УДК 336.7

Брегеда Олена Анатоліївна
кандидат економічних наук, доцент,
доцент кафедри банківської справи та страхування
Київський національний економічний університет імені Вадима Гетьмана
Breheda Olena
Candidate of Economic Sciences, Associate Professor,
Associate Professor of the Department of Banking and Insurance
Kyiv National University of Economics
ORCID: 0000-0003-1361-2500

DOI: 10.25313/2520-2294-2024-7-10163

БІОМЕТРІЯ В ДИСТАНЦІЙНОМУ БАНКІВНИЦТВІ: БЕЗПЕКА ТА ПЕРСПЕКТИВИ

BIOMETRIC IN DISTANCE BANKING: SECURITY AND PROSPECTS

Анотація. *Вступ. Актуальність розвитку біометричних технологій в сучасному світі зумовлена широким її використанням в різноманітних сферах: криміналістиці; при доступі до секретних об'єктів, перетині державних кордонів, видачи віз, під час обліку робочого часу і реєстрація відвідувачів; в системах голосування; соціальних проєктах тощо. Поширилась вона і на сферу банківництва. Біометрія в банківській справі знайшла використання при автентифікації клієнтів та підтриманні безпеки під час цифрових банківських транзакцій і доступу до рахунків. Біометрія полягає в автентифікації особи, використанні її унікальних властивостей, а не володіння певними засобами (код, логін, пароль, платіжна картка), якими можуть скористатись несанкціоновано. Переваги біометричних систем ідентифікації користувачів є незаперечними, серед яких швидкість автентифікації та обробки даних, доступна ціна, зручність. Стрімке поширення використання біометрії в банківництві, поява нових способів та їх адоптація до фінансового середовища зумовлюють необхідність подальших досліджень даної тематики.*

Мета. Метою дослідження є характеристика та систематизація способів автентифікації в банківництві за допомогою біометрії, виокремлення сильних та слабих сторін, оцінка перспектив розвитку, можливості використання з метою підвищення безпеки автентифікації, оброблення та збереження даних.

Матеріали і методи. Матеріалами дослідження є: 1) праці вітчизняних та зарубіжних авторів, що займаються вивченням та дослідженням питань біометричних способів автентифікації, їх пристосуванням до різних сфер людського життя; 2) статистичні дані щодо поширення та динаміки використання різних способів автентифікації та збереження даних, різні кейси щодо практичних аспектів біометрії та розв'язання виявлених проблем.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного групування та узагальнення (для виявлення особливостей способів автентифікації осіб, стабільності результатів, розкриття різних аспектів біометрії, переваг та недоліків, тенденцій розвитку); формалізації, аналізу та синтезу (для побудови схем підвищення безпеки обробки та збереження даних за допомогою ШІ, Машинного навчання, хмарного середовища); логічного узагальнення результатів (при формулюванні висновків).

Результати. Проведене дослідження біометричних способів автентифікації та засобів захисту підтвердило актуальність наявної проблематики, її зв'язок з динамічним розвитком технологій, орієнтацією банків на використання біометричних засобів, потреб в простоті, швидкому проведенні операцій з мінімальними витратами, високою безпекою операцій та збереження даних. Наведено переваги, недоліки та загрози, основні риси біометричних способів автентифікації, тенденції та перспективи. Виявлено, що питання безпеки повинні вирішуватись у поєднанні різних технологій зокрема комбінації різних способів біометричної автентифікації, поєднання біометрії з традиційними засобами і інструментами (банкомати, паролі, коди), поєднання біометрії з іншими новітніми технологіями (штучним інтелектом, машинним навчанням, хмарними технологіями), що в комплексі приведе до суттєвого покращення безпекової ситуації

Перспективи. В подальших наукових дослідженнях пропонується зосередити увагу на удосконаленні існуючих біометричних засобів, які вже стали звичними (автентифікація за відбитками пальців, за райдужною оболонкою ока, за сітківкою ока, за венозним малюнком руки та долоні, голосом) та дослідженні відносно нових, такі як особливості поведінки, рухів,

ходи людини, почерку, термограма обличчя, характеристика ДНК, спектроскопія шкіри, форма вушної раковини тощо, які ще не можуть ефективно бути використані в масовому обсязі на даний момент та потребують подальших розробок та удосконалень, але мають потенціал розвитку. Також слід звернути увагу на можливу синергію певних технологій з метою покращення безпекової ситуації.

Ключові слова: *біометрія, штучний інтелект, хмарні технології, безпека, дистанційний банкінг, фінтех, deepfake.*

Summary. *Introduction. The relevance of the development of biometric technologies in the modern world is due to its wide use in various fields: forensics; when accessing secret facilities, crossing state borders, issuing visas, when recording working hours and registering visitors; in voting systems; social projects, etc. It spread to the sphere of banking. Biometrics in banking have found use in authenticating customers and maintaining security during digital banking transactions and account access. Biometrics consists in the authentication of a person, the use of his unique properties, and not in the possession of certain means (code, login, password, payment card), which can be used by unauthorized persons. The advantages of biometric user identification systems are indisputable, including speed of authentication and data processing, affordable price, and convenience. The rapid spread of the use of biometrics in banking, the emergence of new methods and their adaptation to the financial environment necessitate further research on this topic.*

Purpose. The purpose of the article is to characterize and systematize authentication methods in banking, to identify strengths and weaknesses, to assess development prospects, to use them in order to increase the security of authentication, to facilitate data processing and storage.

Materials and methods. The research materials are: 1) the works of domestic and foreign authors engaged in the study and research of biometric methods of identification, their adaptation to various spheres of human life; 2) statistical data on the distribution and dynamics of the use of various methods of authentication and data storage, various case studies on the practical aspects of biometrics and solving the identified problems. In the process of carrying out the research, the following scientific methods were used: theoretical grouping and generalization (to identify the peculiarities of the methods of authentication of persons, stability of results, disclosure of various aspects of biometrics, advantages and disadvantages, development trends); formalization, analysis and synthesis (to build schemes for increasing the security of processing and saving data with the help of AI, Machine Learning, cloud environment); logical generalization of results (when formulating conclusions).

Results. The conducted study of biometric methods of authentication and means of protection confirmed the relevance of the existing problems, its connection with the dynamic development of technologies, the orientation of banks to the use of biometric means, the need for simplicity, quick operations with minimal costs, high security of operations and data preservation. Advantages, disadvantages and threats, main features of biometric methods of authentication, trends and prospects are given. It was found that security issues should be solved in a combination of different technologies, in particular, a combination of different biometric authentication methods, a combination of biometrics with traditional means and tools (ATMs, passwords, codes), a combination of biometrics with other new technologies (artificial intelligence, machine learning, cloud technologies), which in the complex will lead to a significant improvement of the security situation.

Discussion. In further scientific research, it is proposed to focus on improving the existing biometric means that have already become common (authentication by fingerprints, by the iris of the eye, by the retina of the eye, by the venous pattern of the hand and palm, voice) and the study of relatively new ones, such as behavioral characteristics, movements, human gait, handwriting, facial thermogram, DNA characterization, skin spectroscopy, auricle shape, etc., which cannot yet be effectively used on a large scale at the moment and require further development and improvement, but have potential development. It is also important to pay attention to the possible synergy of certain technologies in order to undermine the security situation.

Key words: *biometrics, artificial intelligence, cloud technologies, security, remote banking, fintech, deepfake.*

Постановка проблеми. Біометричних технологій в сучасному світі широко використовуються в різноманітних сферах: криміналістиці; при доступі до секретних об'єктів, перетині державних кордонів, видачі віз, під час обліку робочого часу і реєстрація відвідувачів; в системах голосування; соціальних проєктах тощо. Поширилась вона і на фінансову сферу, сферу банківництва. Темпи світового приросту використання біометричних технологій перебувають на значному рівні (14,4% у середньому на рік), на початок 2023 року обсяги ринку становили 5,2 мільярда доларів, а до 2030 року очікується що ця цифра сягне 15,2 мільярда [5]. Біометрія в банківській справі знайшла використання при автентифікації клієнтів та підтриманні безпеки під час цифрових банківських транзакцій і доступу до рахунків. Біометрія полягає у використанні унікальних фізіологічних або поведінкових характеристик осіб і відрізняється від традиційних способів автентифікації (код, логін, пароль, платіжна картка), при яких засіб ідентифікації може бути використаний сторонніми особами, оскільки подібні системи ідентифікує наявність відповідного засобу, а не певної особи. Ідентифікаційний засіб може бути вкрадений, втрачений, скопійований і т.п. — все це залишає широке поле для отримання несанкціонованого доступу. Біометричні способи позбавлені даного недоліку, оскільки для автентифікації особи використовують унікальні властивості самої особи. Переваги біометричних систем ідентифікації користувачів є незаперечними, серед яких швидкість

автентифікації та обробки даних, доступна ціна, зручність. Дактилоскопія — найбільш відомий та традиційний метод встановлення особистості за біометричними параметрами, відмінно зарекомендував себе у криміналістиці 20-го століття. Проте, технології не стоять на місці і відбитки пальців перестали буди єдиним ключом ідентифікації. Сучасні технології дозволяють визначати користувачів за іншими біометричними даними такими як сітківка та рогівка ока, форма обличчя, рук, малюнок вен, голос, біологічна активність серця, почерк тощо. Стрімке поширення використання біометрії в банківництві, поява нових способів та їх адоптація до фінансового середовища, підвищення вимог до безпеки зумовлюють необхідність подальших досліджень даної тематики.

Аналіз останніх досліджень і публікацій. Питаннями біометричної автентифікації знаходять своє відображення в вітчизняній та іноземній літературі. Так Коваль Л. Г., Злепко С. М., Крекотень Є. Г., Новіцький Г. М. розглядають біометричні засоби без прив'язки до сфери фінансових послуг, як засіб доступу до певної інформації, локації на підприємствах, в криміналістиці, проводять аналіз методів біометричної ідентифікації та технологій їх реалізації [7]. Аналогічний підхід можна знайти в роботах авторів Дем'янюк М. Ю., Мартиненко А. А., які в своїх дослідженнях зосереджуються на технологіях збору і обробки інформації, а не можливості застосування в фінансовій сфері [6]. Стасев Ю. В., Гончаренко К. Г., Мороз В. І. досліджують технологічні аспекти роботи системи певного виду автентифікації, а саме райдужної оболонки ока, розглядають процедури збору інформації та її оцифрування [8]. Воронько В. О., Цуранов М. В. в своїх дослідженнях зосереджені на безпекових моментах біометрії, захисті об'єктів від несанкціонованого доступу [3]. На відміну від вищезазначених авторів в іноземній літературі чітко спостерігається розмежування досліджень для банківської сфери та підприємств. Хоча таке розмежування в окремих моментах є умовним і технології, які розроблені для банків після певної адоптації можуть бути застосовані на підприємствах. Так Приватбанк пропонує своїм клієнтам-підприємствам скористатись технічними можливостями банку і встановити біометричні системи як FacePay24 — розпізнавання обличчя, розпізнавання та цифрова обробка відбитка пальця з метою контролю допуску на територію інших підприємств, установ, організацій за умови створення такого сервісу на основі технологій чи обладнання банку. На відміну від вітчизняної наукової літератури в іноземній автори приділяють значну увагу використанню біометрії саме в банку. Так Brezitska M. наголошує на важливості безпекових заходів, зокрема у зв'язку з зростанням використання смартфонів [2]. Raktim Singh висвітлює необхідність впровадження біометричних технологій в банківський бізнес, наводить їх переваги порівняно з традиційними [9]. Grinberg D. говорить про активний розвиток біометричних технологій, робить прогнози їх розвитку в цілому, та по окремих видах виходячи з поточної ситуації [5]. Інші автори описують найбільш популярні види біометричних технологій [1]. Разом з тим недостатньо представленою є систематизація біометричних способів, слабких і сильних сторін, спрощення процедури обробки і збереження інформації, проблеми підвищення вимог до безпеки в майбутньому.

Мета. Метою дослідження є характеристика та систематизація способів автентифікації в банківництві, виокремлення сильних та слабких сторін, оцінка перспектив розвитку, можливості використання з метою підвищення безпеки автентифікації, полегшення оброблення та збереження даних.

Матеріали і методи. Матеріалами дослідження є: 1) праці вітчизняних та зарубіжних авторів, що займаються вивченням та дослідженням питань біометричних способів ідентифікації, їх пристосуванням до різних сфер людського життя; 2) статистичні дані щодо поширення та динаміки використання різних способів автентифікації та збереження даних, різні кейси щодо практичних аспектів біометрії та розв'язання виявлених проблем.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного групування та узагальнення (для виявлення особливостей методів автентифікації осіб, стабільності результатів, розкриття різних аспектів біометрії, переваг та недоліків, тенденцій розвитку); формалізації, аналізу та синтезу (для побудови схем підвищення безпеки обробки та збереження даних за допомогою ШІ, машинного навчання, хмарного середовища); логічного узагальнення результатів (при формулюванні висновків).

Виклад основного матеріалу. Біометрію людство використовує вже більше 130 років. Ще у 1892 році британський антрополог, соціолог і психолог Френсіс Гальтон створив першу систему класифікації відбитків пальців. Це відкриття Гальтона було прийнято та адаптовано різними установами. Суть біометричної технології в тому, щоб відсканувати фізіологічні характеристики особи і порівняти їх зі своєю базою даних. Якщо є співпадіння, особа ідентифікується.

Можна помітити зміни, які відбуваються в суспільстві з розвитком біометричних технологій:

1. З'являється більш тісний зв'язок споживачів та бізнесу. Спрощується проведення транзакції, зменшуються перешкоди.

2. Розвиток біометрії відбувається у тісному зв'язку з розвитком смартфонів. Смартфони стають вектором інновацій в галузі платежів з використанням біометричних технологій.

3. Біометричні технології кооперуються з традиційними. Традиційні технології, такі як банкомати, включають біометрію в свою інфраструктуру, тим самим підвищують власну безпеку й одночасно поширюють ці інновації в інших сегментах фінансової галузі.

Популярність біометричної автентифікації в банківській справі зростає, що зумовлено рядом переваг:

1. Посилення безпеки і зменшення шахрайства. Біометрична автентифікація забезпечує високий рівень безпеки мобільного банкінгу та зменшує ризики шахрайства та помилок. Біометричні характеристики є унікальними для кожної людини і, як правило, не можуть бути передані в цифровому вигляді. Таким чином, шахраям практично неможливо отримати несанкціонований доступ до банківських рахунків. Біометрія має певні переваги у виявленні та запобіганні шахрайським діям, таким як крадіжка особистих даних або захоплення облікового запису. Біометрична автентифікація виявляє аномалії в поведінці користувачів або біометричних моделях, які можуть вказувати на шахрайські дії. У такому випадку банк отримує сповіщення в режимі реального часу та може негайно вжити заходів.

2. Підвищена зручність. Біометрична автентифікація для банківських операцій позбавляє клієнтів від необхідності запам'ятовувати складні паролі або турбуватися про втрату своїх фізичних ключів безпеки. Натомість клієнти можуть безперешкодно отримувати доступ до своїх облікових записів за допомогою відбитків пальців, розпізнавання обличчя або голосу.

3. Більша ефективність роботи. Традиційні банківські процеси часто вимагають від клієнтів заповнення кількох форм ідентифікації. Оскільки методи біометричної аутентифікації не передбачають цього етапу, вони дозволяють заощадити час клієнтів. Крім того, банки, які використовують біометричні технології, покращують операційну ефективність, зменшуючи потребу в ручних перевірках і дослідженнях.

Біометричні методи, які застосовуються в банківництві можна поділити на три групи:

- Морфологічні: характеристики, пов'язані з будовою тіла. Це такі фізичні ознаки, як наприклад, очі, відбитки пальців, форма обличчя, скановані за допомогою спеціального програмного забезпечення.
- Біологічні: характеристика генетичного та молекулярного рівнів. Це може бути ДНК, кров або щось інше, отримане з рідин організму.
- Поведінкові: характеристики, що базуються на унікальних моделях поведінки, наприклад хода чи мова.

Банківська біометрична верифікація зазвичай базуються на морфологічних характеристиках як відбитки пальців, розпізнавання обличчя, сканування вен пальців або долонь, райдужної оболонки ока. Що стосується поведінкової біометрії, то найпопулярнішим є розпізнавання голосу. Розглянемо біометричні методи та їх характеристики (табл. 1).

З таблиці видно сильні і слабкі сторони кожного метода.

Розглянемо яскраві приклади використання біометричних технологій.

Нещодавно міжнародна платіжна система MasterCard запустила в 12 європейських країнах сервіс підтвердження покупок в інтернеті за допомогою селфі.

PayByFace для полегшення транзакцій використовує передову технологію розпізнавання обличчя. Користувачі налаштовують послугу, зареєструвавши платіжну картку, селфі та унікальний PIN-код. Таким чином, можна залишити вдома гаманець та гаджети й платити в магазині у буквальному сенсі своїм виглядом.

Біометричну аутентифікацію в e-commerce запроваджує і Visa у співпраці з Abu Dhabi Islamic Bank. Розроблена ними система використовує біометричні датчики, вбудовані в стандартний смартфон. Таким чином, клієнти ADIB у мобільному додатку можуть за допомогою розпізнавання обличчя або відбитків пальців підтверджувати свою особу.

Ще один приклад кооперації — Kookmin Bank, один з найбільших банків Південної Кореї, та Samsung. Вони впровадили нову біометричну систему, яка дозволяє авторизувати користувачів для доступу до облікових записів за допомогою райдужних оболонок.

Компанія Green Payments запускає рішення для точок продажу (POS), яке дозволить торговим підприємствам по всій території Сполучених Штатів приймати біометричні платежі — через зчитування відбитка пальця клієнта. Можна прив'язувати різні варіанти оплати, що зберігаються в цифровому гаманці (включаючи кредитні картки, банківські рахунки та криптовалюти) до окремих пальців, а потім сплачувати за товари на касі, торкаючись відповідним пальцем біометричного датчика. Біометрична модель допоможе суттєво знизити рівень шахрай-

Таблиця 1

Біометричні методи та їх характеристики

Метод	Надійність	Витрати	Розмір шаблону	Довгострокова стабільність
Розпізнавання обличчя	Середня/висока	Низькі	Малий	Середня/висока
Сканування райдужної оболонки ока	Висока	Високі	Малий	Середня
Відбитки пальців	Висока	Низькі	Малий	Середня
Розпізнавання малюнка кисті руки	Низькі	Середня	Середня	Висока
Розпізнавання голосу	Низькі	Середня	Малий	Низькі

Джерело: складено автором на основі [5]

ства при оплаті та спростити всю концепцію здійснення платежів (можна навіть позбутися гаманця).

Розглянемо ще кілька популярних сучасних технологій, які активно підкорюють світ, входячи в повсякденне життя кожного.

Платежі за допомогою малюнку долоні. Ingenico та Fujitsu Frontech представили найбільш безпечне, точне та безпроблемне біометричне платіжне рішення, засноване на ідентифікації вен долоні. Це рішення дозволяє споживачам ідентифікувати себе та здійснювати платежі, просто провівши долонею по спеціальному інфрачервоному (NIR) датчику. Кожна людина має унікальний малюнок вен на долоні, ідентифікація за ними є однією з найточніших технологій біометричної ідентифікації у світі. Ця технологія вважається не тільки безпечнішою, але і простішою у впровадженні та експлуатації, ніж такі альтернативи, як відбитки пальців і розпізнавання обличчя. На відміну від розпізнавання обличчя та відбитків пальців, хакери не можуть сфотографувати внутрішні структури вен долоні крупним планом для здійснення шахрайських транзакцій. Унікальні візерунки під шкірою практично неможливо відтворити.

Подібна технологія наразі просувається і WeChat Pay (Китай). Так, користувачі можуть підтверджувати платежі за допомогою долоні. Для цього компанія пропонує продавцям впроваджувати нову систему біометричної автентифікації Palm Payment. Метод оплати можна використовувати на різних споживчих ринках в автономному режимі, таких як ресторани, супермаркети, гуртові купівлі тощо, та надати користувачам новий спосіб оплати.

Здійснення оплати через сканування ока. Наприклад, компанія з Вроцлава використовує форму оплати, яка сканує райдужну оболонку ока. Працює система на основі технології PayEye та поступово інтегрується на комерційному ринку. Технологія використовує цифрове сканування зображення райдужної оболонки ока, яке потім перетворюється на спеціальний код для авторизації платежу. Система є швидшою, ніж безконтактні платежі карткою, телефоном або смарт-годинником. Людям не потрібно турбуватися про те, що вони щось забудуть, ця частина тіла- незмінний атрибут людини. Система PayEye використовує такі рушійні сили як бачення і переваги науки, технологій і досвід професійної команди.

Ідентифікація за вухами. Геометрія вух унікальна для кожної людини, тому сьогодні можна спостерігати розвиток і такого методу ідентифікації. Ця біометрія є надійною та подібною до зчитування відбитків пальців. Вухо кожної людини є більш стабільним джерелом біометричних даних, ніж риси обличчя, оскільки на нього менше впливають емоції та вік користувачів. Як зазначають аналітики вухо людини може бути об'єктом безконтактної автентифікації, але використання цього методу наразі обмежене через складність процесів збору та аналізу даних. Очевидно, що в кінцевому підсумку, найбільш зручні для користувача системи будуть використовуватися найбільше. У випадку з ідентифікацією по вухах — це поки що не так, але метод має потенціал стати більш широко застосовуваним, якщо продовжуватиметься його дослідження і будуть внесені відповідні вдосконалення.

Метод поведінкової автентифікації. Поведінкова автентифікація перевіряє особу користувача на основі унікальних патернів, записаних під час взаємодії з пристроями (наприклад, смартфоном, планшетом, комп'ютером). Фактори ідентифікації включають в себе все: від кута, під яким користувач тримає телефон, до сили натискання під час набору тексту.

Прикладом використання такої технології є додаток Nod to Pay, який дозволяє за допомогою Google Glass здійснювати платежі. Для цього потрібно лише подивитись на QR-код і двічі кивнути, щоб підтвердити покупку. Поведінкові патерни досить складно підробити. Так само, як відбитки пальців і сітківка ока є унікальними за визначенням для кожної людини, те ж саме стосується і способу взаємодії користувача зі своїм пристроєм. З іншого боку ідентифікація може залежати від фізичного стану та емоційної поведінки користувача.

Розглянемо приклад використання поведінкових біометричних засобів автентифікації клієнтів, яка вже запроваджена і використовується в банках України. Це голосова біометрія -один із найзручніших, найшвидших та найнадійніших методів аутентифікації клієнтів, який стає все більш популярним у всьому світі, зокрема і в Україні. Голосова біометрія — використання голосу людини в якості унікальної біологічної характеристики для її аутентифікації. Також технологія називається «верифікацією голосу» або «розпізнаванням диктора». Метод забезпечує швидкий, безпроблемний та високо безпечний доступ у різних сферах — від колл-центрів, мобільних та онлайн-додатків, до чат-ботів та пристроїв інтернету речей.

Значні досягнення в галузі нейронних мереж за останні кілька років дозволили розробити алгоритми голосової біометрії, які забезпечують методу високу швидкість аналізу та точність, а також дозволяють аутентифікувати користувачів за меншим обсягом мовлення.

Очікується, що щорічні темпи зростання ринку біометричної автентифікації становитимуть 22,8% і до 2026 року його обсяг зросте до $3,9 млрд. (з $1,1 млрд. 2020 року). Існує ряд переваг голосової біометрії (рис. 1).

Людський голос, як і райдужна оболонка ока чи відбиток пальця, є унікальним. Він має такий набір характеристик (наприклад, силу, висоту, тембр і т.д.), що жоден інший індивід не здатний його точно повторити. Більше 70 частин тіла впливають на те, як людина вимовляє слова, і кожна з цих частин унікальна. Голосові біометричні системи працюють шляхом запам'ятовування цих показників.

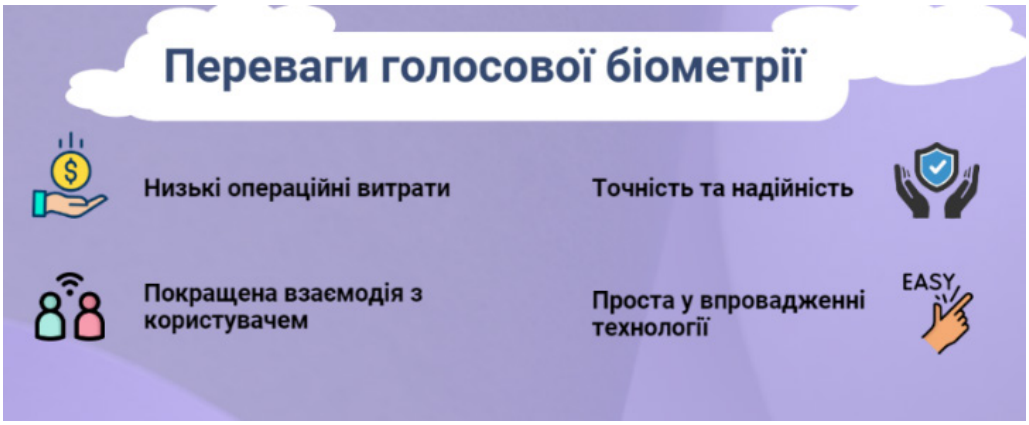

Рис. 1. Переваги голосової біометрії
Джерело: [4]

В результаті виходить відбиток/зліпок голосу, який також називають голосовим шаблоном.

Весною 2022 року ПриватБанк запровадив технологію голосової авторизації, а вже станом на середину осені кількість користувачів, перевищила мільйон людей. Для тестування системи в Приватбанку використовували кейси так звані friendly fraud, що підтвердили безпечність системи. Систему голосової біометрії фізично неможливо обдурити — вона працює на рівні нижче за людський слух, визначаючи власника за спеціальними нотами голосу. З метою підвищення безпеки ПриватБанк використовує технологію, яка дозволяє зрозуміти, що той, хто телефонує не включив запис чужого голосу та не використовує deepfake.

Незважаючи на більш високий рівень безпеки, ніж у стандартних методів аутентифікації, біометричні банківські системи мають вразливі місця. Кожний раз, коли з'являється нові рішення, зловмисники розробляють стратегії, щоб обдурити систему та отримати доступ до особистих даних користувача. Наприклад, дослідницька група з Університету Північної Кароліни в Чапел-Хілл використала 20 фотографій добровольців, завантажених із соціальних мереж, щоб створити 3D-моделі їхніх облич. Ці моделі дозволили зламати чотири з п'яти перевірених систем [1]. Така ж проблема стосується відбитків пальців та інших біометричних даних, які можна клонувати. Також технологія deepfake дозволяє здійснювати нові види атак. Біометричним системам може бути складно виявити глибокі фейки, створені комп'ютером відео- чи аудіозаписи користувача. Біометричне програмне забезпечення генерує та збирає дуже конфіденційну інформацію, тому ставки безпеки є вищими. Якщо не захистити дані, можна втратити великий обсяг особистої інформації. У 2015 році базу даних уряду США було зламано, а відбитки пальців 5,6 мільйонів федеральних службовців — викрадено. Крім того, звичайні форми аутентифікації можуть бути просто змінені у разі викрадення, що неможливо зробити з голосом чи обличчям. Тож потрібно приділяти увагу розвитку кібербезпеки, яка зможе адекватно вирішити ці проблеми.

Можливими шляхами зниження ризиків є:

- використання кількох засобів автентифікації. Наприклад поєднати біометричне сканування з небіометричним підходом або використовувати кілька біометричних підходів безпеки.
- Взаємодія з супутніми технологіями. Віддавати перевагу хмарним системам. Локальне сховище дає банкам більше контролю, але насправді воно менш безпечне, ніж хмара. Тому слід співпрацювати з постачальниками біометричних засобів безпеки, які зберігають дані в хмарі та шифрують їх для запобігання несанкціонованому доступу. Зберігаючи та обробляючи біометричні дані в централізованій безпечній інфраструктурі, хмарні обчислення гарантують дотримання правил конфіденційності даних, забезпечуючи при цьому доступність і масштабованість системи.

Застосування алгоритмів на основі штучного інтелекту є надзвичайно важливим для аналізу біометричних даних, виявлення спроб спуфінгу та постійного моніторингу активності користувачів для виявлення аномалій. Наприклад, непомітний помічник зі штучним інтелектом, який ретельно стежить за фінансовими операціями та захищає рахунки у спосіб, подібний до опікуна і якого неможливо виявити.

Також треба враховувати відмінності між звичайною та поведінковою біометрією. Технологія поведінкової біометрії визначає та розпізнає унікальну поведінку людей, використовуючи всі можливості штучного інтелекту (ШІ)та машинного навчання (МН). Оскільки технології ШІ та МН продовжують розвиватися, їх інтеграція в біометричні системи має величезні перспективи для забезпечення безпечного та зручного банківського досвіду.

Децентралізована реєстраційна система технології блокчейн, реалізація якої все ще перебуває на зародковому етапі, потенційно може підвищити

безпеку та прозорість адміністрування біометричних даних. Можна концептуалізувати децентралізовану книгу, яка зберігає біометричну інформацію особи, обмежуючи доступ користувачам лише за наявності дозволу та забезпечуючи стійкість до маніпуляцій.

Ці технології створюють посилене та безпечне середовище для захисту біометричних даних у фінансовому секторі. Банківські установи можуть посилити свій захист від шахрайства та несанкціонованого проникнення, використовуючи свої спеціалізовані знання для зміцнення протоколів безпеки та гарантування плавного процесу транзакцій для своїх клієнтів. Очікується, що у 2028 році світовий ринок біометричної безпеки у фінансовому секторі досягне 7,7 мільярдів доларів США [9]. Цей прогноз відображає постійну інтеграцію цих додаткових технологій і послідовне зростання галузі.

Висновки і перспективи подальших досліджень. Проведене дослідження біометричних способів автентифікації та засобів захисту підтвердило актуальність наявної проблематики, її зв'язок з динамічним розвитком технологій, орієнтацією банків на використання біометричних засобів, потреб в простоті, швидкому проведенні операцій з мінімальними витратами, високою безпекою операцій та збереження даних.

Наведено переваги, недоліки та загрози, основні риси біометричних способів автентифікації, тенденції та перспективи. Виявлено, що питання безпеки повинні вирішуватись у поєднанні різних технологій зокрема комбінації різних способів біометричної автентифікації, поєднання біометрії з традиційними засобами і інструментами (банкомати, паролі, коди), поєднання біометрії з іншими новітніми технологіями (штучним інтелектом, машинним навчанням, хмарними технологіями), що в комплексі приведе до суттєвого покращення безпекової ситуації

В подальших наукових дослідженнях пропонується зосередити увагу на удосконаленні існуючих біометричних засобів, які вже стали звичними (автентифікація за відбитками пальців, за райдужною оболонкою ока, за сітківкою ока, за венозним малюнком руки та долоні, голосом) та вивченні відносно нових, таких як особливості поведінки, рухів, ходи людини, почерку, термограма обличчя, характеристика ДНК, спектроскопія шкіри, форма вушної раковини тощо, які ще не можуть ефективно бути використані в масовому обсязі на даний момент та потребують подальших розробок та удосконалень, але мають потенціал розвитку. Також слід звернути увагу на можливу синергію певних технологій з метою покращення безпекової ситуації.

Література

1. Biometrics in payment: The case of the biometric bank card (white paper). *Thales.* URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards/biometrics-in-banking (дата звернення: 15.07.2024).

2. Brezitska M. Biometrics in Banking: Which Biometric System Ensures 100% Security. *Binariks.* 2023. URL: https://binariks.com/blog/biometric-security-onilne-banking/ (дата звернення: 14.07.2024).

3. Воронько В. О., Цуранов М. В. Біометрична ідентифікація як захист від несанкціонованого доступу. *Протидія кіберзагрозам та торгівлі людьми.* Харків, 2019. С. 224–226. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/68.pdf (дата звернення: 14.07.2024).

4. Де записати голосову біометрію. *Приватбанк.* URL: https://privatbank.ua/voice-biometrics (дата звернення: 14.07.2024).

5. Grinberg D. Biometrics in Banking: Unlocking Security and Efficiency. *TechMagic.* 2024. URL: https://www.techmagic.co/blog/biometrics-in-banking/ (дата звернення: 14.07.2024).

6. Дем'янюк М. Ю., Мартиненко А. А. Біометричні засоби ідентифікації у сучасних інформаційних системах. *DSpace. Institutional Repository Dnipro University of Technology.* URL: https://ir.nmu.org.ua/bitstream/handle/123456789/148815/demianuk_martynenko.pdf?sequence=1&isAllowed=y (дата звернення: 18.07.2024).

7. Коваль Л. Г., Злепко С. М., Новіцький Г. М., Крекотень Є. Г. Методи і технології біометричної ідентифікації за результатами літературних джерел. *Вчені записки ТНУ імені В. І. Вернадського. Серія: технічні науки.* 2019. Т. 30 (69), Ч. 1, № 2. С. 104–111. URL: https://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf (дата звернення: 25.07.2024).

8. Стасєв Ю. В., Гончаренко К. Г., Мороз В. І. Аналіз методу багатофакторної аутентифікації користувачів інформаційних систем на основі райдужної оболонки ока. *Системи обробки інформації.* 2023. Вип. 3(174). С. 63–69. URL: https://journal-hnups.com.ua/index.php/soi/article/view/1482/1350 (дата звернення: 12.07.2024).

9. Singh R. Biometric in banking. Why Do Banks Need Biometric Technology? *Finextra.* 2024. URL: https://www.finextra.com/blogposting/25560/biometric-in-banking (дата звернення: 20.07.2024).

References

1. Biometrics in payment: The case of the biometric bank card (white paper). *Thales.* URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards/biometrics-in-banking.

2. Brezitska M. Biometrics in Banking: Which Biometric System Ensures 100% Security. *Binariks.* 2023. URL: https://binariks.com/blog/biometric-security-onilne-banking/.

3. Voronko V.O., Tsuranov M.V. Biometrychna identyfikatsiia yak zakhyst vid nesanktsionovanoho dostupu. *Protydiia kiberzahrozam ta torhivli liudmy.* Kharkiv, 2019. S. 224–226. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/68.pdf [in Ukrainian].

4. De zapysaty holosovu biometriiu. *Pryvatbank.* URL: https://privatbank.ua/voice-biometrics [in Ukrainian].

5. Grinberg D. Biometrics in Banking: Unlocking Security and Efficiency. TechMagic. 2024. URL: https://www.techmagic.co/blog/biometrics-in-banking/.

6. Demianiuk M.Yu., Martynenko A.A. Biometrychni zasoby identyfikatsii u suchasnykh informatsiinykh systemakh. *DSpace. Institutional Repository Dnipro University of Technology.* URL: https://ir.nmu.org.ua/bitstream/handle/123456789/148815/demianuk_martynenko.pdf?sequence=1&isAllowed=y [in Ukrainian].

7. Koval L.H., Zlepko S.M., Novitskyi H.M., Krekoten Ye.H. Metody i tekhnolohii biometrychnoi identyfikatsii za rezultatamy literaturnykh dzherel. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: tekhnichni nauky.* 2019. T. 30 (69), Ch. 1, № 2. S. 104–111. URL: https://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf [in Ukrainian].

8. Stasiev Yu.V., Honcharenko K.H., Moroz V.I. Analiz metodu bahatofaktornoi autentyfikatsii korystuvachiv informatsiinykh system na osnovi raiduzhnoi obolonky oka. *Systemy obrobky informatsii.* 2023. Vyp. 3(174). S. 63–69. URL: https://journal-hnups.com.ua/index.php/soi/article/view/1482/1350 [in Ukrainian].

9. Singh R. Biometric in banking. Why Do Banks Need Biometric Technology? *Finextra.* 2024. URL: https://www.finextra.com/blogposting/25560/biometric-in-banking.