Perica Miletić*

UDK 005.334:336.71
005.57:[007:004.056.5
336.71:006.35
DOI: 10.5937/MegRev2104375M
Pregledni naučni članak
Primljen 22.10.2021.
Odobren 17.11.2021.

MEĐUNARODNI NORMATIVNI OKVIR ZAŠTITE INFORMACIJA U BANKAMA I FINANSIJSKIM INSTITUCIJAMA KROZ PRIMER KONSTITUISANJA BAZELSKIH SPORAZUMA I ODREĐENJE OPERATIVNIH RIZIKA**

Sažetak: *Međunarodna koordinacija bankarskih politika može se sagledati kroz rad bazelskog komiteta, gde se svojim značajem za bezbednost i zaštitu informacija u bankama i drugim finansijskim institucijama izdvaja sporazum Bazel II, budući da on određuje operativni rizik kao jedan od ključnih rizika za poslovanje ovih subjekata. Narodna banka Srbije je na osnovu navedenog sporazuma donela prateću normativu, čime oblast zaštite informacija u tom smislu nije iscrpljena, ali predstavlja dobru osnovu za dalju razradu sistema zaštite informacija u bankama, kroz izradu lokalnih bezbednosnih politika i drugih akata koji uređuju oblast zaštite informacija u njima.*

Ključne reči: *Bazel II, operativni rizici, zaštita informacionih sistema, zaštita informacija, bezbednost, bezbednosna svest zaposlenih, bezbednosne politike, interni akti*

* Docent, Pravni fakultet, Megatrend univerzitet, Beograd; pmiletic011@gmail.com

** Rad je rezultat projekta Pravnog fakulteta FPBISD - Bezbednosni izazovi savremenog društva

1. Uvod

Neupitna je povezanost različitih ekonomskih sistema na međunarodnom nivou, odakle se može zaključiti da su oni međusobno osetljivi i da imaju uticaje jedni na druge. Ova povezanost posebno je izražena u oblasti bankarskog i finansijskog poslovanja, budući da njih karakteriše međuzavisnost na globalnom nivou, kao i proces digitalizacije procesa koje obavljaju, što predstavlja još jednu platformu za brisanje nacionalnih granica u njihovom poslovanju, sa jedne strane, i sa druge strane predstavlja još izraženiju potrebu kontrole poslovanja ovih subjekata od strane nadležnih tela.

Takođe, budući da banke i bankarske organizacije predstavljaju celovit sistem, izražena je potreba i za koordinacijom uspostavljenih kontrola i bankarskih politika, ne samo na nivou jedne države (preko nacionalnih regulacionih tela), već i na međunarodnom nivou.

Kompleksnost ovih sistema, podrazumeva i definisanje pravila po kojima se odvijaju poslovni procesi, što se u krajnjem manifestuje kroz uspostavljanje formalnih procesa na nivou jedne organizacije, a time i određivanje odgovarajućih dokumenata u kojima su ova pravila sadržana. S tim u vezi, od velikog je značaja utvrđivanje politika banaka u nekoj oblasti, budući da su na njima kasnije zasnivaju standardi, politike, pravila, procedure i drugi interni akti ovih organizacija, odakle u konačnom imamo normativni okvir uređenja neke oblasti, od čega nisu izuzeti na poslovi bezbednosti i zaštite informacija u bankama i finansijskim institucijama.

Mehanizam međunarodne koordinacije bankarskih politika može se sagledati kroz rad Bazelskog komiteta. Njegovo delovanje ima nekoliko dimenzija: harmonizaciju standarda za poslovanje banaka, nadzor nad radom bananka i saradnju sa drugim međunarodnim mehanizmima za koordinaciju bankarskih politika.[1]

Bazelski komitet za nadzor nad bankama osnovan je sedamdesetih godina prošlog veka, i tada su nacionalni organi za nadzor nad bankama nekoliko razvijenih zemalja ocenili da međunarodno poslovanje banaka, potrebe koordinacije njihovih politika i međuzavisnost nacionalnih bankarskih sistema, zahteva koordinaciju i dalje aktivnosti u tom smislu. Članovi, osnivači Bazelskog komiteta bili su guverneri centralnih banaka zemalja OECD (Organizacija za ekonomsku saradnju i razvoj), odnosno Grupe 10 i Guverner Centralne banke Švajcarske, a sve u okviru Banke za međunarodna poravnanja.[2]

---

1 Ognjanović, Vuk (2005): „Međunarodna koordinacija bankarskih politika", časopis *Bankarstvo*, https://www.ubs-asb.com/Portals/0/Casopis/2005/5_6/UBS-Bankarstvo-5-6-2005-Ognjanovic.pdf (21.08.2021.)

2 Miletić, Perica (2020): *Organizaciono i normativno uređenje zaštite informacija u funkciji bezbednosti poslovanja banaka i finansijskih institucija*, doktorska disertacija, Fakultet bezbednosti, Univerzitet u Beogradu, 241

Banka za međunarodna poravnanja (engl: Bank for International Settlements – BIS) je najstarija međunarodna finansijska organizacija, osnovana 17. maja 1930. godine u Bazelu. Banka je akcionarsko društvo sa ograničenom odgovornošću, u vlasništvu i pod upravom centralnih banaka, koje imaju pravo glasa u skladu sa brojem akcija koje poseduju. Osnovna uloga BIS-a je da podstiče međunarodnu monetarnu i finansijsku saradnju i posreduje u finansijskim transakcijama između centralnih banaka. Narodna banka Kraljevine Jugoslavije je bila članica od 1931. godine. Učešće SFRJ je zamrznuto 1992. godine, a SR Jugoslavija je 2001. godine obnovila članstvo. NBS je 2009. godine je nastavila članstvo sa 2.920 akcija. U maju 2012. godine NBS je postala član Mreže za unapređenje upravljanja centralnim bankama u okviru BIS-a.[3]

Osnovna ideja ovog tela je da standardi i smernice koje utvrđuje budu primenjivani od strane nadzornih organa učesnika, odnosno da predstavljaju neobavezujuće konvencionalne sporazume za druge zemlje. Potrebe međunarodne koordinacije bankarskih politika, zbog kvaliteta i sadržaja pravila koje je Bazelski komitet doneo, učinili su da su akta Bazelskog komiteta opšte prihvaćen model međunarodne koordinacije bankarskih politika. Glavni ciljevi Bazelskog komiteta su: jačanje zdravlja i stabilnosti sve više međuzavisnog međunarodnog bankarskog sistema i – smanjenje postojećih nejednakosti u konkurenciji između banaka osnovanih u različitim zemljama.[4]

Bazelski sporazum je više puta menjan i dopunjivan, a danas postoje: Bazelski sporazumi I, II i III, gde našu pažnju, polazeći od predmeta istraživanja, posebno privlači Bazel II, budući da on tretira operativni rizik, koji je od ključne važnosti za zaštitu informacija u bankama i finansijskim institucijama.

Bazel I sporazum je imao za svrhu uvođenje jedinstvenog načina za izračunavanje adekvatnosti kapitala, kako bi se ojačala finansijska stabilnost. Uprkos prednostima i pozitivnim efektima, vremenom je pokazao neke nedostatke, a za predmet našeg rada je ključno što prema datom standardu adekvatnost kapitala zavisi od kreditnog rizika, dok su ostali rizici (tržišni i operativni) izostavljeni iz analize.[5]

Bazel II se sastoji iz tri stuba:[6]

1) stub 1 definiše minimalne kapitalne zahteve za kreditni, tržišni i ***operativni rizik***, uz mogućnost korišćenja sofisticiranih modela i tehnika za njihovo izračunavanje;

[3] „Odnosi sa Bankom za međunarodna poravnjanja“, https://nbs.rs/sr/ciljevi-i-funkcije/medjunarodna-saradnja/bis/ (12.09.2021.)

[4] Ognjanović Vuk, 55

[5] „Bazel I“, https://nbs.rs/sr/finansijske-institucije/banke/bazelski-stendardi/bazel-I/ (15.09.2021.)

[6] „Bazel II“, https://nbs.rs/sr/finansijske-institucije/banke/bazelski-stendardi/bazel-II/ (16.09.2021.)

2) stub 2 učvršćuje vezu između optimalnih kapitalnih zahteva i vrste i stepena rizika kojima je banka izložena u svom poslovanju, uvodeći proces interne procene adekvatnosti kapitala (ICAAP) i jačajući proces supervizije;
3) stub 3 upotpunjuje vezu između stuba I i stuba II, ističući značaj tržišne discipline uvođenjem minimalnih zahteva za objavljivanje informacija banaka.

Na osnovu Bazel II NBS je donela sledeća akta (objavljena u *Službenom glasniku Republike Srbije*, 45/2011 i 46/2011):
– Odluka o adekvatnosti kapitala banke;
– Odluka o upravljanju rizicima banke;
– Odluka o objavljivanju podataka i informacija banke;
– Odluka o kontroli bankarske grupe na konsolidovanoj osnovi, i
– Odluka o izveštavanju i izveštavanju o adekvatnosti kapitala banke.

Bazel III je donet na bazi prethodnih sporazuma, kao i na osnovu iskustava svetske finansijsko-ekonomske krize. Izmene se odnose pre svega na tržišne rizike i sekjuritizaciju. Prvi put su uvedeni minimalni standardi koji se odnose na zahteve u pogledu likvidnosti banaka.[7]

Polazeći od predmeta istraživanja ovog rada, od posebnog značaja je sporazum Bazel II, budući da on kako smo prethodno naveli, u okviru stuba I tretira operativne rizike (pored kreditnih i tržišnih rizika). Neki domaći autori navode da operativni rizik prvi rizik koji investiciona društva moraju ocenjivati, znatno pre upravljanja kreditnim i tržišnim rizicima.[8]

Uvođenjem operativnog rizika u Bazelski sporazum II težilo se sledećem:[9]
– postići sveobuhvatniji tretman izloženosti rizicima, s obzirom da je prvi put pored kreditnih i tržišnih rizika regulisan i operativni rizik, kao vodeći rizik u grupi nefinansijskih rizika;
– definisanju pojma operativnog rizika;
– utvrđivanju međunarodno priznatog okvira za izračunavanje potrebnog kapitala za ukupne izloženosti rizicima, koji obuhvataju i operativne rizike;
– definisanju okvira za istraživanje i prikupljanje podataka kroz ponuđenu klasifikaciju operativnih rizičnih događaja u nekoliko kategorija.

Bazelski komitet za bankarski nadzor objavio dokument pod nazivom „ Međunarodna merenja kapitala i standardi o kapitalu, revidirani okvir“, šire

7 „Bazel III“, https://nbs.rs/sr/finansijske-institucije/banke/bazelski-stendardi/(17.09.2021.)

8 Sovilj Ranko, Stojković Zlatanović Sanja (2018): „Modeli upravljanja operativnim rizikom u investicionim društvima u procesu evropskih integracija Republike Srbije”, Institut društvenih nauka, *Megatrend revija*, Vol. 15, № 2, 1-16, https://scindeks-clanci.ceon.rs/data/pdf/1820-3159/2018/1820-31591802001S.pdf (20.09.2021.)

9 *Ibid*

poznat kao Bazel II, čime se postigla nova arhitektura bazirana na tri komplementarna koncepta: minimumu kapitalne adekvatnosti, kontrolnoj funkciji i tržišnoj disciplini. Ovaj sporazum zahteva od banaka da razvijaju robusne okvire za upravljanje rizicima, što daje sledeće pogodnosti:[10]

- obuhvatniji tretman rizika (prvi put se pored kreditnog i tržišnih rizika uključuju operativni rizici);
- šira lepeza ponuđenih pristupa za merenje rizika i kalkulacija potrebnog kapitala;
- sofisticirani način merenja rizika koje omogućava precizno određivanje rizičnog profila banke i kalkulaciju potrebnog ekonomskog kapitala;
- nov tretman instrumenata za ublažavanje izloženosti rizicima
- u okviru komplementarong koncepta („stuba") kontrolne funkcije, dat je značajan naglasak široj ulozi nacionalnih kontrola, i to ne samo u smislu razvoja internih metoda za procenu rizika, već i u smislu da kontrolori procene efekat koji rizici proizvode u odnosu na različite metode utvrđivanja ekonomskog kapitala;
- komplementarni koncept 3 („treći stub"), tržišna disciplina, zahteva od banaka da javno prezentuju visinu kapitalnih troškova, kao i procedure i mehanizme za kontrolu rizika.

Veza poslovne funkcije bezbednosti (time i zaštite informacija) i operativnih rizika u bankarstvu je očigledna, posebno kada se sagleda da „operativni rizik, kao nefinansijski rizik, predstavlja rizik direktnih i indirektnih gubitaka, koji su posledica neusaglašenih postupaka, kao i ljudskog, internog i eksternog faktora, te ukoliko se pristupi tehnološkom tumačenju pomenute definicije, primećuje se sinergija u delovanju rizika ljudskog faktora, rizika poslovanja, rizika transakcija, kao i tehnoloških rizika".[11]

Najznačajniji izvori operativnog rizika su:[12]

- interne prevare – obuhvataju pogrešno izveštavanje i druge neovlašćene aktivnosti poput neprijavljenih ili neovlašćenih transakcija, krađe, korupcije, falsifikovanja, utaje poreza, namernog uništavanja imovine, zloupotrebe ličnih podataka klijenata, insajderska trgovanja i drugo;
- eksterne prevare – obuhvataju fizičke krađe, falsifikovanje, neovlašćene upade u informacione sisteme, krađu podataka i drugo;
- propusti u odnosima sa zaposlenima i u sistemu bezbednosti na radu – obuhvataju odgovornost za zaposlene (bezbednost i zdravlje na radu), obešteće-

[10] Matić, Vesna (2009): „Bazelski sporazum II", časopis *Bankarstvo*, 7-8/2009, 118, https://www.casopisbankarstvo.rs/Portals/0/Casopis/2009/7_8/B07-08-2009-Ekoleks.pdf (22.09.2021.)

[11] Sovilj Ranko, Stojković Zlatanović Sanja, 3

[12] *Ibid,* 3-4

nje zaposlenih (isplata zarada, naknada, beneficija, prekid radnog odnosa i dr.), kao i sve vrste diskriminacije na radnom mestu;
- gubici nastali u odnosima sa klijentima, plasmanom proizvoda ili u poslovnoj praksi – odnose se na transparentnost poslovanja (kao što su agresivna prodaja, narušavanje privatnosti, zloupotreba poverljivih informacija i dr.), neodgovarajuću tržišnu ili poslovnu praksu (kršenje antimonopolskih propisa, insajdersko trgovanje, pranje novca i dr.), greške u proizvodima, loš izbor klijenata i drugo;
- oštećenje sredstava i imovine – nastalih usled prirodnih katastrofa, vandalskihi ili terorističkih napada i drugo;
- prekidi u poslovanju i pad sistema – odnose se na pad sistema prouzrokovan padom hardvera, softvera, telekomunikacijskih problema, prekidom u napajanju električnom energijom, gasom, vodom i drugo;
- gubici nastali izvršenjem transakcija, isporukom i procesima upravljanja – odnose se na evidentiranje i izvršavanje transakcija (na primer: pogrešan unos podataka, neoperativnost, propušteni rokovi, računovodstvene greške, pogrešne isporuke i dr.), propusti u obaveznom izveštavanju, nepotpuna dokumentacija klijenta, neovlašćeni pristup računima klijenata, šteta na imovini klijenata, različite vrste sporova i drugo.

Sa aspekta zaštite informacija, neusaglašenost postupaka zaposlenih, odnosno kako je to prethodno dato u određenju operativnih rizika, sinergija ljudskih i tehnoloških rizika, prave ambijent u kojem se najčešće i događaju bezbednosni propusti, na ovom mestu manje važno da li sa ili bez elemenata zlonamernosti.

Funkcionalan sistem zaštite informacija podrazumeva zaštitu od svih izvora ugrožavanja (posebno u teorijskom konceptu), ali razumljivo je da nisu svi oni događaji sa jednakom verovatnoćom nastanka, kao i događaji čije nastupanje izaziva jednako vredne posledice za poslovanje organizacije.

S tim u vezi, moguće je odrediti osnovne kategorije operativnih rizika i to:[13]
- standardni operativni rizici: prate redovne, tekuće aktivnosti u poslovanju i u proseku se događaju jednom nedeljno, a gubici su male vrednosti;
- ključni operativni rizici: javljaju se ređe, ali prouzrokuju veće gubitke naspram standardnih, ali ne mogu svojim iznosom da ugroze opstanak organizacije;
- izuzetni operativni rizici: katastrofalni, ili „rizici ubice", javljaju se izuzetno retko (jednom u deset godina), ali su posledice toliko razorne, da onemogućavaju realizovanje strateških ciljeva društva, a ponekad prete i njihovom opstanku.

[13] *Ibid.*

Na koji način je moguće suprotstaviti se ovakvim rizicima, a posebno onim koji su ključni ili katastrofalni, uvek je aktuelno pitanje. Načelno, ne postoji jednoznačan odgovor, a organizacija sistema zaštite informacija (kao i celokupnog sistema bezbednosti) zavisi od mnogo činilaca. U njih se mogu svrstati (pored identifikacije rizika) osobine koje se odnose na samo organizaciju, a gde mogu da spadaju: vrsta delatnosti (samo bankarstvo, kada je o tome reč, ima različite vrste usluga koje banke pružaju klijentima i od čega će zavisiti vrsta rizika kojoj je banka izložena. Banke koje rade pretežno sa fizičkim licima i u tradicionalnoj ekspozituri, neće biti izložena istoj vrsti rizika kao ona koja radi pretežno uslugu elektronskog bankarstva, ili ona koja pretežno radi sa privredom i drugo), veličina organizacija, razuđenost/raširenost poslovne mreže, kadrovska struktura, materijalna i tehnička opremljenost, organizacija poslovnih funkcija i brojni drugi elementi.

Nasuprot ovim različitostima, bazelski komitet je predvideo mehanizme na koji način se organizacije nose sa velikim i specifičnim skupom događaja koji mogu da predstavljaju operativni rizik, pa su na osnovu toga nacionalni regulatori (u slučaju Republike Srbije –Narodna Banka Srbije) predvidele konkretne nadležnosti. Odlukom o upravljanju rizicima banke, određeno je da:[14]

- Odbor direktora – usvaja strategije upravljanja operativnim rizicima. Ključni deo je odobravanje tolerisanog rizika od strane organizacije. Odgovoran je za efikasan nadzor nad procesom upravljanja operativnim rizikom, za razmatranje politika i procedura, preispitivanje planova za vanredne situacije. Usvaja plan kontinuiteta poslovanja (engl. *Busiess Continuity Plan* – BCP) i plan oporavka aktivnosti u slučaju katastrofa (engl: *Disaster Recovery Plan* – DRP)
- Zaposleni zaduženi za upravljanje operativnim rizicima – prate izloženost operativnom riziku prema vrstama, uzrocima i značaju događaja i o tome redovno izveštavaju članove uprave

Istim normativnim aktom Narodne banke Srbije navodi se „operativni rizik je rizik od mogućeg nastanka negativnih efekata na finansijski rezultat i kapital banke usled propusta (nenamernih i namernih) u radu zaposlenih, neodgovarajućih unutrašnjih procedura i procesa, neadekvatnog upravljanja informacionim i drugim sistemima u banci, kao i usled nastupanja nepredvidivih eksternih događaja. Operativni rizik uključuje pravni rizik.[15]

[14] Odluka o upravljanju rizicima banke, *Službeni glasnik Republike Srbije*, 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 – dr. odluka, 43/2013, 92/2013, 33/2015, 61/2015, 61/2016, 103/2016 i 119/2017, čl. 67 i 68, https://nbs.rs/export/sites/NBS_site/documents/propisi/propisi-kpb/upravljanju_rizicima_p_2017119.pdf (25.09.2021.)

[15] *Ibid,* čl. 64

Mišljenja smo da se na ovaj način potencira značaj podizanja svesti zaposlenih (engl: risk awareness) i kulture njihovog ponašanja u odnosu na izloženost operativnim rizicima, što i jeste intencija u savremenom naučnom pristupu organizovanja sistema bezbednosti organizacije. Miletić navodi da je podizanje svesti o informacionoj bezbednosti moguće organizovati preko organizacione kulture, kao i da je standardom ISO 17799 (odnosno kasnije ISO/IEC 27002) edukacija korisnika za zaštitu informacija jedan od ključnih faktora u ostvarivanju zaštite informacija.[16] I drugi naučni radovi potvrđuju postojanje značajnog pozitivnog odnosa između organizacione kulture, kulture bezbednosti i informacione bezbednosti.[17]

Polazeći od navedenog u ovom radu, možemo primetiti da je zaštita informacija, odnosno sama oblast bezbednosti, prepoznata kroz bazelske sporazume određenjem operativnih rizika kao grupe ključnih rizika za poslovanje banaka i finansijskih institucija. Narodna banka Srbije je s tim u vezi donela prethodno navedenu Odluku o upravljanju rizicima banke (način identifikacije, merenja i procene rizika kojima je banka izložena u svom poslovanju), gde se bliže određuju obaveza banaka u ovom pogledu, ali je takođe donela i druge akte koji se u većoj ili manjoj meri odnose na zaštitu informacionih sistema, gde se prema svom značaju za zaštitu informacija ističe Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije (u daljem tekstu: Odluka o minimalnim standardima).[18]

Ovaj dokument utvrđuje minimalne standarde i uslove stabilnog i sigurnog poslovanja koji se odnose na upravljanje informacionim sistemima u bankama kao i minimalne standarde za upravljanje kontinuitetom poslovanja i oporavak u slučaju katastrofa.[19] Na taj način, ovaj normativni akt eksplicitno se odnosi na zaštitu informacija u bankama i finansijskim institucijama. Od posebne važnosti, polazeći od predmeta istraživanja ovog rada, jeste odredba da je *finansijska institucija dužna da donese unutrašnji opšti akt kojim se uspostavlja okvir za upravljanje bezbednošću informacionog sistema – Politiku bezbednosti informacionog sistema*.[20] Takođe, aktom je određeno da upravljanje bezbednošću informacionog sistema podrazumeva uključivanje dovoljnog broja zaposlenih koji imaju odgovarajuću stručnost i profesionalno iskustvo.[21]

Većina autora se slaže da se dobri bezbednosni programi zaštite informacija zasnivaju upravo na politikama (engl: *policy*). Vitman i Matord (Michael E. Whitman, Herbert J. Mattord) navode da iako su politike najjeftinije sredstvo za

16 Miletić Perica, 334

17 *Ibid*, 294-303

18 Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, *Službeni glasnik Republike Srbije*, 23/2013, 113/2013, 2/2017, 88/2019 i 37/2021

19 *Ibid*, čl. 1/1 i 2

20 *Ibid*, čl. 16

21 *Ibid*, čl. 17/3/3

kontrolu, njih je obično i najteže primeniti, budući da zavise od mere u kojoj ih prihvate zaposleni u organizaciji.[22] Na ovaj način, potencira se značaj obuka, treninga, edukacija, odnosno naglašava se značaj svesti o bezbednosti zaposlenih, budući da se ovim aktivnostima utiče na njen rast.

Iako je bezbednosna politika dokument koji u strateškom smislu određuje politiku organizacije prema oblasti zaštite informacija, odakle je u tom smislu jedinstven za svaki slučaj ponaosob, može se zaključiti da postoje određena pravila za njihovo oblikovanje, i to:[23]

– nikada ne smeju da budu u suprotnosti sa zakonima;
– moraju da budu u stanju da budu održive na sudu, ukoliko ih neko osporava;
– moraju da budu ažurirane (da uvažavaju konkretne potrebe i specifičnosti organizacije, naše je mišljenje).

U praksi, svi se slažu da bezbednosne politike nije teško definisati. Problem je u njihovoj primeni, kao što smo već izneli. Autori navode da prihvatanju politika od strane organizacije pomažu sledeće smernice:[24]

– moraju se odnositi na organizaciju;
– menadžment mora obezbediti adekvatnu podelu odgovornosti za poštovanje zaštite informacija;
– krajnji korisnici (dakle svi zaposleni) treba uključiti u proces definisanja politika;
– moraju se pisati jasnim i konciznim stilom, kako njihova komplikova struktura ne bi demoralisala zaposlene da je primenjuju (ovo se obično događa kada su politike zasnovane na komplikovanim tehničkim rešenjima ili kada su pisane jezikom koji razume samo tehničko osoblje).

Bezbednosne politike (u smislu dokumenta) definišu se kao plan akcije, slično kao u politici, tako je i u poslovnom kontekstu. Ona predstavlja formalnu izjavu upravljačke filozofije organizacije u pogledu zaštite informacija. Jednom kada se politike osmisle, definišu, odobre i primene, postupci koji su potrebni za realizaciju proklamovanog mogu se nadograđivati (specifikovati prema problemu koji dokument obrađuje) i dalje primeniti. Politike su dakle skup *pravila* koja određuju prihvatljivo i neprihvatljivo ponašanje u organizaciji. Konkretizacija utvrđene politike, daje se kroz druga dokumenta, kao što su: standardi, procedure, uputstva, smernice i drugo.

Standardi su više detaljni od politika i određuju *šta* je potrebno tačno uraditi da bi bilo u skladu sa politikom. U tom smislu mogu se odrediti i tehničke kon-

[22] Whitman, M., Mattord, H. J.: Management of Information security, Course Technology Cengage Learning, second edition, Boston, USA, 2008., стр. 108. – 113.

[23] Miletić Perica, 144

[24] *Ibid.*

trole koje obezbeđuju nadgledanje primene politike, kao i napisati pripadajuće procedure. Uputstva, procedure i smernice daju odgovor na pitanje *kako* nešto uraditi, da bi bilo saglasno politici.

Politika zaštite informacija razlikuje se za svaku organizaciju pojedinačno, čak i kada je u pitanju ista industrija, budući da je svako pravno lice specifično u pogledu mnogih elemenata, a posebno kada je u pitanju njihova veličina, interna organizacija, tehnologija koja se koristi, organizaciona kultura, bezbednosna kultura i drugo.

Ipak, mogu se pronaći neka opšta načela koja ovi dokumenti treba da ispunjavaju, kao što su:[25]

- osvrt na bezbednosnu filozofiju u organizaciji;
- informacije o strukturi informacone bezbednosti u organizaciji, kao i podaci o pojedincima koji su u tom smislu najodgovorniji;
- potpuno definisanu odgovornost za bezbednost svih učesnika u organizaciji (svi zaposleni, poslovni saradnici, konsultanti, posetioci i dr.);
- potpuno definisanu odgovornost za bezbednost za svaku ulogu u organizaciji.

Da ova opšta načela mogu da variraju, u zavisnosti od mnogih uslova (nacionalna kultura, organizaciona kultura, bezbednosna kultura organizacije, normativni okvir ambijenta, vrsta industrije i drugo), možemo primeti u praktičnom ostvarivanju poslova zaštite informacija. Nije redak slučaj da se teorija bavi istraživanjima odnosa navedenih elemenata (promenljivih) i bezbednosne svesti zaposlenih, što može biti sugestija za dalja istraživanja na polju bezbednosti.[26]

U industriji bezbednosti ne postoji opšteprihvaćena praksa o klasifikaciji dokumentacije koja se odnosi na zaštitu informacija, tako da se osnovni principi, koje smo prethodno izneli, u načelu poštuju, sa povremenim odstupanjima.

Kinari (Kinnari Johanna) je istraživala problem potrebne dokumentacije za uspostavljanje bezbednosne politike u organizaciji. Tom prilikom je pregledom literature i analizom rada više autora, došla je do zaključka da ne postoji jedinstveni stav o ustrojstvu bezbednosne dokumentacije, ali da razlike u mišljenjima nisu suštinske, te da pristup ovog problema zavisi od konteksta (od konkretnih uslova organizacijskog ambijenta).[27] Autorka je u svom radu proučila devet različitih pristupa, u pogledu hijerarhijske uređenosti bezbednosne dokumentacije, a

[25] *Ibid*, 145

[26] *Ibid*, 146

[27] Kinnari Johanna (2013): „Development of a Structured Security Document Framework", Laurea University of Applied Sciences, Master's Thesis, Vantaa, Finland, https://www.theseus.fi/bitstream/handle/10024/57628/Kinnari_Johanna.pdf;jsessionid=7599D39C85C7600A43B55B320B786B8B?sequence=1 (01.10.2021.)

prema njihovoj prioritizaciji, kojom prilikom su dokumenta koja su predstavljala normativni okvir data prema sledećem:

- Povelja (deklaracija) o bezbednosti (engl: *Charter/Code of Conduct*)
- Politika bezbednosti (engl: *Policy*)
- Bezbednosni standardi (engl: *Standard*)
- Smernice iz oblasti bezbednosti (engl: *Guideline*)
- Bezbednosne procedure (engl: *Procedure*)
- Instrukcije iz oblasti bezbednosti (engl: *Instuction*)
- Kontrolne liste, alati i slično (engl: *Tool, Control, Baseline etc*)

Različiti izvori dali su i različite stavove po pitanju prioritizacije bezbednosnih dokumenata. Ne ulazeći u detaljnija razmatranja ovog istraživanja, možemo da zaključimo, da pored određenih različitosti, postoje i sličnosti koje su indikativne i mogu da nam koriste za buduća teorijska i stručna razmatranja, prema sledećem:[28]

- Bezbednosne politike se neizostavni deo normative u organizacijama. Ovaj dokument ima najveći prioritet, u skladu sa prethodno iznetim u našem radu, ukoliko se zanemare deklarativne (ali ne manje važne) „svečane izjave" o važnosti zaštite informacija
- Standardi su dokumenti koji po prioritetu prate bezbednosne politike, s tim da neki izvori, koji su u manjini, navode da im prethode smernice, odnosno procedure. Ovaj nalaz nam može biti prihvatljiv sa stanovišta konteksta o kojem smo prethodno govorili (dakle prioritet u donošenju ovog akta zavisi od konkretne organizacije, normativnog ambijenta, bezbednosne kulture organizacije i dr.)
- Smernice i procedure se gotovo jednako često nalaze na listi normativnog okvira, kao i Standardi, kao dokumenta sa nižom prioritizacijom u normativnom okviru zaštite informacija i sa većim stepenom konkretizacije tretirane oblasti koju regulišu

Ne ulazeći u detaljniju diskusiju, možemo da konstatujemo da u praksi postoje izvesna odstupanja kada je u pitanju terminologija naziva dokumenata koji čine normativni okvir organizacija kod ostvarivanja zaštite informacija. Ovo se posebno odnosi na domaću nomenklature internih akata koji se donose u organizacijama. Sa druge strane, odluke, pravilnici, naredbe, uputstva, i drugi dokumenti koji mogu biti sadržani u normativnom okviru, neće u potpunosti biti prepoznati ako to iskustvo svedemo na ravan iskustva najbolje međunarodne prakse, kada je u pitanju zaštita informacija. Tako se može dogoditi da neka organizacija nema Politiku zaštite informacija, ali ima Pravilnik koji reguliše ovu oblast. Ili – da organizacija nema Politiku koja reguliše obavezu sklanjanja dokumentacije na kraju radnog vremena (engl: *Clean Desk Policy*), ali da ima

[28] Miletić Perica, 146-147

Pravilnik u kojem su sadržane ovakve obaveze zaposlenih, ili Naredbu, odnosno drugi dokument kojim je suštinski regulisan *Clean Desk Policy*.

Na primeru donošenja Odluke o upravljanju rizicima banke i Odluke o minimalnim standardima, bez detaljnije analize njihovog sadržaja, želeli smo da ilustrujemo na koji način međunarodni normativni okvir (bazelski sporazumi) može da predstavlja osnovu za dalje regulisanje neke problemske oblasti (zaštite informacija) kod nacionalnog regulatora (Narodne banke Srbije). Odlukom u upravljanju rizicima, postigao se obavezujući tretman prisutnih rizika u bankarskom poslovanju, a posebno operativnih rizika (i rizika od kojih dolazi najveći broj bezbednosnih rizika), čime su (u ovom delu) ispunjene obaveze bazelskih sporazuma. Takođe, Odlukom o minimalnim standardima, dodatno je regulisana oblast zaštite informacionih resursa u bankama i finansijskim institucijama, na osnovu čega ovi subjekti mogu posle izrade opšteg akta (Politike bezbednosti) da dalje razrađuju drugim aktima mere i postupke koji se odnose na zaštitu informacija, a što praktično predstavlja neograničen skup pratećih tema i dokumenata, u zavisnosti od osobina konkretne organizacije i (promenljivog i nepresušnog) skupa bezbednosnih izazova, rizika i pretnji.

Literatura:

- Miletić Perica (2020): *Organizaciono i normativno uređenje zaštite informacija u funkciji bezbednosti poslovanja banaka i finansijskih institucija*, doktorska disertacija, Fakultet bezbednosti, Univerzitet u Beogradu, 241

Elektronska literatura:

- „Bazel I", https://nbs.rs/sr/finansijske-institucije/banke/bazelski-stendardi/bazel-I/ (15.09.2021.)
- „Bazel II", https://nbs.rs/sr/finansijske-institucije/banke/bazelski-stendardi/bazel-II/ (16.09.2021.)
- „Bazel III", https://nbs.rs/sr/finansijske-institucije/banke/bazelski-stendardi/(17.09.2021.)
- Kinnari Johanna (2013): „Development of a Structured Security Document Framework", Laurea University of Applied Sciences, Master's Thesis, Vantaa, Finland, https://www.theseus.fi/bitstream/handle/10024/57628/Kinnari_Johanna.pdf;jsessionid=7599D39C85C7600A43B55B320B786B8B?sequence=1 (01.10.2021.)
- Matić, Vesna (2009): „Bazelski sporazum II", *časopis Bankarstvo*, 7-8/2009, 118, https://www.casopisbankarstvo.rs/Portals/0/Casopis/2009/7_8/B07-08-2009-Ekoleks.pdf (22.09.2021.)
- Odluka o upravljanju rizicima banke, *Službeni glasnik Republike Srbije*, 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 – dr. odluka, 43/2013, 92/2013, 33/2015, 61/2015, 61/2016, 103/2016 i 119/2017, čl. 67 i 68, https://

nbs.rs/export/sites/NBS_site/documents/propisi/propisi-kpb/upravljanju_rizicima_p_2017119.pdf (25.09.2021.)

- Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, *Službeni glasnik Republike* Srbije, 23/2013, 113/2013, 2/2017, 88/2019 i 37/2021
- „Odnosi sa Bankom za međunarodna poravnjanja", https://nbs.rs/sr/ciljevi-i-funkcije/medjunarodna-saradnja/bis/ (12.09.2021.)
- Ognjanović Vuk (2005): „Međunarodna koordinacija bankarskih politika", *časopis Bankarstvo*, https://www.ubs-asb.com/Portals/0/Casopis/2005/5_6/UBS-Bankarstvo-5-6-2005-Ognjanovic.pdf (21.08.2021.)
- Sovilj Ranko, Stojković Zlatanović Sanja (2018): „Modeli upravljanja operativnim rizikom u investicionim društvima u procesu evropskih integracija Republike Srbije", Institut društvenih nauka, *Megatrend revija*, Vol. 15, № 2, 1-16, https://scindeks-clanci.ceon.rs/data/pdf/1820-3159/2018/1820-31591802001S.pdf (20.09.2021.)

Perica Miletić

UDC 005.334:336.71
005.57:[007:004.056.5
336.71:006.35
DOI: 10.5937/MegRev2104375M
Review scientific article
Received 22.10.2021.
Approved 17.11.2021.

INTERNATIONAL NORMATIVE FRAMEWORK FOR INFORMATION PROTECTION IN BANKS AND FINANCIAL INSTITUTIONS THROUGH THE EXAMPLE OF CONSTITUTING BASEL AGREEMENTS AND DETERMINING OPERATIONAL RISKS

Abstract: *International coordination of banking policies can be seen through the work of the Basel Committee, where the importance of security and protection of information in banks and other financial institutions highlights the Basel II agreement, as it identifies operational risk as one of the key risks for these entities. Based on the said agreement, the National Bank of Serbia adopted an accompanying norm, which does not exhaust the field of information protection in that sense, but represents a good basis for further elaboration of information protection systems in banks, through development of local security policies and other acts regulating information protection in them.*

Keywords: *Basel II, operational risks, information systems protection, information protection, security, employee security awareness, security policies, internal acts*