PRILAGOĐAVANJE PRAVNE REGULATIVE AKTUELNIM TRENDOVIMA U REGIONU

Priredio: Redovni profesor dr Milorad Bejatović

ADAPTING LEGAL REGULATIONS TO CURRENT TRENDS IN THE REGION

Edited by: Full Professor Milorad Bejatović, PhD

Pravni fakultet za privredu i pravosuđe
Univerzitet Privredna akademija Novi Sad
Faculty of Law for Business and Justice
University Business Academy Novi Sad

Novi Sad 2015.

Zbornik referata sa međunarodnog naučnog skupa održanog
od 24. – 26. septembra 2015. godine u Novom Sadu
u organizaciji Pravnog fakulteta za privredu i pravosuđe
Univerziteta Privredna akademija u Novom Sadu.

Izdavač:
Pravni fakultet za privredu i pravosuđe
Univerziteta Privredna akademija u Novom Sadu,
Geri Karolja br. 1, telefon: 021 400 – 499
Web: www.pravni-fakultet.info

Recezenti:
Prof. dr Milorad Bejatović
Prof. dr Mirko Kulić
Prof. dr Dragan Mrkšić
Prof. dr Bora Čejović
Prof. dr Miroslav Vitez
Prof. dr Milan Počuča
Prof. dr Milutin Đuričić
Prof. dr Zoran Pavlović
Prof. dr Ivan Joksić
Doc. dr Predrag Mirković

Za izdavača:
Prof. dr Marko Carić

Urednik:
Prof. dr Milorad Bejatović

Štampa:
Štamparija FELJTON, Novi Sad

Tiraž: 150

ISBN 978-86-6019-058-3

Štampanje Zbornika podržao
Sekretarijat za nauku i tehnološki razvoj AP Vojvodine

Članovi Programskog odbora:

Prof. dr Marko Carić
Dekan Pravnog fakulteta za privredu i pravosuđe u Novom Sadu,
Univerziteta Privredna akademija, Republika Srbija
Prof. dr Milorad Bejatović
Profesor Pravnog fakulteta za privredu i pravosuđe u Novom Sadu, Republika Srbija
Akademik prof. dr Miodrag Simović
Potpredsednik Ustavnog suda Bosne i Hercegovine
Prof. dr Borce Davitovski
Ss. Cyril nad Methodeus University, Republic of Macedonia
Prof. dr Kostadin Pušara
Predsednik Udruženja Lobista Crne Gore
Profesor Univerziteta Alfa u Beogradu, Republika Srbij**a**
Prof. dr Bora Čejović
Predsednik Krivičara Srbije
Prof. dr Miroslav Vitez
Ekonomski fakultet u Subotici, Republika Srbija
Prof. dr Dragan Mrkšić
Fakultet tehničkih nauka u Novom Sadu, Republika Srbija
Prof. dr Branko Vučković
Predsednik Osnovnog suda u Kotoru, Republika Crna Gora
Čedomir Backović
Pomoćnik ministra pravde Republike Srbije
Doc. dr Mirko Smoljić
Veleučilište „Lavoslav Ružička" u Vukovaru, Republika Hrvatska
Prof. dr Rok Lampe
Research Institute of European Faculty of Law in Nova Gorica, Republic of Slovenia
Sebastian Spinei
Faculty of Law, University „Lucian Blaga", Sibiu, Romania
Igor Denisov Yurevich
Vice President for Development at the Federal State Educational Institution of
Higher Professional Education, Omsk State Institute of Service, Russia

Članovi Organizacionog odbora:
Prof. dr Milorad Bejatović
Prof. dr Mirko Kulić
Doc. dr Predrag Mirković
Doc. dr Darko Golić
Dr. Dragan Grahovac

Sekretar skupa:
Msr Nenad Stefanović

UDK: 336.71:004.738.5

Doc. dr Gordana Bejatović / Gordana Bejatovic, PhD
Pravni fakultet za privredu i pravosuđe
Univerzitet Privredna Akademija u Novom Sadu
Faculty of Law, University Business Academy in Novi Sad
E – mail: gb@smartphoneconcept.com

Doc. dr Radmila Bejatović / Radmila Bejatovic, PhD
Informatika d.o.o. Novi Sad
E – mail: rada.bejatovic@gmail.com

Dr Jasmina Rajaković / Jasmina Rajakovic, PhD
Privileg Šabac
E –mail: jasminarajakovic@yahoo.com

RIZIK U FINANSIJSKOM POSLOVANJU

The Risk in the Finance Business

A p s t r a k t

Strategijsko opredeljenje banaka koje je uključeno u elektronsko bankarstvo i elektronski novac sve više imaju rizik kome se izlažu u samom poslovanju. Banke moraju preduzet sve raspoložive zakonske i tehnološke mere u sprečavanju rizika koji može da dovede do katastrofalnih posledica u samom opstanku poslovanja – banke. Obezbeđenje je kombinacija sistema, aplikacija i interne kontrole koja se koristi za očuvanje integriteta, autentičnosti i poverljivosti podataka i operativnih procesa. Za elektronsko bankarstvo i aktivnosti u vezi sa elektronskim novcem praćenje je posebno značajno, zbog oslanjanja pojedinih proizvoda na korištenje pojedinih mreža. Da bi se pojačala interna kontrola-revizija, menadžment mora nastojati da pronađe kvalifikovane eksterne revizore radi procene elektronskog bankarstva i aktivnosti u vezi s tim.

Ključne reči: *elektronsko poslovanje, bankarski rizici, kontrola, procena.*

A b s t r a c t

Strategic preference of banks that are involved in electronic banking and electronic money are increasingly beeing exposed to risks in everyday business. Banks must take all available legal and technological measures to prevent risks that could lead to disastrous consequences in everyday business survival of the banks. Security is a combination of systems, applications and internal controls used to

safeguard the integrity, authenticity and confidentiality of data and operational processes. For electronic banking activities in connection with electronic money tracking is particularly important, because some products are relying on the use of certain networks. To enhance internal control-auditing management must strive to find a qualified external auditors to assess electronic banking activities in that regard.

Keywords: *electronic business, banking risk, control, evaluation*

UVOD

Strategijsko opredeljenje banaka je uključivanje u elektronsko bankarstvo i aktivnosti u vezi sa elektronskim novcem. Brža upotreba elektronskog bankarstva i elektronskog novca može povećati efikasnost bankarskog i platnog sistema, na zadovoljstvo potrošača i trgovaca. U isto vreme, postoje i rizici kojima se banke izlažu u elektronskom bankarstvu i aktivnostima u vezi sa elektronskim novcem. Rizici se upoređuju sa koristima, a banke trebaju da budu u stanju da upravljaju rizikom, da ga kontrolišu i da, eventualno, apsorbuju izvesne gubitke ako to bude potrebno. Rizik u elektronskom bankarstvu i aktivnostima u vezi s elektronskim novcem treba da se procenjuje u kontekstu ostalih rizika sa kojima se banka suočava. Iako aktivnosti elektronskog bankarstva danas čine relativno veliki deo ukupnih bankarskih aktivnosti, nadzorni organi mogu zahtevati uverenje od višeg menadžmenta banaka da kritični sistemi nisu ugroženi rizikom koji banka preuzima.

Brz tempo tehnoloških inovacija je izmenio prirodu i obim rizika sa kojima se banke suočavaju u elektronskom bankarstvu i aktivnostima u vezi s elektronskim novcem. Nadzorni organi očekuju da banke imaju izgrađene procese koji omogućavaju menadžmentu banke da reaguje na postojeće rizike i da se prilagode novim rizicima. Proces upravljanja rizikom, koji se sastoji od tri osnovna elementa - procene rizika, kontrole izloženosti riziku i praćenja rizika, pomoći će bankama i nadzornim organima u postizanju ovih ciljeva. Banke mogu angažovati jedan ovakav proces kada uvode nove aktivnosti u vezi s elektronskim novcem i elektronskim bankarstvom, ili kada procenjuju već postojeće angažovanje u ovim aktivnostima.[1]

Od suštinskog značaja je da banke imaju jedan sveobuhvatan proces upravljanja rizikom, koji je pod odgovarajućim nadzorom upravnog odbora i višeg menadžmenta. Nakon identifikacije i procene novih rizika u elektronskom bankarstvu i aktivnostima u vezi s elektronskim novcem, upravni odbor i viši menadžment, treba informisati o ovim promenama. Pre nego što se otpočne bilo koja nova aktivnost mora se sprovesti sveobuhvatan pogled, kako bi viši menadžment utvrdio da li je proces upravljanja rizikom adekvatan za procenu,

1 *Basle Committee on Banking Supervision, Risk Management for Electronic Banking and Electronic Money Activities Basle, str. 10-11, mart 1998.*

kontrolu i praćenje bilo kog rizika koji se javlja u vezi s predloženom novom aktivnošću.

KONTROLA RIZIKA

Kontinuirani proces procene rizika obično obuhvata sledeće korake:

1. Prvo, banka može preduzeti jedan detaljni analitički proces za identifikaciju rizika i, kada je to moguće za njihovo kvantificiranje. U slučaju da rizici ne mogu da se kvantiflciraju, menadžment ipak može da identifikuje pojavu potencijalnih rizika i korake koje treba preduzeti da bi se ovi rizici ograničili. Menadžment banke treba da formira jednu nepristrasnu ocenu veličine bilo kog rizika, kako u pogledu uticaja koji on može imati na banku (uključujući i maksimalni potencijalni uticaj), tako i u pogledu verovatnoće da će se takav događaj desiti.

2. Drugi korak u proceni rizika jeste da upravni odbor ili viši menadžment banke odrede toleranciju rizika za datu banku. Ova procena se izvršava na bazi procene gubitaka koje će banka moći relativno bezbolno da pretrpi u slučaju da se neki dati problem materijalizuje. Konačno, menadžment može da uporedi ovako procenjenu toleranciju rizika sa procenom veličine rizika kako bi zaključio da li neka izloženost riziku ulazi u okvire tolerancije.

Posle procene rizika i tolerancije istog, menadžment banke treba da preuzme korake za upravljanje i kontrolu rizika. Ova faza procesa upravljanja rizikom obuhvata aktivnosti kao što su implementacija sigurnosnih politika i mera, koordinacija interne komunikacije, procena i unapređenje proizvoda i usluga, primena mera za upravljanje i kontrolu rizika usled oslanjanja na spoljne vršioce usluga, dostavljanje izveštaja klijentima i njihova edukacija, i razvoj »rezervnih« planova. Viši menadžment treba da omogući da osoblje koje je odgovorno za primenu ograničenja rizika ima ovlašćenja nezavisna od poslovne jedinice koja obavlja elektronsko bankarstvo ili aktivnosti u vezi s elektronskim novcem. Banke povećavaju svoju sposobnost da kontrolišu različite rizike svojstvene svim aktivnostima i da upravljaju njima kada su politike i procedure izložene u formi pisanog dokumenta i dostavljene svim relevantnim kadrovima.[2]

POLITIKA OBEZBEĐENJA

Obezbeđenje je kombinacija sistema, aplikacija i interne kontrole koja se koristi za očuvanje integriteta, autentičnosti i poverljivosti podataka i operativnih procesa. Dobro obezbeđenje oslanja se na razvoj i implementaciju adekvatnih politika i mera obezbeđenja za procese u okviru banke, kao i za komunikaciju

2 *Basle Committee on Banking Supervision, Risk Management for Electronic Banking and Electronic Money Activities Basle, str.10-1 l,mart 1998.*

između banke i spoljne sredine.[3] Mere i politike obezbeđenja mogu ograničiti rizik od eksternih i internih napada na sisteme elektronskog novca ili elektronskog bankarstva, kao i reputacioni rizik koji nastaje usled proboja obezbeđenja.

Politika obezbeđenja izrazava nameru menadžmena da podrži sigurnost informacija i obezbedi objašnjenje organizacije obezbeđenja banke. Ona takođe, postavlja smernice koje definišu sigurnosnu toleranciju rizika banke. Ova politika može definisat odgovomost za dizajn, implementaciju i uvođenje mera za bezbednost informacija, a može da ustanovi i procedure za procenu saglasnosti s politikom, uvede disciplinske mere i izveštaje o kršenju bezbednosti.

Mere obezbeđenja su kombinacija hardverskih i softverskih alata i kadrovskog menadžmenta, koji doprinose izgradnji sigurnih sistema i poslovanja. Viši menadžment treba da posmatra obezbeđenje kao jedan sveobuhvatan proces, koji je jak koliko i najslabija karika u torn procesu. Banke mogu da izaberu neke od brojnih mera obezbeđenja kako bi sprečile ili ublažile eksterne i interne napade i zloupotrebu elektronskog bankarstva i elektronskog novca. Ove mere obuhvataju, na primer, enkripciju, šifre, zaštitu od virusa i proveru zaposlenih. Enkripcija je upotreba kriptografskih algoritama za kodiranje čisto tekstualnih podataka u šifrirani tekst, kako bi se sprečilo njegovo neovlašćeno pregledavanje. Šifre, lozinke, lični identifikacioni brojevi i hardverski simboli su tehnike za kontrolu pristupa i identifikaciju korisnika.

"Požarni zid" (firewall) je kombinacija hardvera i softvera koja prati i ograničava eksterni pristup internim sistemima, koji su povezani na otvorene mreže, kao što je Internet. Protivpozarni zid može, takođe, da razvija segmente internih mreža korišćenjem Internet tehnologije (tzv. Intranet).[4] Tehnologija protivpožarnog zida, ako je pravilno dizajnirana i implementirana, može biti efikasno sredstvo za kontrolu pristupa i očuvanje poverljivosti i intergriteta podataka. Pošto je ova tehnologija vrlo kompleksna, a trenutno je i vrlo skupa, njena jačina i mogućnost treba da budu usklađeni sa osetljivošću informacija koje se štite. Dobro planirani dizajn treba da obuhvati mere obezbeđenja u čitavom preduzeću, jasne procedure za poslovanje, podelu dužnosti i izbor poverljivog osoblja, koje će biti odgovorno za konfigurisanje i funkcionisanje protiv požarnog zida.

Iako "požarni zid" prikazuje dolazeće poruke, on ne mora nužno da pruža zaštitu od programa koji se podižu sa Interneta, a koji su inficirani virusima. Kao posledica toga, menadžment treba da razvije mere za prevenciju i detekciju, kako bi se umanjile šanse za infekciju virusom i uništenja podataka, pogotovo kada je u pitanju elektronsko bankarstvo. Da bi smanjili rizik od infekcije virusima, programeri moraju da vrše kontrolu mreže, obuku krajnjih korisnika i ugradnju softvera za detekciju virusa. Nisu svi napadi na obezbeđenje eksterni. Elektronsko bankarstvo i aktivnosti u vezi s elektronskim novcem treba da budu zaštićeni, što je

3 Vidi više: Bejatović Milorad, Bankarsko pravo i hartije od vrednosti II izdanje, Apeiron, Banja Luka , 2008.

4 Basle Committee on Banking Supervision, Risk Management for Electronic Banking and Electronic Money Activities, Basle, mart 1998.

moguće više, od neovlašćenih aktivnosti sadašnjih i bivših uposlenika date banke. Kao i kod tradicionalnih bankarskih aktivnosti, provera biografskih podataka novih uposlenika, privremenih uposlenika i savetnika, kao i interna kontrola i podela dužnosti, važne su predpostavke za zaštitu bezbednosti sistema.[5]

Kad je u pitanju elektronski novac, još neke dodatne mere mogu biti od koristi pri odbijanju napada i zloupotreba, uključujuci falcifikovanje i pranje novca. Ovakve mere obuhvataju on-line interakciju sa emitentom ili centralnim operatorom; nadgledanje i praćenje individualnih transakcija; ugradnju nekvarljivih uređaja u kartice sa uskladištenom vrednošću i uređaje u trgovinama; kao i ograničavanje novčanih iznosa i datuma isteka kod kartica sa uskladištenom vrednošću.

INTERNA KOMUNIKACIJA

Aspekti operativnog, reputacionog, pravnog i ostalih rizika mogu se kontrolisati ako viši menadžment saopšti ključnom osoblju kako će elektronsko bankarstvo i elektronski novac podržati ukupne ciljeve banke.[6] U isto vreme, tehničko osoblje treba jasno da stavi do znanja višem menadzmentu kako su sistemi dizajnirani i koje su njihove prednosti i nedostaci. Ovakva procedura može smanjiti operativni rizik usled loše dizajniranih sistema, uključujući nekompaktibilnost različitih sistema u okviru bankarske organizacije; probleme u vezi s integritetom podataka; reputacioni rizik povezan sa nezadovoljstvom klijenata zbog toga što sistem ne funkcionise onako kako su oni očekivali; i kreditni i likvidnosni rizik. Da se obezbedi adekvatna interna komunikacija, sve politike i procedure treba da budu u pisanoj formi. Pored toga, viši menadžment treba da usvoji politiku korporacije o neprestanoj edukaciji i poboljšavanju veštine i znanja, koja je u saglasnosti sa tempom tehnoloških inovacija, kako bi se smanjili operativni rizici koji se javljaju usled nedostatka kadrova i stručnog menadzmenta. Obuka može obuhvatati tehničke kurseve, kao i upoznavanje osoblja sa najnovijim značajnim kretanjima na tržištu.

UNAPREĐENJE I PROCENA RIZIKA

Procena proizvoda i usluga, pre njihovog šireg uvođenja, može biti od koristi pri ograničavaju operativnog i reputacionog rizika. Testiranje potvrđuje da oprema i sistemi funkcionišu pravilno i proizvode željene rezultate. Pilot-programi ili prototipovi mogu biti od pomoći pri razvoju novih aplikacija. Rizik od usporavanja ili prekida rada sistema može biti smanjen putem politike periodične revizije mogućnosti postojećeg hjardvera i softvera.

5 Vidi više: Bejatović Milorad, Bankarsko pravo i hartije od vrednosti II izdanje, Apeiron, Banja Luka , 2008.

6 Howland, Gary: Development of an Open and Flexibile

SPOLJNI VRŠIOCI USLUGA

Rastuci trend u bankarskoj industriji i jeste da se banke strategijski fokusiraju isključivo na svoju delatnost, oslanjajući se na spoljne vršioce usluga, koji su specijalizovani za obavljanje aktivnosti koje su izvan okvira stručnosti banke. Mada ovakvi aranžmani mogu pružiti koristi, kao što su smanjenje troškova i ekonomija obima, oslanjanje na spoljne vršioce usluga ne ublažava krajnju odgovornost banke za kontrolu rizika koji utiču na njeno poslovanje. Shodno tome, banke treba da usvoje politike za smanjenje rizika usled oslanjanja na spoljne vršioce usluga. Na primer, menadzment banke treba da prati operativne i finansijske performanse spoljnih vršilaca usluga; zatim da osigura da odgovorni odnosi između ovih strana, kao i obaveze i odgovornosti svake strane, budu jasno defmisani i izloženi u formi pisanih ugovora; i da održavaju "rezervne" aranžmane za, eventualnu, brzu zamenu vršioca usluga, ako to bude potrebno.[7]

Bezbednost poverljivih informacija banke je od kritičnog značaja. Aranžman sa spoljnim vršiocima usluga možda će zahtevati da banka deli svoje poverljive podatke sa vršiocima usluga. Menadžment banke treba da proceni sposobnost vršioca usluga da održi isti nivo bezbednosti kao kad bi se ove aktivnosti obavljale unutar banke, putem pregleda politika i procedura vršioca usluga u pogledu zaštite osetljivih podataka. Pored toga, nadzorni organi će, možda, želeti da imaju pravo na nezavisnu procenu stručnosti i poslovnih i finansijskih performansi vršilaca usluga.

EDUKACIJA KLIJENATA

Edukacija klijenata može pomoći banci da ograniči pravni i reputacioni rizik. Informisanje i programi za edukaciju klijenata, koji upućuju na to kako se koriste novi proizvodi i usluge, kakve su provizije koje se zaračunavaju za proizvode i usluge, koji su mogući problemi i kakve su procedure za njihovo rešavanje, mogu pomoći banci da posluje u saglasnosti sa zakonima i regulacijama o zaštiti potrošača i privatnosti. Informacije i objašnjenja o prirodi odnosa banke sa povezanim Internet sajtovima mogu pomoći u smanjenju pravnog rizika banke, koji se javlja zbog problema sa proizvodima ili uslugama na povezanim sajtovima.

REZERVNI PLANOVI

Neka banka može smanjiti rizik poremećaja internih procesa ili isporuke proizvoda-usluga razvojem rezevnih planova, koji utvrđuju smer akcije u slučaju poremećaja funkcionisanja elektronskog bankarstva i usluga u vezi s elektronskim novcem. Rezervni plan treba da obuhvati spašavanje podataka, alternativne mogućnosti za obradu podataka i podršku klijenata. Rezervni sistemi treba

7 Krstic, Borko: "Bankarstvo", Prosveta, Nis, 1996

periodično da se testiraju kako bi se obezbedila njihova kontinuirana efikasnost. Banke treba da obezbede da njihovo rezervno poslovanje bude podjednako sigurno kao i normalno poslovanje.

Jedan značajan aspekt elektronskog bankarstva i elektronskog novca jeste oslanjanje na eksterne entitete, uključujuci dobavljače hardvera, softvera, vršioce usluga na internetu i telekomunikacione kompanije. Menadzment banke može insistirati da ovi vršioci usluga, takode, imaju mogućnost prelaska na rezervno poslovanje.[8]

Pored toga, menadžment banke može da razmotri kompenzirajuće akcije koje može da preduzme u slučaju da vršioci usluga iskuse probleme u poslovanju. Ovakvi planovi mogu da obuhvate kratkoročne ugovore sa drugim vršiocima usluga i politiku naknade gubitaka koje su klijenti pretrpeli zbog pogoršavanja kvaliteta usluga. Banka, takođe, treba da razmotri korisnost zadržavanja prava za hitnu promenu vršioca usluga, ako to bude neophodno.

Rezervni planovi mogu, takođe, doprineti ograničenju reputacionog rizika koji se javlja usled akcija same banke, ili zbog problema koje su iskusile druge institucije koje nude iste ili slične proizvode ili usluge u oblasti elektronskog novca ili elektronskog bankarstva. Na primer, banke mogu ustanoviti procedure za rešavanje problema klijenata u slučaju poremećaja u sistemu. [9]

PRAĆENJE RIZIKA

Kontinuirano praćenje je značajan aspekt bilo kog procesa upravljanja rizikom. Za elektronsko bankarstvo i aktivnosti u vezi s elektronskim novcem praćenje je posebno značajno, kako zbog toga što je u samoj prirodi ovih aktivnosti da se brzo menjaju uporedo sa inovacijama, tako i zbog oslanjanja pojedinih proizvoda na korišćenje otvorenih mreža. Dva značajna elementa praćenja su testiranje sistema i revizija.

Testiranje funkcionisanja sistema pomaže nam da otkrijemo neuobičajene aktivnosti i sprečimo krupnije probleme, poremećaje ili napade na sistem. Testiranje prodora fokusira se na identifikaciju, izolaciju i potvrdu grešaka u dizajnu i implementaciji sigurnosnih mehanizama putem kontrolisanih pokušaja prodora u sistem, koji su izvan uobičajenih procedura. Posmatranje je forma praćenja pri kome se softver i aplikacije za reviziju koriste za praćenje aktivnosti. Za razliku od testiranja prodora, posmatranje se fokusira na praćenje rutinskih operacija, ispitivanje anomalija i kontinuirano procenjivanje efikasnosti obezbeđenja putem testiranja njegove podudarnosti sa politikom obezbeđenja.

Revizija (interna i eksterna) je važan nezavisni kontrolni mehanizam za otkrivanje nedostataka i minimiziranje rizika u obavljanju elektronskog bankarstva

8 Howland, Gary: Development of an Open and Flexibile

9 Bejatović Milorad, Javne Finansije, Beogradska Poslovna Škola, 2012.god

i vršenju usluga u vezi s elektronskim novcem. Uloga revizora je da se uveri da su razvijeni odgovarajuci standardi, politike i procedure, i da ih se banka konzistentno pridržava. Osoblje koje vrši reviziju mora posedovati odgovarajuće kvalifikacije, kako bi obavilo precizan pregled. Interni revizor treba da bude odvojen i nezavisan od osoblja koje donosi odluke o uprvljanju rizikom. Da bi se pojačala interna revizija, menadžment mora nastojati da pronađe kvaliflkovane ekstrne revizore, kao sto su konsultanti iz oblasti računarske bezbednosti ili drugi profesionalci sa odgovarajućom stručnošću, radi vršenja nezavisne procene elektronskog bankarstva i aktivnosti u vezi s elektronskim novcem.

ZAKLJUČAK

Kontrola rizka u finansijskom poslovanju ne predstavlja potrebu, već apsolutnu nužnost sa kojom se suočavaju banke koje posluju na finansijskom tržištu. U radu smo ukazali na suštinski značaj realnog i pravovremenog sagledavanja svih rizika poslovanja banaka. Mišljenja smo da je od izuzetnog značaja da banke, kao veoma značajne finansijske institucije, adekvatno upravljaju rizikom, koji će se obavljati jednom vrstom monitoringa višeg menadžmenta banke. Pored toga, u radu je ukazano na potrebu kontinuiranog procesa praćenja rizika. Ukazali smo da banke moraju da preduzmu odgovorajuće korake u tom pravcu, ali i da obavljaju upravljanje rizikom. Stojimo na stanovištu da banke putem svojih aktivnosti moraju da vrše implementaciju sigurnosnih politika i mera, a što je još važnije i da vrše konstantnu i kvalitetnu komunikaciju u okviru njenog internog organizovanja. Segment rada u o pogledu istraživanja je bio usmeren i na politiku obezbeđenja, pa smo u prilikom teorijskog istraživanja zaključili da kombinacijom hardverskih i softverskih alata, banke mogu adekvatno da izgrade jedan siguran sistem bezbednosti poslovanja, koji je umnogome skopčan sa rizicima sa kojima se banke svakodnevno susreću. Posebno možemo istaći da procena rizika svakako predstavlja polaznu osnovu u sagledavanju stepene izloženosti rizicima poslovanja svake banke, te da iste moraju u okviru svog internog uređenja, kvalitetno i savremeno da urede ovaj segment interne organizacije. Na kraju možemo zaključiti da smo u radu ukazali i na potrebu adekvatne edukacije klijenata banke. Zaključak do kojeg smo došli ukazuje da adekvatno informisanje klijenata, kao i različiti programi za njihovu edukaciju, mogu da pomognu kako banci kao pružaocu usluga tako i klijentima kao korisnicima istih. Time se umnogome smanjuje jedna vrsta rizika koja je u korelaciji između banke i klijenata.

LITERATURA

1. Baker S.:'Encryption:Shielding Cyberspace", 25.Jul 1995.
2. Bauer, Paul W. -."MakingPayments in Cyberspace", Economic Commentary, Federal Reserve Bank of Cleveland, 1. oktobar 1996.
3. Basle Committee on Banking Supervision, Risk Management for Electronic

Banking and Electronic Money Activities, Basle, mart 1998.
4. Bejatović Milorad, Bankarsko pravo i hartije od vrednosti II izdanje, Apeiron, Banja Luka , 2008.
5. Bejatović Milorad, Javne Finansije, Beogradska Poslovna Škola, 2012.god
6. Berentsen, Aleksander: http://www.firstmonday.dk
7. Electronic Money/Internet Payment Systems, Electronic Banking Resourse Center, http://www2.cob.ohio-state.edu/-richards/bankpay.htm
8. Emerging Electronic Methods for Making Retail Payments, The Congress of the United States, Congressional Budget Office gopher://gopher.cbo.gov:7100/ll/reports/online/wpd.
9. Goldswothy, Mary-Anne: "Smart Card Ends Plastic Proliferation", Journal of Internet Banking and Commerce, Vol. 2, No. 3., jul 1997, http://www.ARRAYdev.com/cbmmerce JIBC/articles/
10. Howland, Gary: Development of an Open and Flexibile
11. Krstic, Borko: "Bankarstvo", Prosveta, Nis, 1996.
12. Muscovitch, Zak: "Taxation of Internet Commerce", First Monday-Peer-Reviewed Journal on the Internet, www. rirstmonday.dk.
13. Online Advertising Report, Jupiter Communications, 1996, http;//www.jup.com/
14. Security and the Internet, National Association of Clearing House Association, http://www.nacha.org/publications/digsig.htm.
15. http://www.mikro.rs/main/index.php?q=papirnoizdanje&tekstID=3921

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад

340.134(497)(082)

МЕЂУНАРОДНИ научни скуп "Прилагођавање правне регулативе актуелним трендовима у региону" (2015 ; Нови Сад)
[Zbornik referata sa Međunarodnog naučnog skupa "Prilagođavanje pravne regulative aktuelnim trendovima u regionu", 24-26. septembar 2015, Novi Sad] / [priredio Milorad Bejatović]. - Novi Sad : Pravni fakultet za privredu i pravosuđe, 2015 (Novi Sad : Feljton). - 825 str. : ilustr. ; 24 cm

Tiraž 150. - Bibliografija uz svaki rad. - Rezime na engl. jeziku uz većinu radova.

ISBN 978-86-6019-058-3

а) Правна регулатива - Усаглашавање - Балкан - Зборници
COBISS.SR-ID 299340807