначає порядок здійснення банками фінансового моніторингу, а саме: організацію та забезпечення внутрішнього контролю за дотриманням вимог антикорупційного законодавства тощо.

Стосовно ризиковості дистанційного банкінгу, то серед ризиків можна виділити такі:

1. Кібербезпека: збільшення обсягів онлайн-операцій із зростанням популярності дистанційного банкінгу збільшує ймовірність кібератак та крадіжки персональних даних клієнтів. Одним з найбільших ризиків дистанційного банкінгу є безпека. До правил безпеки можуть належати використання складних паролів та двофакторної автентифікації, оновлення програмного забезпечення та запобігання використанню громадських мереж Wi-Fi.

2. Технічні проблеми: можливість відмови системи дистанційного банкінгу внаслідок технічних проблем, які можуть призвести до перерв у обслуговуванні клієнтів.

3. Адміністративні ризики: неправильна інтерпретація законодавства та порушення норм та правил банківської діяльності можуть призвести до санкцій від регулятора або негативного впливу на репутацію банку.

4. Фінансові ризики: несплата кредитів, зменшення доходів внаслідок незначних процентних ставок та зниження кількості клієнтів.

Для управління ризиками в дистанційному банкінгу використовуються такі методи:

1. Відповідальний підхід до кібербезпеки: банки повинні використовувати заходи захисту від кібератак та забезпечувати безпеку персональних даних клієнтів. Одним із методів забезпечення кібербезпеки є застосування багатофакторної аутентифікації, яка передбачає використання декількох факторів для підтвердження особи користувача. Наприклад, можна вимагати введення пароля, використання біометричних

FINANCE AND CREDIT

даних (відбитків пальців, розпізнавання голосу тощо), а також відправлення SMS-коду на мобільний телефон.

2. Розробка та впровадження стратегії управління ризиками: банки повинні мати конкретну стратегію для управління ризиками в дистанційному банкінгу та регулярно оновлювати її.

3. Забезпечення надійності систем: банки повинні мати ефективну систему контролю та моніторингу, щоб вчасно виявляти технічні проблеми та усувати їх. Одним з методів забезпечення надійності є використання різноманітних технічних засобів захисту, таких як антивіруси, фаєрволи, системи виявлення вторгнень та інші.

4. Регулярне навчання та підвищення кваліфікації тощо.

Висновки. Отже, дистанційний банкінг є важливою складовою розвитку банківської сфери, популярність якого швидко зростає. Аналіз ризиків, пов'язаних з дистанційним банкінгом, показав, що важливими аспектами управління ризиками є забезпечення кібербезпеки, регулярне навчання та підвищення кваліфікації працівників, забезпечення надійності систем, а також розробка та впровадження стратегії управління ризиками. В процесі дослідження законодавчого регулювання дистанційного банкінгу в Україні з'ясовано, що ця сфера підпорядковується ряду законодавчих актів, які регулюють умови та правила здійснення банківських операцій у дистанційному режимі. Однак, для успішного функціонування дистанційного банкінгу необхідно пильно стежити за ризиками та вживати всіх необхідних заходів для їх управління та зниження.

References:

- [1] Про банки і банківську діяльність: Закон України від 7 грудня 2000 р. Верховна Рада України. *Голос України*. 2000. 28 грудня. С. 1 – 83.
- [2] Про захист персональних даних: Закон України від 01 червня 2010 р. Верховна Рада України. *Голос України*. 2010. 1 липня 2010. С. 1 – 30.
- [3] Про затвердження Положення про здійснення банками фінансового моніторингу. Постанова Національного банку України від 19 травня 2020 р. *Голос України*. 2020. 21 травня. С. 1 – 24.
- [4] Чумак Н.В. Види дистанційного банківського обслуговування в міжнародному електронному бізнесі. Науковий вісник Ужгородського університету. Серія: Економіка. 2012. Вип. 3 (37). С. 2.
- [5] Основи та принципи технології блокчейн. URL: <http://surl.li/fwhyс> (дата звернення: 27.03.2023).