Synthesis
International Scientific Conference of IT and Business-Related Research

PRIMENA SAVREMENIH TEHNOLOGIJA U BANKARSTVU: ZLOUPOTREBE I MOGUĆA REŠENJA

THE USE OF MODERN TECHNOLOGIES IN BANKING: ABUSE AND POSSIBLE SOLUTIONS

Jelena Obradović[1], Miloš Dragosavac[1], Sonja Arsić[2]
[1]Visoka poslovna škola strukovnih studija, Vladimira Perića-Valtera 4, Novi Sad, Srbija
[2]Ekonomski fakultet, Univerzitet u Nišu, Trg kralja Aleksandra Ujedinitelja 11, Niš, Srbija

Apstrakt:
U savremenom finansijskom sistemu se sve više zahteva od finansijskih institucija da proširuju svoje uslužne sisteme i povećavaju kvalitet pruženih usluga. Da bi to ostvarile, upućene su na korišćenje novih, pre svega Internet tehnologija, i usvajanje e-banking paradigme, što doprinosi lakšem pristupu uslugama, manjim troškovima, većoj transparentnosti i olakšanoj komunikaciji prilikom obavljanja finansijskih transakcija. Međutim, pored značajnog doprinosa savremenih tehnologija i Interneta u bankarskom sektoru, od velikog je značaja utvrditi i njihove negativne efekte. Uprkos stalnoj borbi da se bezbednost i privatnost na polju elektronskog bankarstva održe na što većem nivou, porast sajber kriminala narušava poverenje i utiče na povećan broj zabrinutih korisnika. Uporedo sa usvajanjem novih tehnologija, neophodno je razvijati i metode zaštite od sajber kriminala kako bi korisnici usluga bili bezbedni. U ovom radu, prikazaćemo negativne efekate primene savremenih tehnologija u bankarstvu, kao i najefikasnija rešenja za dati problem.

Ključne reči:
elektronsko bankarstvo, Internet, sigurnost, korisnici usluga.

Abstract:
In modern financial systems, the financial institutions are increasingly more expected to expand their service systems and enhance the quality of services provided. In order to achieve this, they are focused on the use of new, predominately Internet technologies, and adoption of e-banking paradigm, which enables easier access to services, lower costs, greater transparency and more facilitated communication while carrying out financial transactions. However, besides significant contribution of modern technology and the Internet to the banking sector, it is important to identify their negative effects. Despite the continuous struggle to maintain the highest possible level of security and privacy in the field of electronic banking, the increase in cyber crime distorts trust and leads to a greater number of concerned users. Along with the adoption of new technologies, it is necessary to develop methods for protection against cyber crime in order to make the users feel safe. This paper presents adverse effects of using modern technology in the banking industry, and proposes the most effective solutions for the given issues.

Key words:
e- banking, Internet, security, service users.

1. UVOD

U cilju dostizanja što bolje tržišne pozicije, u uslovima postojanja ogromne konkurencije, rastućih zahteva klijenata i korišćenja novih tehnologija, banke prolaze kroz proces tehnološke revolucije. Prolazeći kroz taj proces, svoje usluge sve više pružaju elektronskim putem što doprinosi većem kvalitetu poslovanja. Elektronsko bankarstvo (*e-banking*) je doprinelo značajnom povećanju baze korisnika putem veće dostupnosti usluga.

Uvođenje savremenih tehnologija u bankarsko poslovanje eliminisalo je problem geografske distance i značajno doprinelo lakšoj komunikaciji, povezivanju klijenata i protoku informacija. Tokom poslednjih desetak godina Internet je promenio pravila u gotovo svim privrednim granama, uključujući i bankarski sektor (Muñoz-Leiva *et al.*, 2010). Današnje banke su se transformisale u složene finansijske „makro megatrendere" – finansijske „hobotnice sa pipcima" u svim tradicionalnim bankarskim, nebankarskim, pa čak i u pomoćnim finansijskim poslovima (Momirović, 2008).

Uprkos činjenici da elektronsko bankastvo pruža mnoge prednosti i dalje postoji velika grupa klijenata koji odbijaju da usvoje takvu uslugu zbog naizvesnosti i zabrinutosti za bezbednost (Littler & Melanthiou, 2006). Shodno tome, kada je reč o primeni savremenih tehnologija u bankarskom poslovanju, bitno je identifikovati nedostatke i pretnje u procesu primene, ali i pronaći adekvatna rešenja za nastale probleme. Davaoci ovakvih usluga moraju odgovoriti na zahteve u polju bezbednosti. Iako nema sumnje da Internet bankarske trasakcije imaju slojevitu zaštitu od bezbednosnih pretnji, provajderi moraju imati takav pristup bezbednosti da je obezbeđuju u sastavu ponude usluga (Amtul, 2011).

2. RIZICI U ELEKTRONSKOM BANKARSTVU

U svakom području poslovanja, pa i u elektronskom bankarstvu, kompanije i banke se suočavaju sa određenim rizicima koji mogu ugroziti ostvarivanje njihovih ciljeva. Rizik je stanje u kojem postoji mogućnost negativnog odstupanja od poželjnog ishoda ili ishoda kome se nadamo. Stoga možemo reći da bi ri-

E-mail: jelena.obradovic.vps@gmail.com
DOI: 10.15308/Synthesis-2015-463-468

zik postojao u finansijskom poslovanju mora da bude moguć, da izaziva ekonomsku štetu, bude neizvestan i bude slučajan (Vaughan & Vaughan, 1995). Prema ISO Priručniku rizik se definiše kao efekat neizvesnosti u odnosu na ciljeve. Taj efekat može biti pozitivan ili negativan. U oba slučaja rizik predstavlja mogućnost da rezultati poslovanja odstupaju od očekivanih rezultata. Dakle, privredni subjekti koje se bave elektronskim bankarstvom (banke) projektuju svoje ciljeve za budući vremenski period na osnovu podataka o pojavama koje mogu uticati na ostvarenje ciljeva u definisanom vremenskom intervalu. Iako danas postoje mnogi modeli i programi za projektovanje određenih veličina (u ovom slučaju rezultata poslovanja banke) na osnovu njihovog odnosa sa drugim veličinama, nijedan od tih modela ne daje 100% precizne podatke upravo zbog toga što se okolnosti ne mogu uvek predvideti. Poslovanje banaka prati određeni stepen neizvesnosti koji se može definisati kao rizik poslovanja. Neizvesnost je prisutna u različitim područjima poslovanja banke tako da se može napraviti klasifikacija neizvesnosti, odnosno rizika, sa kojima se banka, kao subjekt koji se bavi elektronskim poslovanjem, sreće. U tabeli 1 dat je pregled osnovnih vrsta rizika sa kojima se banka susreće u svom poslovanju.

Operativni rizik	Reputacioni rizik	Pravni rizik	Rizik internacionalnog poslovanja
Rizik pouzdanosti i održavanja sistema Rizik dizajniranja, implementacije i održavanja sistema Rizik zloupotrebe proizvoda ili usluge od strane klijenta	Rizik negativnog javnog mnjenja Rizik odliva klijenata	Rizik pranja novca Rizik neusaglašenosti sa zakonima	Rizik zemlje Politički rizik

Tabela 1. Rizici u elektronskom bankarstvu
Izvor: Bank for International Settlements

Operativni rizik je izraz opasnosti od direktnih ili indirektnih gubitaka koji su rezultat neadekvatnih internih procesa, ljudi, sistema ili spoljašnih događaja (Vuković & Stakić, 2010). Dakle, izvor operativnog rizika su ljudi zaposleni u samoj banci, ali izvor operativnog rizika mogu biti i klijenti ukoliko zloupotrebe usluge ili proizvod banke.

Reputacija je jako bitna za svaki privredni subjekat, pa i za banku. Ukoliko banka ima lošu reputaciju klijenti nemaju poverenja i ne žele da posluju sa takvom bankom. Gubici banke zbog loše reputacije mogu biti veliki. Istraživanje koje je 2014. godine u Hrvatskoj sprovela *Hypo* banka u saradnji sa konsultanstkom kućom *A.T. Kerney* pokazalo je da je najbitniji faktor prilikom izbora banke od strane klijenata reputacija banke, a na drugom mestu je blizina banke i cena usluge.

Prvi Zakon o sprečavanju pranja novca u Republici Srbiji donet je 1. jula 2002. godine. U skladu sa ovim Zakonom formirana je finansijsko-obaveštajna služba čiji je cilj sprečavanje pranja novca. Godišnje služba primi nekoliko hiljada prijava o sumnjivim transkacijama, a najveći broj tih transakcija odnosi se upravo na bankarski sektor.

Danas su gotovo sve banke svoje poslovanje proširile i na međunarodno tržište, tako da pružaju usluge klijentima izvan granica države na čijoj teritoriji imaju svoje sedište. To je velika prednost za njih jer mogu proširiti obim svojih poslova, ali s druge strane to bankama donosi i dodatni rizik koji se pre svega odnosi na postojanje drugačijih propisa i prakse poslovanja u drugim zemljama koje im često nisu dovoljno poznati.

Lista rizika sa kojim se banke susreću u elektronskom poslovanju nije konačna. Sa razvojem modernih tehnologija i njihovom sve većom primenom u elektronskom bankarstvu lista rizika se stalno proširuje. Od banke se pre svega zahteva da razvije sistem upravljanja rizicima kako bi omogućila njihovo praćenje, pravovremeno indentifikovanje i reagovanje na njih. U procesu upravljanja rizikom, odnosno prilikom monitoringa rizika, najčešće se koristi ALM koncept koji se drugačije naziva upravljanje aktivom i pasivom banke. U okviru ovog koncepta ključno je indentifikovati rizike sa kojima se banka suočava, ali i definisati limite rizika koji moraju biti u skladu sa poslovnom strategijom banke. ALM predstavlja strategiju upravljanja ukupnom bilansnom i vanbilansnom strukturom banke koja treba da obezbedi zadovoljavajuću profitabilnost, efikasno upravljanje aktivom i pasivom i kontrolu upravljanja rizicima banke (Ercegovac & Momčilović, 2012). Primena ALM koncepta zahteva od menadžmenta banke da stalno usavršava svoj sistem upravljanja rizikom.

Potreba za stalnim praćenjem i kontrolom rizika u elektronskom bankarstvu prepoznata je i od strane Bazelskog komiteta na čiji predlog je formirana Elektronska bankarska grupa koju sačinjavaju kontrolori banaka i centralnih banaka. Cilj ove grupe je indentifikovanje osnovnih principa za praćenje rizika u elektronskom bankarsku i definisanje mera kako bi štetno dejstvo rizika bilo ublaženo, a ako je moguće i eliminisano. Korišćenje savremenih tehnologija u bankarstvu je bankama donelo odlične mogućnosti u smislu da svoje poslovanje mogu proširiti izvan granica zemlje u kojoj posluju, a da pri tom ne moraju fizički biti prisutne na tom tržištu, odnosno ne moraju otvarati svoje ekspoziture. Širenje elektronske aktivnosti banaka je pred supervizore i kontrolore banaka stavilo nove izazove koji se ogledaju u sledećem:

- Potencijalna lakoća i brzina kojom banke koje su locirane bilo gde u svetu mogu obavljati poslove sa klijentima preko povezanih elektronskih mreža iz zemalja u kojima banke nemaju licencu za poslovanje i nisu pod nadzorom;
- Potencijalna sposobnost banke koja koristeći Internet lako može da poveže svoje bankarske aktivnosti (koje su obično predmet nadzora) sa nebankarskim aktivnostima;
- Praktične teškoće sa kojima se suočavaju nacionalne vlasti koje žele da kontrolišu *e-banking* pristup sajtovima poreklom iz drugih zemalja koje ne sarađuju sa zemljom domaćinom (Bank for International Settlements, 2000).

3. ZLOUPOTREBE U ELEKTRONSKOM BANKARSTVU

Zloupotrebe su u elektronskom bankarstvu vrlo česta pojava i mogu znatno narušiti reputaciju pružaoca elektronskih usluga, ali i naneti velike štete klijentima. Zloupotreba tuđih podataka u elektronskom obliku poznata je pod nazivom sajber kriminal i poprima sve veće razmere. Tačna procena štete od sajber kriminala se ne može utvrditi prvenstveno zbog toga što banke, želeći da zaštite svoju reputaciju, često ne priznaju mogućnost "provaljivanja" njihovog sistema poslovanja i zloupotrebe njihovih podataka, odnosno privatnih podataka njihovih klijenata. Ipak, postoji uverenje da je sajber kriminal u porastu i da se svaki sistem zaštite koji koriste banke može oboriti ukoliko se u tom pokušaju uloži dovoljno vremena i sredstava. Najčešće zloupotrebe koje se javljaju u elektronskom bankarstvu su sledeće:

1. Zlonamerni kod – ovde se pre svega radi o različitim virusima i aplikacijama koje otežavaju ili praktično onemogućavaju rad sistema, a deluju tako što kopiraju višak

DOI: 10.15308/Synthesis-2015-463-468

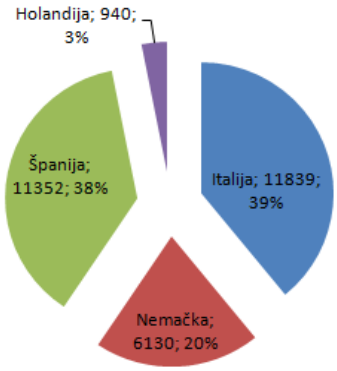
fajlova i na taj način mogu „zaraziti“ određeni program ili računar. Na primer, kreiran je *I love you* virus koji je dosta uspešno napadao *JavaScript* aplikacije.

2. Hakeri i sajbervandalizam – napadi hakera mogu biti motivisani različitim razlozima kao što je uništavanje konkretnog sajta, krađa informacija, izmena sadržaja sajta i drugo. Pod hakerima se podrazumevaju svi oni koji nemaju ovlašćeni pristup podacima, a pokušaju na nedozvoljeni način da do tih podataka dođu.
3. Zloupotreba kreditnih kartica je jako česta pojava i ona se može ogledati u krađi kreditne kartice ili zloupotrebe podataka vlasnika kreditne kartice. Zato mnoge banke svojim opštim uslovima poslovanja definišu osnovne mere opreza kojih se klijent treba pridžavati kako ne bi došlo do zloupotrebe kreditne kartice.
4. Lažno predstavljanje – ovu vrstu zloupotrebe najčešće koriste hakeri kako bi prikrili svoj indentitet prilikom neovlašćenog pristupa određenim podacima i time izbegli eventualno kaznu za to krivično delo. Najčešće u tu svrhu hakeri koriste lažne mail adrese kako bi prikrili svoj stvarni indentitet.
5. Napadi usmereni na odbijanje usluga sajta – ovi napadi se pre svega sastoje u pokušaju da se konkretni sajt optereti podacima i informacijama koje nisu bitne i to u velikom obimu kako bi se blokirao pravilan rad sajta odnosno sistema.
6. Uhođenje – predstavlja vid zloupotrebe gde se koriste posebni programi za prisluškivanje kako bi se došlo do poverljivih privatnih informacija i da bi se te iste informacije kasnije prezentovale javno.
7. Napadi iznutra – predstavljaju vrstu zloupotrebe koju čine zaposleni u određenoj organizaciji kada neovlašćeno koriste privatne informacije kojima nemaju pristup ili ih prenose neovlašćeno drugim licima izvan organizacije (Vidas-Bubanja, 2005.).

Na osnovu predstavljenih mogućih vrsta zloupotrebe može se zaključiti da banke i drugi subjekti koji se bave elektronskim poslovanjem moraju konstantno unapređivati svoje sisteme zaštite kako bi sačuvali reputaciju i onemogućili zloupotrebe privatnih podataka. S obzirom da zloupotrebe uzrokuju velike materijalne (gubitak u poslovanju), ali i nematerijalne štete (gubitak reputacije, a samim tim i klijenata), njihovom sprečavanju se treba posvetiti ogromna pažnja. Često se dešava da pojedinci nisu ni svesni da su meta sajber kriminalaca. Tako je studija u Velikoj Britaniji pokazala da 62% potrošača misli da se zloupotrebe ne mogu dogoditi njima, a 40% potošača nisu sigurni da li su do sada bili meta sajber kriminala ili ne (Polić, 2006).

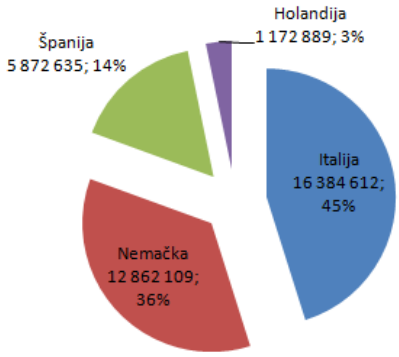
4. PRIMER ONLAJN BANKARSKE PREVARE – VIRUS EUROGRABBER

Brojnim online bankarskim prevarama pridužio se i virus *Eurograbber* koji je nastao 2012. godine i uzrokovao štetu od preko 40 miliona evra preuzimajući kontrolu nad računarima klijenata širom Evrope. Nakon što se žrtva najpre zarazi ovim virusom, napadač čeka prvu uspešnu *e-banking* prijavu žrtve, prilikom koje izlazi lažna poruka o proveri podataka sa molbom da klijent bude strpljiv. Tokom tog perioda čekanja, u pozadini, haker je u stanju da neovlašćeno prenese sredstva sa računa klijenta (OTP banka, 2012). Dakle, ukoliko korisnik nenamerno klikne na zlonamerni link, dolazi do prezimanja računara od strane trojanca koji čeka da se korisnik prijavi na svoj nalog i pokuša da izvrši neku transakciju. Kada korisnik poseti sajt banke, *Eurograbber* će ubrizgati *JavaScript* i *HTML* oznaku u njegov pretraživač, što će rezultirati sa prozorom koji će od korisnika zatražiti njihov broj telefona pod izgovorom „nadogradnje bezbednosti bankinog softvera”. To je ustvari ključ sa kojim Eurograbber prolazi autentifikaciju sa dva faktora (Online Tržište, 2012). Kada korisnik prisuti svom nalogu i pokuša da izvrši transakciju, ovaj virus omogućava napadaču da prenosi sredstva sa računa korisnika na račun napadača (tzv. račun „mule“). Slika 1 prikazuje broj pogođenih korisnika po zemljama. Uočavamo da je najviše korisnika pogođeno u Italiji (11839 korisnika - 39%), potom u Španiji (11352 korisnika – 38%) i Nemačkoj (6130 – 20%), a najmanje u Holandiji (940 korisnika – 3%).



Slika 1. Broj pogođenih korisnika po zemljama (Kanižai, 2013)

Slika 2 prikazuje količinu ukradenog novca u evrima po zemljama. Najveća količina novca je protivpravno prisvojena u Italiji (16384612€ - 45%) gde je i pogođen najveći broj korisnika, zatim u Nemačkoj (12862109€ - 36%) i Španiji (5872635€ - 14%), a najmanje u Holandiji (1172889 – 3%). Korisnici usluga elektronskog bankarstva su „osetili na svojoj koži“ koliko je bitan oprez i ogromna pažnja prilikom unosa ličnih podataka, pristupanja nalogu i vršenja transakcija.



Slika 2. Iznos protivpravno prisvojenog novca u evrima po zemljama (Kanižai, 2013)

5. SIGURNOSNA REŠENJA U ELEKTRONSKOM BANKARSTVU

Elektronsko bankarstvo menja način na koji klijenti obavljaju svoje bankarske poslove (Moga *et al.*, 2012) i oni više ne moraju da posete banku kako bi realizovali određenu aktivnost (Fonseca, 2014). U cilju eliminisanja bezbednosnih pretnji i održavanja poverenja klijenata na što višem nivou, zaposleni u okviru banke koja pruža usluge elektronskog bankarstva moraju biti obavešteni o svim mogućim pretnjama. Ulaganja u cilju dostizanja bezbednosti *e-banking* sistema su jednako bitna kao i ulaganja u sam njihov razvoj, jer opstanak elektronskog ban-

DOI: 10.15308/Synthesis-2015-463-468

karstva zavisi od ugleda banaka i njihovih sposobnosti da ubede klijente da su njihova sredstva i transakcije sigurni. Kao i kod svih online transakcija, postoje rizici u elektronskom bankarstvu koji uključuju bezbednost transakcija, finansijski gubitak zbog lične ili bankovne greške i gubitak vremena u korišćenju sistema i ispravljanju grešaka (Tassabehji & Kamala, 2012). Imajući ove rizike u vidu, svaka banka mora da razvije strategiju za smanjenje rizika ukoliko želi da zadrži klijente, privuče nove i opstane na tržištu.

U pogledu sistema elektronskog bankarstva, neki od bezbednosnih zahteva su:

- Kriptovana komunikacija (kako bi komunikacija bila zaštićena od „*man-in-the-middle*" napada, neophodno je da ista bude kriptovana);
- Limiti transakcija (limiti mogu biti po transakciji, dnevni, mesečni, itd.);
- Dvofaktorska identifikacija;

Adekvatno logovanje (sistem mora da je sposoban da ključne bezbednosne događaje loguje i da se ti logovi mogu čuvati, pretraživati i analizirati, uz čuvanje integriteta istih) (Kanižai, 2013).

Kriptografija obezbeđuje čuvanje tajnosti informacija. Ona pruža mogućnost šifrovanja poruka prilikom prenošenja poverljivih podataka putem Interneta, kao i deširovanja prilikom prijema. Ovi procesi se vrše korišćenjem kriptografskih ključeva, uz pomoć kriptografskog algoritama. Cilj ovih metoda je da se onemogući stizanje poruke u „pogrešne ruke". Slika 3 prikazuje proces kriptografije. Pošiljalac poruke transformiše otvoreni tekst u šifrant, uz pomoć ključa, i šalje ga putem komunikacionog kanala primaocu, koji ga po prijemu dešifruje. Protivnik može da dođe do širanta, ali ne poseduje ključ za dešifrovanje, tako da je otvoreni tekst zaštićen od zloupotrebe.

Najkvalitetnija kriptografska rešenja koja se primenjuju u savremenim računarskim mrežama baziraju se na primeni simetričnih kriptografskih sistema za zaštitu tajnosti (po mogućstvu uz korišćenja sopstvenih simetričnih algoritama višeg kriptografskog kvaliteta), asimetričnih kriptografskih sistema baziranih na tehnologiji digitalnog potpisa, digitalnih certifikata i hardverskih modula (kriptografski koprocesori i smart kartice) (Nuković & Soti, 2013).

Simetrični i asimetrični kriptografski algoritmi se koriste u procesu zaštite Internet i Intranet računarskih mreža. Kada su u pitanju simetrični kriptografski algoritmi, ključevi za šifrovanje i dešifrovanje su identični, što nije slučaj kod asimetričnih kriptografskih algoritama za koje je karakteristično postojanje javnog i tajnog ključa. Ključ za šifrovanje dostupan svima, dok je tajni ključ poznat samo onome ko treba da dešifruje poruku.

Dvofaktorska identifikacija predstavlja upotrebu dva identfikaciona faktora pri autentifikaciji –lozinka + PIN kod očitan sa posebnog uređaja ili biometrija (Kanižai, 2013). Dakle, postoje tri metode potvrda identiteta: potvrda „nešto što znam", kao što je lozinka, PIN kod; potvrda „nešto što imam", kao što je lična karta; i potvrda „nešto što jesam", kao što je otisak prsta i sl. (Hyun-Jung, 1995). Dvofaktorska identifikacija pruža viši nivo zaštite u poređenju sa primenom samo jedne od navedenih metoda.

Kada su u pitanju lozinke, banke najčešće preporučuju da lozinka bude složena, tj. da sadrži kombinaciju malih i velikih slova, brojeva i simbola, da ne bude laka za pogađanje, da ne sadrži značajne datume i imena i da se redovno menja.

PIN kodovi za dvofaktorsku identifikaciju generišu se na posebnim uređajima, i to najčešće na svaki minut se generiše novi kod. Uređaji za generisanje kodova mogu biti različiti, od USB tokena, preko običnog tokena u obliku priveska za ključeve, pa do jednostavne aplikacije na mobilnom telefonu (Kanižai, 2013).

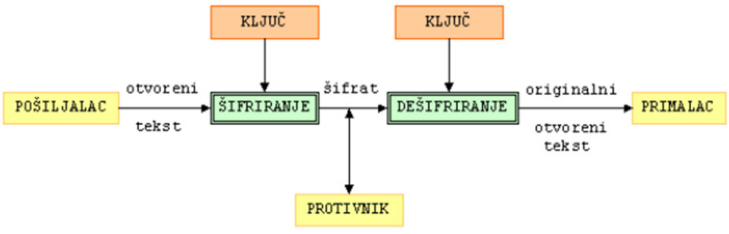
Biometrijska identifikacije se često koristi kao oblik zaštite od rizika i zloupotreba u elektronskom bankarstvu. Korišćenje PIN-ova i lozinki u e-banking proverama identiteta je često mnogo jače sredstvo u teorijskom nego u praktičnom smislu, jer korisnici u velikom broju slučajeva imaju problem da zapamte više PIN-ova i lozinki. Shodno tome, dolazi do rasta bezbednosnih rizika jer korisnici biraju jednostavne lozinke koje lako pamte i pri tome ignorišu bezbednosne savete banaka. U ovom slučaju, kao nauka o identifikovanju i prepoznavanju korisnika na osnovu njegovih fizičkih osobina i ponašanja, biometrija je efikasno rešenje. Ove osobine krisnika je veoma teško falsifikovati i kopirati. Njih korisnik ne može da izgubi ili zaboravi.

Da bi neka biometrijska karakteristika bila pogodno sredstvo za identifikaciju, mora ispunjavati sledeće uslove:

1. Univerzalnost – mora biti prisutna kod svake osobe;
2. Jedinstvenost ili individualnost – kod svake osobe karakteristika mora biti različita;
3. Trajnost i nepromjenjivost – ne sme i ne može se promijeniti protekom vremena;
4. Jednostavnost prikupljanja i poređenja – najveća prednost u odnosu na druge metode (Radmilović, 2008).

Biometrija igra značajnu ulogu u obezbeđivanju sigurnosti, i predstavlja budućnost sigurne provere identiteta. Sve više uređaja koje svakodnevno koristimo su povezani sa biometrijom (prepoznavanje glasa na mobilnim uređajima, prepoznavanje lica na pametnim telefonima i sl.). Kao posledica toga, klijenti će biti sve zahtevniji kada je u pitanju bezbednost njihovih bankovnih računa. U testu različitih biometrijskih tehnologija, provera putem otiska prsta, glas i potpisa, dobijen je rezultat da je biometrijska identifikacija putem otiska prsta korisnicima najjednostavnija za korišćenje i smatrana je najsigurnijom kada se uzmu u obzir ove tri vrste identifikacije (Tassabehji & Kamala, 2012), odnosno, izazvala je veći stepen poverenja korisnika.

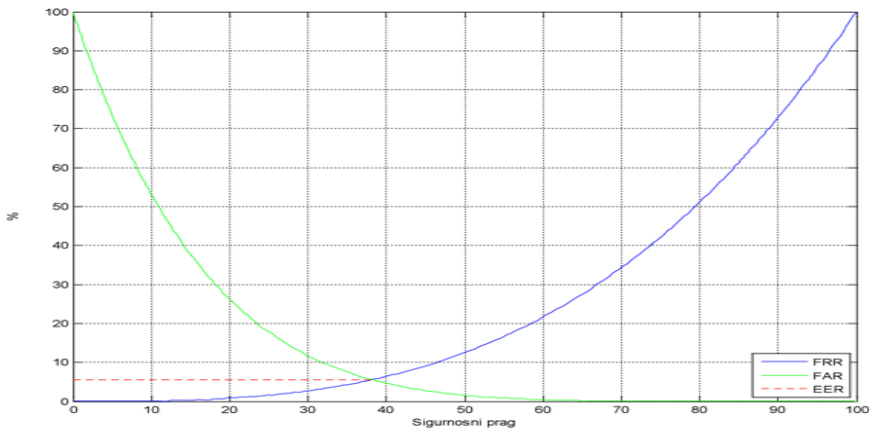
Međutim, pored brojnih prednosti, za biometrijski sistem su karakteristične i greške i nedostaci. Treba imati u vidu to da biometrija, naročito kada je u pitanju online bankarstvo za fizička lica, iako doprinosi povećanju sigurnosti, može značajno uticati na narušavanje privatnosti korisnika. Greške koje se najčešće javljaju u ovom sistemu su: pogrešno prihvatanje i pogrešno odbijanje. Pogrešno prihvatanje podrazumeva prihvatanje lažnog krisnika jer je sistem prepoznao ulazni podatak kao sličan postojećem podatku u bazi. Pogrešno odbijanje je odbijanje legitimnog korisnika jer sistem nije prepoznao podudaranje ulaznih podataka sa podacima u bazi. Da bi se bolje analizirao uticaj ovih grešaka na rad sistema potrebno je izračunati odnos između broja pogrešnih prihvatanja i broja neovlašćenih pristupa, odnosno procenat pogrešnog prihvatanja, (*False Acceptance Rate,*



Slika 3. Proces kriptografije
Izvor: Nuković & Soti (2013)

DOI: 10.15308/Synthesis-2015-463-468

FAR). Takođe, je potrebno naći i odnos između broja pogrešnih odbijanja i broja ovlašćenih pristupa, odnosno procenat pogrešnog odbijanja, (*False Rejection Rate, FRR*) (Paunović & Starčević, 2013). Sigurnosni prag sistema (*Security Threshold*) utiče na vrednosti za FAR i FAP, a njegova visina zavisi od svrhe biometrijskog sistema. Ukoliko se traži viši nivo sigurnosti nekog sistema, doćiće do smanjenja FAR-a, ali će proporcionalno doći do povećanja FRR-a. Slika 4 prikazuje vrednosti FAR i FRR i njihovu zavisnost od sigurnosnog praga u biometrijskom sistemu.



Slika 4. Primer zavisnosti FAR-a i FRR-a od sigurnosnog praga
Izvor: Paunović & Starčević (2013)

Tačka preseka krivih FAR i FRR se naziva jednaki procenat greške (*Equal Error Rate – EER*). Što je vrednost EER manja, to sistem ima bolje performance (Barzut & Milosavljević, 2013), ali ipak u praksi EER ne služi za poređenje kvaliteta sistema različitih proizvođača, pogotovo ako se vrednosti neznatno razlikuju (Paunović & Starčević, 2013).

Narodna banka Srbije (NBS) je tokom marta 2013. godine donela Odluku o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, koja je stupila na snagu 01.01.2014. godine i u kojoj se, između ostalog, ističe i značaj dvofaktorske autentifikacije u procesu povećanja sigurnosti i zaštite korisnika elektronskog bankarstva. U tački 50 Odluke se navodi da je banka dužna da, pri izvršavanju platnih transakcija u okviru elektronskog bankarstva, obezbedi da autentifikacija korisnika tog bankarstva uključi kombinaciju najmanje dva elementa za potvrđivanje korisničkog identiteta (Službeni glasnik RS, 2013). U skladu sa Odlukom neophodno je da banke u narednom periodu posvete više pažnje pitanju sigurnosti njihovih korisnika, pri čemu je, pored ovih uputstava, od ključnog značaja i to da se vode primerima iz prakse. Kada je dvofaktorska autentifikacija u pitanju, praksa pokazuje da je za njen uspeh ključna suštinska odvojenost faktora, jer bi u tom slučaju bilo neophodno hakovati istovremeno dva sistema, što otežava i komplikuje napad.

6. ZAKLJUČAK

U svom poslovanju banke se susreću sa brojnim rizicima, pri čemu su najznačajniji operativni, reputacioni, pravni i rizik internacionalnog poslovanja. Razvoj i primena savremenih tehnologija je u elektronskom bankarstvu pružila mogućnost bankama da znatno povećaju obim poslovanja i da značajno prošire svoju bazu klijenata i van granica države u kojoj je pozicionirano njihovo sedište. Međutim, savremene tehnologije su značajno povećale i rizike kojima su izložene banke i klijenti. Zbog toga je veoma bitno da banke razviju strategiju upravljanja rizicima.

Za očuvanje reputacije banaka i dostizanje uspeha u uslovima oštre konkurencije na tržištu, banke moraju neprestano raditi na povećanju nivoa sigurnosti svojih podataka, a naročito privatnih podataka klijenata, kako bi smanjila mogućnost zloupotrebe istih. Najveća pretnja za zloupotrebu privatnih podataka klijenata su različite vrste sajber kriminala, kao što su virusi, neovlašćeno korišćenje kartice, razni programi za prisluškivanje, lažno predstavljanje i sl.

U cilju eliminisanja ovakvih pretnji, očuvanja sigurnosti i privatnosti na najvišem mogućem nivou, pred banke i njihove klijente se stavljaju mnogi bezbednosni zahtevi, kao što su kriptovana komunikacija, limiti transakcija, dvofaktorska identifikacija i adekvatno logovanje. Narodna banka Srbije je donela Odluku o minimalnim standardima upravljanja informacionim sistemom finansijske institucije koja se primenjuje od početka 2014. godine i koja je, između ostalog, imala za cilj povećanje sigurnosti korišćenjem dvofaktorske autentifikacije pri obavljanju elektronskog bankarstva. S obzirom da ovakva autentifikacija podrazumeva kombinaciju dva faktora pri autentifikaciji, smanjuje se mogućnost zloupotrebe, a naročito jer se preporučuje suštinska odvojenost faktora, kako bi se otežao napad. Jedan od faktora najčešće podrazumeva biometrijsku identifikaciju koja se u praksi pokazala kao veoma uspešna. U savremenim uslovima poslovanja je neizbežno da banke usvajaju i koriste savremene tehnologije koje značajno doprinose unapređenju njihovog poslovanja, ali i to da će i dalje često biti meta hakera i sličnih pretnji. Jedino što mogu da učine jeste da nastoje da uvek budu bar jedan korak ispred njih na polju sigurnosti.

LITERATURA

Amtul, F. (2011). E-Banking Security Issues: Is There A Solution in Biometrics? *Journal of Internet Banking & Commerce, 16*(2), 1-9.

Bank for International Settlements. (1998). *Risk Management for Electronic Banking and Electronic Money Activities*. Preuzeto 2. marta 2015. sa https://www.bis.org/publ/bcbsc215.pdf

Bank for International Settlements. (2000). *Electronic Banking Group Initiatives and White Papers*. Preuzeto 2. marta 2015. sa http://www.bis.org/publ/bcbs76.htm

Barzut, S., & Milosavljević, M. (2013). Pregled savremenih Sistema za biometrijsku autentifikaciju. Interenet u edukacionom i poslovnom okruženju : zbornik radova / IV naučni skup Mreža 2013, 14.6.2013. godine, Valjevo. Beograd : Univerzitet Singidunum.

Ercegovac, D., & Momičilović, M. (2012). Investiciona strategija poslovnih banaka na finansijskim tržištima. *Škola biznisa, 2(2012)*, 35-48.

Fonseca, J. (2014). E-banking culture: A comparison of EU 27 countries and Portuguese case in the EU 27 retail banking context. *Journal of Retailing and Consumer Services, 21*(5), 708-716.

Gunson, N., Marshall, D., McInnes, F., & Jack, M. (2011). Usability evaluation of voiceprint authentication in automated telephone banking: Sentences versus digits. *Interacting with Computers, 23*(1), 57–69.

DOI: 10.15308/Synthesis-2015-463-468

Hyun-Jung, K. (1995). Biometrics, is it a Viable Proposition for Identity Authentication and Access Control? *Computers & Security, 14*(3), 205-214.

Jović, Z., & Ćorić, G. (2013). Elektronsko poslovanje kao uslov kvaliteta bankarskog poslovanja. XII međunarodni naučni skup Sinergija 2013. "Kvalitet-put u Evropu ", 29.03.2013. godine, Bijeljina (str. 448-455). Bijeljina: Univerzitet Sinergija.

Kalige, E. & Burkey D. (2012). *A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware*. Preuzeto 10. marta 2015. sa http://www.checkpoint.com/downloads/product-related/whitepapers/Eurograbber_White_Paper.pdf.

Kanižai, V. (2013). Preventivna zaštita elektronskog bankarstva. Konferencija o bezbednosti informacija BISEC 2013. 19.06.2013. (str. 35-39). Beograd: Narodna banka Srbije.

Littler, D., & Melanthiou, D. (2006). Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of Internet banking. *Journal of Retailing Consumer Services, 13*(6), 431–443.

Moga, L.M., Nor, K.M., Neculita, M., & Khani, N. (2012). Trust and Security in E-banking Adoption in Romania. *Communications of the IBIMA*, pp. 1-10.

Momirović, D. (2008). Inovacije u bankarstvu Srbije: usvajanje savremenog evropskog načina poslovanja. *Tržište, novac, kapita, 41*(3), 97-110.

Muñoz-Leiva, F., Luque-Martínez, T., & Sánchez-Fernández, J. (2010). How to improve trust toward electronic banking. *Online Information Review, 34*(6), 907–934.

Narodna Banka Srbije. (2013). *Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije*. Preuzeto 15. marta 2015. sa http://www.nbs.rs/internet/latinica/scripts/showContent.html?id=6339&konverzija=no.

Nuković, M., & Soti, R. (2013). Zaštita podataka u računarskim sistemima korišćenjem kriptografskih metoda. *Pravne teme,* 1(1), 66-78.

Online tržište. (2012). *Trojanac Eurograbber prošao autentifikaciju sa dva faktora i ukrao 40 miliona evra iz evropskih banaka*. Preuzeto 8. marta 2015. sa http://onlinetrziste.com/2012/12/trojanac-eurograbber-prosao-autentifikaciju-sa-dva-faktora-i-ukrao-40-miliona-evra-iz-evropskih-banaka/.

OTP banka. (2012). *Važno obaveštenje*. Preuzeto 15. marta 2015. sa https://www.otpbanka.rs/PDF/e_bank/Vazno_obavestenje.pdf.

Paunović, S., & Starčević, D. (2013). Biometrijski sistemi za utvrđivanje identiteta. Zbornik radova: međunarodna konferencija i izložba: XXVIII naučno-stručni skup InfoTech 2013, Aranđelovac, 12. jun - 13. jun 2013. Beograd : JURIT.

Polić, S. (2006). *Zaštita podataka u internet okruženju*. Zbornik radova: Zloupotrebe informacionih tehnologija i zaštita - ZITEH '06, Tara, 07-10.11.2006. Beograd : IT Veštak.

Radmilović, Ž. (2008). Biometrijska identifikacija. *Policija i sigurnost, 17*(3-4), 159-180.

Službeni glasnik RS. (2013). *Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije*. Službeni glasnik RS, br. 23/2013 i 113/2013. Preuzeto 15. marta 2015. sa http://www.nbs.rs/export/sites/default/internet/latinica/20/sis/min_standardi_upravljanja_IT_sistemom.pdf.

Tassabehji, R., & Kamala, M. (2012). Evaluating biometrics for online banking: The case for usability. *International Journal of Information Management, 32*(5),489-494.

Vaughan, E., & Vaughan, T. (1995). *Osnovi osiguranja: Upravljanje rizicima*. Zagreb: John Wiley & Sons.

Vidas-Bubanja, M. (2005). *E-poslovanje: menadžment, tehnologije, aplikacije*. Beograd: Beogradska poslovna škola.

Vuković, V., & Stakić, B. (2010). Rizici u bankarstvu sa posebnim osvrtom na operativni rizik. *Singidunum revija, 7*(1), 7-20.

DOI: 10.15308/Synthesis-2015-463-468