St. Cyril and St. Methodius University of Veliko Tarnovo
Faculty of Economics

ПРИЛОЖЕНИЕ НА БИОМЕТРИЧНИТЕ ДАННИ В МОБИЛНОТО БАНКИРАНЕТО

APPLICATION OF BIOMETRIC DATA IN MOBILE BANKING

Венелина Цаневска
Venelina Tsanevska

Великотърновски университет „Св. св. Кирил и Методий“
St. Cyril and St. Methodius University of Veliko Tarnovo

Abstract: Nowadays, digitalisation is increasingly manifesting itself all around us and affecting every sector of the economy. This raises the question of how we can be sure of our security systems. In particular it applies to the banking sector, especially when it comes to access to e-banking and the security of personal financial resources. Mobile devices have become an important tool used by people for banking, budgeting and shopping. Biometric identification is expected to change the way we use banking services. This paper discusses the application of biometrics in mobile banking, firstly highlighting the impact of mobile technology in the online banking process. Secondly, attention is given to the types of biometrics with their advantages and disadvantages. Some studies on the adoption of biometric technologies are also discussed in the paper.

Keywords: biometrics, biometric date, banking, m-banking, digitalization
JEL: G21

ВЪВЕДЕНИЕ

Дигитализация се въвежда във все по-голям брой услуги с цел оптимизиране на процесите в организацията и вземане на бързи, надеждни, сигурни и ефективни решения. Ключов фактор се оказва защитата на данните и избора на подходящи средства и мерки за това, така че от една страна да се пазят данните на потребителите, а от друга имиджа на организацията.

Сигурността е свързана с обмен на данни – пароли, ПИН кодове и друга лична информация. Част от потребителите изпитват затруднение в запомнянето им и често забравят (или объркват) паролите си за достъп, както и застрашават сигурността си, използвайки една и съща парола за множество акаунти и устройства. Подобни действия имат своите рискове – загуба на поверителност и увеличаване на нивата на измами със самоличност. В резултат на това постепенно паролата се заменя от използването на някои човешки характеристики като пръстов отпечатък, лицево разпознаване, гласово разпознаване или поведенчески черти. Всъщност отново става дума за идентифициране, но този път с помощта на техники, приложими за дигиталния свят. Това е от важно значение в банковия сектор, особено що се касае до достъпа до електронно банкиране и сигурност на личните финансовите средства.

ИЗЛОЖЕНИЕ

1. Въздействие на мобилните технологии в процеса на онлайн банкиране

В световен мащаб, а и у нас, все повече хора използват ежедневно смарт телефоните си, за да използват голям спектър от услуги. Една от ключовите иновации при използването на тези смарт устройства е навлизането на биометричните данни. Въздействието на смартфона (Mastercard, 2020, p.5) започна още през 2011 г., когато компанията Samsung пусна първото си мобилно устройство с лицево отключване. Две години по-късно от Apple пуснаха първата си защитна функция с

пръстови отпечатъци на телефона iPhone 5S. От тогава биометричните данни революционизираха пазара на мобилни устройства и се превърнаха в стандартна функция за сигурност. Очакванията са тези технологии да продължават да се развиват и за в бъдеще всички мобилни смарт телефони да имат някаква биометрична система.

Неминуемо дигитализацията и технологичният напредък се отрази и на услугите в банковия сектор. Навлизането на смарт устройствата способства за това все повече хора да банкират отдалечено (с дистанционен достъп) и все по-често чрез мобилните си смарт телефони, което представлява т.н. „мобилно банкиране“.

Класическите начини при отдалеченото банкиране, с оглед удостоверяване на идентичността, са:

• нещо, което знаем – това са имена, пароли, ПИН кодове, отговори на тайни въпроси;

• нещо, което имаме – касае информация, която физически носим със себе си, обикновено през хардуерно устройство или софтуерно приложение;

• нещо, което сме – касае уникалните биологични черти на човека като пръстови отпечатъци, длани, лице, глас, ретина и ирис, подпис, ДНК.

Традиционните методи за автентикация (като въвеждане на потребителско име, парола, ПИН код) не са достатъчно надеждни, тъй като хакерите могат лесно да хакнат банковите сметки на потребителите, за да получите достъп до идентификационни данни за вход (Kiyani, Lasebae, Ali, & Masood Ur-Rehman, 2020). Общото между първите два начина е, че лесно могат да се забравят или загубят, докато при третия начин тази опасност се избягва, тъй като използваните характеристики при него трудно могат да се възпроизведат.

Може да се каже, че развитието на биометричните технологии в сферата на банкирането се дължи на динамичното развитие на мобилните технологии. Например – в съвременните модели смарт телефони широко се използват технологии, които позволяват да се извърши идентификация по лицето и ириса на окото с помощта на камера, а също така широко е разпространена и технологията за разпознаване по пръстов отпечатък. Президентът Ajay Bhalla на Cyber & Intelligence в Mastercard казва, че „начинът, по който плащаме, трябва да е в крак с начина, по който живеем, работим и правим бизнес, предлагайки избор на потребителите с най-високи нива на сигурност“ (Mastercard, 2022). Бизнесът изгражда приоритетите си, ориентирайки се предимно към увеличаване размера на печалбата, устойчивостта на приходите си и възможността за минимизиране на рисковете (Vrachovska, 2019, p.66) и тъй като говорим за все повече дигитализация, банките стават все по-загрижени за по-доброто преживяване на клиентите си и тяхната сигурност. С оглед повишаване на сигурността им, банките приемат различни стратегии, за да направят процесът на интернет банкиране по-сигурен. Една такава стратегия е свързана с увеличеното използване на биометричните показатели за целите на идентификацията.

2. Биометрични данни

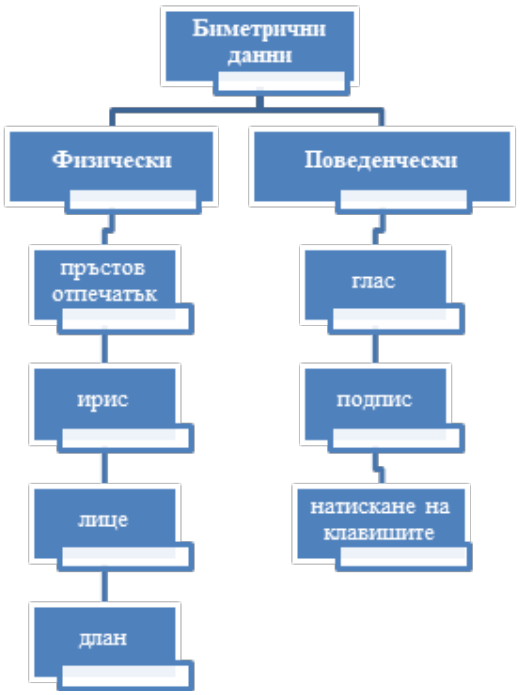
Думата „биометрия“ е комбинация от две гръцки думи – „bios“, което означава „живот“ и „metrikos“, което означава означава „измерване“ (Eneji, Ekwegh, Onyenweua, & Ajie, 2019, p.9551). Според гръцкото описание това означава, че биометрията е мярка за предоставяне на уникална идентичност на различни индивиди. Примери за такива могат да са пръстовия отпечатък, лицето, ДНК, ириса, гласа и др. В по-широк аспект може да се каже, че биометрията е измерване на характеристиките на тялото и отделни части от него, които съдържат уникални „данни“, с които никой друг индивид не разполага.

Използването на биометрични данни в банковите институции е популярно в развитите страни, поради което степента на приемане на биометрични данни нараства значително. Банковите клиенти все повече банкират онлайн, като по този начин необходимостта от лесен и защитен достъп до техните банкови данни се превърна в основен приоритет за доставчиците на банкови услуги. Следователно с разширяването на цифровизацията банките трябва да осигурят баланс между сигурността и достъпността (Morake, Khoza, & Bokaba, 2021, p.2-3).

2.1 Видове биометрични данни

Биометричните данни могат да се разделят на два вида – физически биометрични показатели и поведенчески. В някои литератури източници ги наричат още показатели от първо и второ поколение.

Физическите биометрични показатели (показатели от първо поколение) използват атрибути (белези), които лесно се виждат с очи (напр. лице, пръстови отпечатъци, ретина), докато към поведенческите биометрични показатели (показатели от второ поколение) се отнасят навици и склонности, които хората развиват с течение на времето предвид взаимодействието им с различни устройства (глас, натискания на клавиши, личен подпис) – вж. фиг.1. Тоест, поведенческата биометрична система се фокусира върху това как дадено лице извършва конкретна дейност, а не върху резултата от дейността (Banga, & Pillai, 2021, p.7).



Фиг. 1. Видове биометрични данни

Биометричните данни са естествена характеристика за устройството на индивида и опитите за злонамерена атака са почти невъзможни, тъй като само собственикът на съответното устройство, с което ползва различни онлайн услуги, може да зареди данните. При биометричните технологии отсъства вероятността за „забравяне на данни на идентификационен вход“, а също така и не стои въпросът за неправилно сканиране (напр. на пръстов отпечатък или лице), а само вероятността дали сканирането ще съвпадне или не.

Усъвършенстваните устройства, които използваме в ежедневието, използващи изкуствен интелект, са способни да се научат да разпознават само онези аспекти от поведението на индивида, които са свързани с поставената задача. Така например, използвайки мобилният си телефон, поведенческите анализи могат да оценят пасивните биометрични данни за това как всеки човек взаимодейства с телефона си: как пише, плъзга и навигира в уебсайтове и приложения.

А. Физически биометрични данни

Пръстови отпечатъци – те са най-дългогодишният, успешен и широко разпространен метод за персонална идентификация. Пръстовите отпечатъци са отличителни черти по повърхността на пръста, наричани още „триещи ръбове“, които са уникални за индивида. Пространственото разпределение на тези детайлни точки е уникално за всеки пръст.

Предимствата на използването на този биометричен показател могат да се сведат до следните (Mahajan, Malekar, More, Wairagade, & Mahalakshmi, 2016):

1. Универсалност – Пръстовият отпечатък е универсално достъпен за всеки човек. Само някои редки хора нямат пръсти.

2. Уникалност – Няма двама души с еднакви модели на пръстови отпечатъци, всеки човек има уникален пръстов отпечатък.

3. Постоянство – Пръстовият отпечатък остава за постоянно при потребителя от развитието на седеммесечния плод докато човекът умре.

Основните проблеми, които могат да възникнат при идентификация с пръстови отпечатъци, е вероятността те да не бъдат разпознати от сензора. Върху този процеса влияние могат още да окажат влага, температура, мръсотия, белези и дори износени пръстови отпечатъци. Влияние върху чувствителността на сензорите оказват още и разположението им на мобилните устройства и местоположението на пръста. От значение е височината на сензора и това дали сензорът е разположен отпред или отзад на смарт телефона, на екрана или извън него. Съществува вероятност, заради по-малката площ, която заемат сензорите, те да не разпознаят пръстовия отпечатък, ако той не е поставен на правилната част от него.

Ирис – той разполага със сложни текстурни модели с многобройни индивидуални атрибути (ивици, вдлъбнатини и др.), които се образуват до осем месеца след раждането на индивида и не се променят повече, което прави този идентификатор изключително надежден. Технологията за съпоставяне на ириса обикновено използва математически модели за разпознаване и сравняване на моделите на ириса. Тя се определя като изключително приобщаваща, сигурна и точна (International Bank for Reconstruction and Development, 2018, p.20). Към момента не се използва широко заради високите разходи за инсталиране и поддръжка.

Лицево разпознаване – един от най-широко използваните идентификатори днес. Тази технология използва характеристиките на лицето, които не се променят значително с възрастта или чрез операция. Основното предимство на този показател е, че в световен план милиарди лица вече са заснети и съществуват в различни документи, което прави биометричното разпознаване да изглежда и самостоятелно (Gates, 2011, p.47).

През 2015 г. MasterCard провеждат пилотен пробен период за одобряване на онлайн покупки с помощта на сканиране на лицето (или дланта) (CNN, 2015). Резултатите показват, че потребителите обичат биометричните данни и искат извършването на плащания в магазини да е толкова удобно, колкото отварянето на телефона им. Очаква се около 1,4 милиарда души да използват технологията за лицево разпознаване за удостоверяване на плащане до 2025 г. (CNN, 2015).

Основен проблем при използването на лицевото разпознаване като биометричен показател би могло да бъде разстоянието от устройството. Потребителите често държат камерата си по-далеч от лицето си, ако не одобряват външния си вид, а някои приложения не успяват да се справят с това. В допълнение, осветлението, като фактор на околната среда, също може да повлияе негативно на работата на системата за лицево разпознаване.

Длан – този показател постепенно придобива все повече популярност, въпреки че не е толкова разпространен колкото пръстовите отпечатъци и лицевото разпознаване. Основната идея е, че изображението на дланта с ниска разделителна способност може да се използва за извличане на самоличността на даден клиент. При използването му за мобилно банкиране, трудности се създават от това, че потребителят държи с едната си ръка телефона, докато с другата ръка заснема изображението. Проблеми се създават и за потребители с мускулно-скелетни заболявания (напр. ревматоиден артрит), които са имали проблеми с натискането на бутон и оставането стабилно по време на снимането.

Б. Поведенчески биометрични данни

Гласово разпознаване – по своята същност гласовото разпознаване е процес на преобразуване на гласа в цифрови данни. Човешкият глас се генерира от комбинация от поведенчески и физиологични характеристики. Нарича се още „гласов отпечатък“ и е показател, който предлага

безконтактно, софтуерно базирано решение, което се счита за едно от най-удобните биометрични решения за удостоверяване. Гласовите отпечатъци могат да бъдат измерени активно (например когато трябва да се произнесе конкретна парола) и пасивно (например когато човек говори естествено). Гласовата биометрична система е нововъзникваща тенденция за предупреждение с висока степен на сигурност за всяка организация (Saliha, Youssef, & Abdeslam, 2019).

Ключовите предимства на гласовото разпознаване са свързани с това, че този показател е широко достъпен за удостоверяване на мобилни телефони, тъй като всички телефони имат микрофони. Технологията е удобна и позната на повечето потребители. Заради тези предимства гласовото разпознаване може успешно да се използва и в банкирането, като в някои банки то вече е приложимо – една от най-големите британски банки използва гласова биометрична технология при банкиране по телефона за клиенти в Азия (Financial Promoter, 2024). Според някои изследвания гласово-биометричната система е бъдещето на напредналите технологии, като системата намира широко приложение и във финансите (Khan Mk, & Aithal, 2021), и в частност банковата сигурност (Khan Mk, & Aithal, 2022, p.199).

Важен фактор в процеса на идентификация е разположението на високоговорителя, както и ориентацията на телефона[1]. Основният проблем при гласовото разпознаване е свързан с произношението на думи от потребители, които не са носители на съответния официален език. Обикновено този показател изисква говорене на живо, а не от запис, което също може да затрудни процеса по идентифициране. В допълнение, не е подходящ за употреба на шумни места.

Личен подпис – това е биометрична модалност, която се използва широко за бизнес дейности. Идеята е, че се улавят поведенческите биометрични данни на ръкописния подпис (включително скорост, ускорение, ритъм, движения във въздуха и налягане) и така подписът се вгражда в електронен документ. Все още продължават опитите за разработване на много точна система за разпознаване на подписи. За подобряване ѝ са направени опити за разработване на химикалка, чувствителна на натиск.

Натискане на клавиши - разпознаването на натискането на клавиши е определено от бизнеса и от академичните среди като процес на измерване и оценка на ритъма на писане на цифрови устройства, в т.ч. на компютърни клавиатури, мобилни телефони и панели със сензорен екран.

3. Предимства и недостатъци на биометричната система

Преимуществата на биометричните системи за безопасност са очевидни – уникалните човешки характеристики са ценни за това, че трудно могат да бъдат подправени. За тях може да се обобщят следните предимства:

• Уникалност – Физическите човешките характеристики са ценни заради трудността им да бъдат подправени (трудно е да се остави фалшив отпечатък от пръст или да се промени ирисът на окото, така че да прилича на нечий друг). Този метод за идентифициране на човек е най-тясно свързан с личната самоличност, което осигурява максимално ниво на сигурност при извършване на банкови транзакции (Клочко, & Волченко 2021).

• Универсалност и постоянство – особено що се касае за пръстовите отпечатъци, тъй като те са универсално достъпни за всеки човек и само някои хора нямат пръсти. Те остават за постоянно при потребителя от развитието на седеммесечния плод до края на живота му.

• Биометричните данни не могат да бъдат забравени, изгубени или дублирани.

• Биометричните данни са по-сигурни, тъй като не може да се споделят или използват от друг потребител

• При биометричните данни отпада необходимостта да се запомнят пароли или ПИН кодове.

Към основните недостатъци на имлементирането на отделните видове биометрични показатели спадат:

• високи разходи в процеса на прилагането им;

• вероятността от кражба на биометричните данни на дадено лице и последващото им незаконно използване;

[1] Това може да се проследите при потребители с мобилни устройства с “Android” и “iOS”, тъй като сензорите се намират на различни места.

• ако вследствие на злополука потребител загуби око, пръст или промени в лицето поради драскотини или порязвания, биометричната система няма да го разпознае и ще го отхвърли в резултат на физически промени или повреди (Morake, Khoza & Bokaba, 2021, p.2-3).

• липса на законодателна уредба и отговорност за незаконното използване на биометричните данни.

Някои учени от Украйна (Клочко, & Волченко, 2021) застъпват тезата, че широкото внедряване на биометрични технологии в областта на банковата дейност е възможно на етапа на осъзнаване от потребителите на банкови услуги на предимствата на предлаганата технология и съответното законодателно регулиране на функционирането на биометричните системи. Това са системи, които комбинират няколко различни вида биометрична идентификация или комбинирани видове удостоверяване, по-специално хардуер (например електронни ключове) и биометрични технологии.

4. Проучвания за възприемане на биометричните технологии

През 2018 г. проучване на Mastercard и Оксфордския университет (Mastercard, 2018, p.10) измерва възприемането на биометричните технологии сред потребителите. То е проведено с 449 крайни потребители на внедрена система за биометрично разпознаване в случай на използване на онлайн плащания, като са изследвани техните възприятия преди, по време и след като са използвали нова биометрична система във финансов контекст в продължение на три месеца. Констатациите сред потребителите са следните:

• 93% заявяват, че ще приемат биометрични решения;

• 73% смятат, че биометричните данни ще намалят измамите;

• 83% смятат, че биометричните данни са по-сигурни от паролите;

• 92% намират биометричните данни за по-удобни от паролите.

През 2022 г. Mastercard обявява на сайта си (Mastercard, 2022) резултати от друго изследване сред потребителите си, което затвърждава положителната нагласа към използването на биометрични показатели:

• 74% имат положително отношение към биометричните технологии;

• 60% се чувстват по-сигурни, като използват биометрични данни за проверка на покупка в сравнение с пин код;

• 93% обмислят да използват нововъзникващ метод на плащане през 2022 г.

Може да се обобщи, че биометричната технология е иновативната технология, която различните банкови институции могат да използват за подобряване на сигурността и иновациите, за защита на средствата на своите клиенти срещу измамници, хакери и други ограничения. Следователно по-нататъшни проучвания могат да се съсредоточат върху комбинираната връзка между биометрични данни, цифрово банкиране и финансови технологии.

Заключение

Потребителското изживяване е основната нужда на всички мобилни потребители. Всички организации искат да подобрят изживяването на своите клиенти, за да получат предимство пред своите конкуренти. В банковата сфера се очаква биометричното идентифициране да промени начина, по който използваме банковите услуги. За да останат банките успешни и конкурентоспособни в днешния конкурентен свят, те трябва да предоставят иновативни и най-добре защитени услуги на своите клиенти.

Клиентите все повече изискват мобилни плащания, които да са лесни, бързи и сигурни. Използваните в момента методи за удостоверяване като пароли, проверка на имейли са доста проблематични както за сигурността, така и за потребителското изживяване. Това води до постепенното въвеждане на поведенческата биометрия, която удостоверява потребителя по време на сесия, работейки във фонов режим, като по този начин не пречи на потребителското изживяване. Изводът е, че бъдещето на плащанията е мобилно, като непрекъснатото удостоверяване е единственото решение за намаляване на рисковете от злоупотреби. Необходимо е да се въведат нормативни постановки, свързани със сигурността на биометричните данни.

REFERENCES

1. Клочко, А. & Волченко, Н. 2021. Біометричні технології для безпеки проведення банківських операцій в Україні та зарубіжних державах, Часопис Київського університету права, № 1

2. Banga, L. & Pillai, S. 2021. Impact of Behavioural Biometrics on Mobile Banking System, *Journal of Physics: Conference Series*, Volume 1964, Advances in Computational Electronics and Communication Engineering, p.7

CNN, 2015. MasterCard will approve purchases by scanning your face, viewed 2 February 2024 <http://money.cnn.com/2015/07/01/technology/mastercard-facial-scan/index.html>

Eneji, S. & Ekwegh, K. & Onyenweua O. & Ajie O. 2019. Enhanced Platform for the Application of Biometric Security in Electronic Banking : Case Study of Nigeria, *Asian Journal of Science and Technology*, Vol. 10, Issue, 03, March, p. 9551

3. Gates, K. 2011. Our Biometric Future. Facial Recognition Technology and the Culture of Surveillance; NYU Press: New York, p.47

International Bank for Reconstruction and Development / The World Bank. 2018. Technology Landscape for Digital Identification, viewed 2 February 2024 <https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf>, p.20

4. Khan, A. & Aithal. Sr. 2021. Future of Voice Biometric System: A Case Study, Advances in ICT & Knowledge Management: *In Cyber SpacePublisher*: New Delhi Publishers, New Delhi, India

5. Khan, A. & Aithal. Sr. 2022. Voice Biometric Systems for User Identification and Authentication – A Literature Review, *International Journal of Applied Engineering and Management Letters*, April, p.199

6. Kiyani, A. & Lasebae, A. & Ali, K. & Ur Rehman, M. 2020. Secure Online Banking With Biometrics, *International Conference on Advances in the Emerging Computing Technologies (AECT)*, Publisher: IEEE

7. Mahajan, P. & Malekar, s. & More, a. & Wairagade, a. & Mahalakshmi, B. 2016. Secured Internet Banking Using Fingerprint Authentication, *International Journal of Computer Science and Information Technology Research***,** Vol. 4, Issue 3

Mastercard, 2018. A mastercard market intelligence report, Biometrics - Meeting the challenge of authentication and payments technology, viewed 2 February 2024 <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/smb/other/biometrics_updated_030619.pdf>, p.10

Mastercard, 2020. From Password to Person The Evolution of Biometrics, viewed 2 February 2024 <https://www.mastercard.com/news/media/bchny214/evolution-of-biometrics_white-paper_v10.pdf>, p.5

Mastercard, 2022. With a smile or a wave, paying in store just got personal, Press release, viewed 8 February 2024 <https://www.mastercard.com/news/press/2022/may/with-a-smile-or-a-wave-paying-in-store-just-got-personal/>

8. Morake, A. & Khoza, L.T. & Bokaba, T. **2021**. 'Biometric technology in banking institutions: "The customers' perspectives"', *South African Journal of Information Management* 23(1), p.2–3

9. Saliha, B. & Youssef, E. & Abdeslam, D. 2019. A Study on Automatic Speech Recognition. *Journal of Information Technology Review*, 10(3), p. 77–85.

10. Vrachovska, M. 2019. Conceptual Institutionalisation and Structuring of the Public Private Partnership. V. Tarnovo: I and B, p.66

https://financialpromoter.co.uk/standard-chartered-use-sound-to-unify-brand-identity/

За контакти:
Венелина Цаневска, главен асистент, доктор
Служебен адрес: В. Търново, ул. „Арх. Георги Козарев" 1, корпус 4
ВТУ „Св. св. Кирил и Методий", Стопански факултет
Катедра „Финанси и счетоводство"
Ел. поща: v.tsanevska@ts.uni-vt.bg