РОЗДІЛ 6. ГРОШІ, ФІНАНСИ І КРЕДИТ

БІОМЕТРИЧНЕ МАЙБУТНЄ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ФІНАНСОВИХ ПОСЛУГ

BIOMETRIC FUTURE OF AUTHENTICATION OF FINANCIAL SERVICES USERS

У статті розглянуто необхідність підвищення поінформованості про переваги та ризики застосування біометричних технологій, що породжують особливі проблеми через розрив між впровадженням технологічних інновацій та прийняттям законів, що регулюють ці технології. Відповідно, розглянуто певний досвід використання таких нових технологій та розроблені рекомендації щодо нинішнього та можливого майбутнього застосування біометрії з метою автентифікації споживачів фінансових послуг. Проблема внутрішнього шахрайства та неправомірного доступу до даних через облікові записи є актуальною для фінансових організацій у всьому світі. Банки знаходяться в пошуку рішень, здатних захистити їхню внутрішню інфраструктуру даних, і все частіше віддають перевагу біометричним технологіям. Застосування біометричних технологій для авторизації дозволяє забезпечити необхідний рівень безпеки даних та контролю доступу до чутливої інформації.

Ключові слова: біометрія, автентифікація, конфіденційність інформації, інноваційні технології, кіберризик, захист даних.

УДК 336.71

DOI: https://doi.org/10.32782/infrastruct68-36

Борисова Л.Є.
к.е.н., доцент кафедри обліку і фінансів
Одеський національний університет імені І.І. Мечникова
Колесник О.О.
к.е.н., доцент кафедри обліку і фінансів
Одеський національний університет імені І.І. Мечникова
Шрамко О.О.
спеціаліст вищої категорії,
Одеський торговельно-економічний фаховий коледж

Borysova Larysa
Odessa I.I. Mechnikov National University
Kolesnik Olga
Odessa I.I. Mechnikov National University
Shramko Helen
Odesa Professional College of Trade and Economics

The article discusses biometric technologies, which allow not only to ensure the proper level of security of financial transactions, but also to speed up the process of customer service both in traditional branches and through remote service channels. A few years ago, in order to attract new customers, it was enough for banks to offer them cheaper products and services. Today the situation is rapidly changing, users prefer convenience and reliability. The most common types of biometric data used in the financial sector include facial image, fingerprints, hand geometry and iris pattern. This data can be used to identify customers in online banking, to provide access to financial services on self-service devices and at bank branches, and to gain access to safe deposit boxes. The most popular in the banking sector is two-factor authentication using a PIN code or one-time password and biometrics, which ensures the highest level of data security and access control. The problem of internal fraud and unauthorized access to data through employee accounts is relevant for financial institutions around the world. Also biometrics is able to play an increasingly important role in the global fight against different forms of terrorism, namely in countering fraud, identity theft and other criminal offenses committed by terrorists in order to support their activities. Banks are looking for solutions that can protect their internal data infrastructure and are increasingly opting for biometric technologies. However, of course, biometric technologies' usage can have more advantages than risks of using. The use of biometric technologies for employee authorization ensures the necessary level of data security and access control to sensitive information, and also provides enough opportunities for monitoring the work of employees of a financial institution. One of the most reliable means of user authentication is biometrics. Biometric data cannot be tampered with, stolen or otherwise used without the knowledge of the bearer. The use of biometric data for authentication on self-service devices provides a high level of security and reduces the time of the transaction, relieves users of the need to carry payment means with them, remember passwords or a PIN code from a card, etc.

Key words: *biometrics, authentication, confidentiality of information, innovative technologies, cybersecurity, protection of data.*

Постановка проблеми. Біометрія здатна відігравати все більш важливу роль у глобальній боротьбі з тероризмом, а саме у протидії шахрайству, розкраданню особистих даних та інших кримінальних злочинів, скоєних терористами з метою підтримки своєї діяльності. Разом з тим, щоб повною мірою реалізувати потенціал біометричних технологій, урядам необхідно вирішувати питання, пов'язані із захистом осіб, що ідентифікуються такими системами, домагаючись, щоб збирання, зберігання та використання біометричних даних велися відповідно до міжнародних стандартів у галузі прав людини та міжнародних законів про недоторканність приватного життя.

Аналіз останніх досліджень і публікацій. Оскільки проблема біометрії є багатоаспектною, дослідження у цій сфері активно проводилися науковцями майже усіх галузей, зокрема в економічній, юридичній та технічній сферах. Серед них такі, як Горошко М. П., Миклуш С. С., Хомюк П. Г., Русин Б. П., Варецький Я. Ю. та ін.

Постановка завдання: метою статті є узагальнення досвіду використання біометричної автентифікації в сфері фінансових послуг. З позиції переваг та ризиків використання останньої.

Виклад основного матеріалу дослідження. Біометрія – технологія ідентифікації особистості, що використовує фізіологічні параметри людини, набуває все більшого поширення в різних галузях, кардинально змінюючи способи проведення платежів, системи доступу та безпеки. Вона використовується правоохоронними органами, у галузі охорони здоров'я, реклами, дизайну та виробництва, а також активно почала використовуватися

при наданні фінансових послуг. Застосування біометрії набуває все більш розповсюдженого характеру, і одночасно з цим громадськість все більшою мірою приймає цю технологію, користуючись біометричними технологіями в мобільних телефонах, але не завжди усвідомлюючи можливі наслідки. Це вказує на необхідність підвищення проінформованості про переваги та ризики застосування біометричних технологій. Біометрія зручна і може забезпечити вищий рівень безпеки. При цьому, однак, вимагає вирішення ряду проблем, таких як захист права на недоторканність приватного життя, захист даних і боротьба зі спуфінгом. До того ж при розпізнаванні голосів та осіб можливі помилки. Персональні дані, у тому числі біометричні, слід збирати та зберігати лише в тих випадках, коли це одночасно і необхідно, та доцільно. Згідно з прогнозами компанії Research and Markets, яка займається дослідженнями ринку, обсяг цього сектора до 2025 р. досягне 15 млрд. доларів США. При розпізнаванні голосів та осіб можливі помилки [5].

Біометрична перевірка – це наступний крок еволюції платежів разом із набором нещодавніх інновацій, таких як «Shop Anywhere», «Enhanced Contactless (ECOS)» і «Cloud Point of Sale», які були впроваджені, щоб надати споживачам і продавцям гнучкість без проблем і безпечний досвід роботи в магазині. У сфері біометрії лідером є Китай, оскільки він посів перше місце у списку широкого використання технологій розпізнавання осіб, а також поширеній практиці спостереження. Маштаб використання біометрії в цій країні можна визначити за найпопулярнішою технологією «Face++», що містить біометрію 1,3 мільярдів громадян країни. За Китаєм слідують країни Європи та Латинської Америки. Так, в ресторані Kentucky Fried Chicken в Ханчжоу, Китай, відвідувачі посміхаються, щоб отримати свій обід. Звісно, пандемія вплинула на розмір ринку біометричних технологій, оскільки багато біометричних пристроїв, такі як сканери відбитків пальців, припускають дотик до поверхонь. Але, незважаючи на те, що носіння масок ускладнювало розпізнавання людини біометричними пристроями, попит на багато біометричних пристроїв, такі як розпізнавання осіб та інші значно зріс, оскільки тут не потрібен будь-який контакт і тим самим можливо забезпечувати ефективну аутентифікацію. Система «Smile to Pay» («посміхнися, щоб заплатити»), запроваджена в 2017 р. компанією Alibaba, одним із світових лідерів у галузі електронної комерції, використовує технологію розпізнавання осіб для ідентифікації особи та виконання платіжних операцій. Британський банк Barclays замінив традиційне голосове меню на систему розпізнавання голосу. Citigroup планує запровадити технологію розпізнавання голосу для своїх клієнтів-фізичних осіб у Азії. Для підтвердження онлайн-платежу за технологією «Identity Check» у платіжній системі Mastercard клієнтам потрібно скористатися камерою смартфона. У Міжнародному аеропорту Аруба система Aruba Happy Flow фіксує біометричні дані пасажирів під час реєстрації на рейс. Оснащені камерами контактні термінали для пасажирів здатні розпізнавати обличчя та виконувати їхню ідентифікацію з подальшою обробкою даних.

Платіжна система Mastercard вже давно є піонером біометрії – у магазині та онлайн – як безпечного способу підтвердження особи, замінюючи пароль на особу. Зусилля, які базуються на стандарті EMV 3-D Secure, дозволяють людям робити покупки та платити за допомогою біометричних платіжних карток, пристроїв і носіїв. Біометрія також використовувалася для підтвердження особи онлайн-покупців за допомогою «селфі-оплати» та онлайн, використовуючи ключові стандарти, такі як FIDO (Fast Identity Online).

Оскільки ця технологія все більше впроваджується в усьому світі, Mastercard допомагає всім зацікавленим сторонам підтримувати найвищий рівень безпеки та конфіденційності для захисту споживачів. Програма оформлення біометричних даних регулюється принципами Mastercard щодо відповідальності за дані, що підтверджує, що споживачі мають право контролювати, як їхні персональні дані передаються, і отримувати вигоду від їх використання. У той час як технологія розпізнавання обличь давно викликала обурення у правозахисників, платіжний гігант Mastercard просуває програму біометричних розрахунків, яка, як стверджується, пришвидшить платежі, скоротить черги та забезпечить більший рівень безпеки, ніж стандартна кредитна чи дебетова картка. Причиною запуску Mastercard цієї суперечливої програми, яка дозволить покупцям розплачуватися в касі простою посмішкою або помахом руки, є бажання збільшити частку ринку біометрії. Компанія також підтверджує, що нова платіжна система буде більш гігієнічною, враховуючи проблеми зі здоров'ям, які вийшли на перший план під час пандемії Covid.

Перші пілотні проекти плануються до запуску у Бразилії в п'яти супермаркетах St Marche в Сан-Паулу, де покупці зможуть зареєструватися для біометричних платежів у магазині або через додаток місцевого партнера Mastercard Payface.

Компанія зосередиться на запуску технології на ринках Латинської Америки, Близького Сходу, Африки та Азії. Ця схема є частиною зусиль Mastercard щодо виходу на ринок безконтактних біометричних технологій, вартість якого до 2026 року, згідно з даними KBV Research, очікується в 18,6 млрд доларів [4].

Платіжний гігант конкурує з такими великими технологічними конкурентами, як Amazon, який використовує пристрої для зчитування з долоні у

своїх магазинах, що викликали критику американських політиків через проблеми з конфіденційністю даних. Згідно досліджень 74% світових споживачів «позитивно ставляться» до біометричних технологій, хоча решта активно висловлюють занепокоєння щодо зберігання та відстеження даних[1].

Mastercard визнали проблеми з даними та безпекою, пов'язані з використанням біометрії. Якщо біометричні дані зламано, ризик шахрайства може бути значно вищим, ніж у традиційних способів оплати. Також дискусійним залишається питання про те, як ці дані можна використовувати для відстеження, перевірки або моніторингу нічого не підозрюючих споживачів.

Технології, подібні до біометрії, породжують особливі проблеми через розрив між впровадженням технологічних інновацій та прийняттям законів, що регулюють ці технології. Відповідно, деякі держави створюють органи з експертизи етичних аспектів та інші наглядові органи, щоб у запобіжному порядку вивчити такі нові технології та додатки та виробляти рекомендації щодо нинішнього та можливого майбутнього законодавства, урядової політики та стратегічного планування. До складу цих органів зазвичай входять висококваліфіковані провідні фахівці, які представляють громадянське суспільство, а також можуть входити представники державного та приватного секторів, науково-технічні працівники, діячі науки та пересічні громадяни. Подібні групи з етичного нагляду прагнуть розглядати питання в широкому ракурсі, у тому числі потенційні наслідки застосування біометричних технологій для окремих груп і співтовариств, насамперед щодо расової приналежності, статі, віку, релігійних переконань і сексуальної орієнтації.

Незважаючи на те, що Mastercard вжила заходів для захисту та шифрування цих даних, оскільки біометричні платежі стають більш поширеними, використання таких даних, ймовірно, розвиватиметься, і неминуче стане важче захищати права людей на конфіденційність.

Для створення біометричної системи, яка була б ефективною і водночас відповідною законам щодо захисту даних та що забезпечує дотримання права на недоторканність приватного життя, необхідно взяти до уваги наведені нижче фактори.

Також необхідно встановити високі стандарти якості реєстрації даних, щоб забезпечити точну реєстрацію та зіставлення біометричних даних у різних умовах, у тому числі у віддалених районах, на прикордонних пропускних пунктах або в аеропортах, де все більше зростає потреба у прискореній обробці даних пасажирів за підтримки належного рівня точності. Коли йдеться про дітей або юридично неповнолітніх, які супроводжують батьків або подорожують наодинці, слід врахувати можливість зміни деяких біометричних даних дітей у міру їхнього дорослішання. Крім того, Рада Безпеки Організації Об'єднаних Націй у своїй резолюції 2396 (2017) наголошує, що з дітьми необхідно поводитися таким чином, щоб дотримувалися їхніх прав і поважати їхню людську гідність, відповідно до застосовних норм міжнародного права [2].

Законодавство про недоторканність приватного життя свідчить про те, що правоохоронні органи можуть обмежувати право на недоторканність приватного життя в тому випадку, якщо вжиті ними заходи є необхідними та пропорційними та відповідають нормам міжнародного права в галузі прав людини. Наприклад, персональні дані підозрюваних та їх спільників використовуються в надзвичайних ситуаціях, коли можна не враховувати необхідність дотримання основних принципів конфіденційності, таких як усвідомлена згода або збирання супутніх особистих даних. Проте, в більшості випадків дотримання таких принципів конфіденційності, як усвідомлена згода, збирання та використання персональних даних тільки для заявлених цілей, а також право на виправлення неточних або свідомо неправдивих відомостей, слід вважати вимогою за замовчуванням. Крім того, слід документувати та реєструвати в журналі причини відмови від виконання цих вимог за умовчанням. Для забезпечення високого рівня безпеки доступ операторів до цих систем повинен також контролюватись за допомогою біометричних даних. Ще одним важливим моментом є той факт, що іноді процеси ідентифікації та автентифікації ототожнюються, хоча це не так. Процес ідентифікації полягає у знятті та запису біометричних зразків, переведення їх у математичний код з наступним порівнянням наданого зразка з уже збереженим у системі та висновком результату – збігаються чи біометричні зразки. Процес автентифікації передбачає підтвердження, що людина є тим, ким вона себе називає при отриманні будь-якої фінансової послуги.

Біометричні дані можуть бути використані в рамках системи заходів, спрямованих на запобігання пов'язаним з тероризмом, шахрайством, крадіжками ідентифікаційних даних та фінансових операцій та зменшення цих загроз у фінансовій системі. Таким чином, одним із ефективних варіантів є використання біометричних даних для контролю доступу до транзакцій. Чимало переваг з погляду цивільного населення та охорони правопорядку мають національні програми захисту споживачів від пов'язаних із тероризмом випадків шахрайства та крадіжки ідентифікаційних даних.

Міжнародні стандарти захисту персональних даних повинні відповідати міжнародним стандартам в більшій мірі, ніж менш поширеним варіантам або технічним стандартам, які можуть залежати від таких факторів, як лобістські зусилля місцевих

компаній, або навіть ґрунтуватися на системах, що є безкоштовними донорськими програмами для надання допомоги. Як початкові критерії при виборі системи слід використовувати відповідні стандарти Міжнародної організації зі стандартизації, Міжнародної організації цивільної авіації та Всесвітньої митної організації, підкріплені розробленими Інститутом біометрії принципами недоторканності приватного життя та контрольним переліком питань для оцінки впливу на недоторканність приватного життя.

Зростання кількості випадків фінансового шахрайства, крадіжок особистих даних та інших кіберзагроз змусив банки вивчати нові технології, тому використання біометричних рішень стає чудовим варіантом рішення проблеми. Банки та інші фінансові організації з усьому світу пропонують клієнтам можливість біометричної автентифікації при використання, наприклад, мобільного банку. Паролі, які ще недавно широко використовували для доступу до банківських мобільних програм, вже не відповідають очікуванням клієнтів, тому впровадження біометрії якісно змінює користувацький досвід, роблячи його простим та безпечним.

Висновки з проведеного дослідження. Отже, найчастішим сценарієм розкрадання коштів є отримання даних клієнта, необхідних для ідентифікації та проведення операцій на віддалених каналах обслуговування. Сьогодні клієнт може вибрати різні способи ідентифікації: звичайний PIN-код або пароль, відбиток пальця, розпізнавання голосу, перевірка за допомогою відео, тощо. Жоден із способів не забезпечує 100% захист від дій зловмисників, біометрія – не виняток. Однак використання біометрії як другого чи третього фактору автентифікації може значно підвищити безпеку даних та покращити клієнтський досвід.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Горошко М. П., Миклуш С. С., Хомюк П. Г. Біометрія. Львів : Вид-во «Камула», 2004. 236 с.

2. Русин Б. П., Варецький Я. Ю. Біометрична аутентифікація та криптографічний захист. Львів : Коло, 2007. 287 с.

3. Ratha N. K., Connell J. H., Bolle R. M. Підвищення безпеки та конфіденційності в системах автентифікації на базі біометричних систем. *IBM Systems Journal».* 2001. Vol. 40. С. 614–634.

4. Static vs behavioural: what's the future of biometric authentication? 2017. URL: http://www.itproportal.com/features/static-vs-behavioural-whats-the-future-of-biometric -authentication.

5. Mastercard launches tech that lets you pay with your face or hand in stores. 2022. URL: https://www.cnbc.com/2022/05/17/mastercard-launches-tech-that-lets-you-pay-with-your-face-or-hand.html.

REFERENCES:

1. Horoshko M. P., Myklush S. S., Khomiuk P. H. (2004) *Biometriia* [Biometrics]. Lviv: Vyd-vo «Kamula», 236 p.

2. Rusyn B.P., Varetskyi Ya.Iu. (2007) *Biometrychna autentyfikatsiia ta kryptohrafichnyi zakhyst* [Biometric authentication and cryptographic protection]. Lviv: Kolo, 287 p.

3. Ratha N. K., Connell J. H., Bolle R. M. (2001) Pidvyshchennia bezpeky ta konfidentsiinosti v systemakh avtentyfikatsii na bazi biometrychnykh system [Increasing security and privacy in authentication systems based on biometric systems]. *IBM Systems Journal,* vol. 40, pp. 614–634

4. Static vs behavioural: what's the future of biometric authentication? 2017. Available at: http://www.itproportal.com/features/static-vs-behavioural-whats-the-future-of-biometric -authentication.

5. Mastercard launches tech that lets you pay with your face or hand in stores. 2022. Available at: https://www.cnbc.com/2022/05/17/mastercard-launches-tech-that-lets-you-pay-with-your-face-or-hand.html.