MENADŽMENT ORGANIZACIONE BEZBEDNOSTI PLATNOG PROMETA

Ilija Životić[15], Kristijan Ristić[16], Snežana Krstić[17], Srboljub Nikolić[18], Bruno Đuran[19]

doi: 10.5937/Oditor2203072Z

Pregledni rad
UDK: 005:336.717.13

Apstrakt

Menadžment rizika u platnom prometu obuhvata identifikovanje, merenje i upravljanje rizicima. Zato je neophodno uspostaviti njegovu efikasnu funkciju u platnom prometu. U poslednjih deset godina, evedentan je razvoj menadžmenta rizika u zemljama u tranziciji. Imajući ove činjenice u vidu, cilj ove istraživačke studije sastoji se u sagledavanju rizika u platnom prometu, sa posebnim osvrtom na analizu upravljanja gotovinom. Rezultati ove pregledne studije pokazuju da svaka banka posluje sa manjim ili većim brojem rizika, pozicionirajući se između dva ekstrema: apsolutno prihvatanje rizika i apsolutno neprihvatanje rizika. Nepohodno je da stepen prihvatanja rizika bude proporcionalan sposobnosti banke da pokrije nastale gubitke, kao i da ostvari prihvatljivu stopu prinosa. Ostvarivanje viših prinosa je moguće ukoliko banka uspostavi efikasnu identifikaciju, merenje i upravljanje rizicima poslovanja. Nosioci narušavanja sigurnosti proizlaze iz vrste izvora iz kojih će kasnije proizići i oblici narušavanja sigurnosti. Da bi se sprovela odbrambeno-zaštitna funkcija, potrebno je da se u njoj uvrstite one mere koje pružaju mogućnost eleminisanja elemenata koji dovode do narušavanja sigurnosti i opasnosti. Te mere moraju da budu sastavni deo institucije i izvođenja radnog procesa. Uslov za sigurno i normalno poslovanje u platnom prometu gotovinom podrazumeva

[15] dr Ilija Životić,docent, Univerzitet Union "Nikola Tesla", Fakultet za inženjerski menadžment, Bulevar vojvode Mišića 43, Beograd, R. Srbija, email: ilijazivotic@gmail.com
[16] dr Kristijan Ristić, vanredni profesor, Univerzitet MB, Poslovni pravni fakultet, Knez Mihajlova 33, Beograd, Srbija, E-mail: kristijanristic.fpim@yahoo.com
[17] dr Snežana Krstić, vanredni profesor, Univerzitet odbrane, Vojna akademija, Veljka Lukića Kurjaka 33, Beograd, R. Srbija, email: snezanakrstic17@gmail.com
[18] dr Srboljub Nikolić, docent, Univerzitet odbrane, Vojna akademija, Veljka Lukića Kurjaka 33, Beograd, R. Srbija, email: srboljub.nikolic@yahoo.com
[19] dr Bruno Đuran, vanredni profesor, Univerzitet za poslovne studije, Jovana Dučića 23a, Banaja Luka, BiH, email: ups@univerzitetps.com

neophodnost posedovanja obučenog ljudstva za sprovođenje funkcije sigurnosti. Da bi se sprovela funkcija sigurnosti i da bi se njome uspešno upravljalo, potrebno je da se itegrišu različite norme u postojećim zakonskim propisima.

Ključne reči: *menadžment rizika, platni promet, gotovina i sigurnost.*

JEL: *E42, E49.*

Uvod

Usled globalizacije stanovništva, ekonomije i politike, rasta stranih investicija i prekograničnih transfera, integracija berzi u jedinstveni sistem i rasta njihovih plasmana, ukidanja suvišnih finansijskih procesa kroz smanjivanje uticaja države na finansijske aktivnosti, uspostavljanja savremene tehologije, fluktuacije deviznih kurseva i cena strateških proizvoda, dolazi do povećanog rizika u poslovanju kod svih učesnika na finansijskom tržištu. Rizik je prisutan u svim institucijama koje posluju na tržištu. Rizik definišemo kao procenat verovatnoće pojave negativnih događaja, koji imaju negativne posledice na poslovanje. Njegova osnovna karakteristika je stalnost. On postoji u svim institucijama u većoj ili manjoj meri, nije ga moguće eleminisati, ali ga je moguće smanjiti.

Tradicionalne finansijske institucije su izložene riziku likvidnosti, kreditnom riziku, kamatnom riziku, deviznom riziku, riziku koncentracije, operativnom riziku i strateškom riziku. Istim rizicima izložene su i centralne banke, ali sa većim stepenom zaštite jer se njihov portfolio sastoji od plasmana visoke sigurnosti. Za razliku od tradicionalnih finansijskih institucija, centralne banke su neprofitne institucije, osnovane sa ciljem obezbeđenja sigurnosti javnih fondova.

Analizom relevantne literature, u poslednjih deset godina, prisutna je tendecija upravljanja rizicima centralne banke, njihovo identifikovanje i razvoj instrumenata za procenu rizika odnosno njihovo merenje.

Cilj rada

Obzirom da poslednjih godina u svetu postoji rastući trend napada na institucije koje se bave platnim prometom, a pre svega gotovinom, cilj ove istraživačke studije sastoji se u sagledavanju rizika u platnom prometu, sa posebnim osvrtom na analizu upravljanja gotovinom.

Metod rada

Sistematski pregled literature je obavljen putem pretrage u bazama podataka PubMed, Google Scholar Advanced Search i Konzorcijuma biblioteka Srbije za objedinjenu nabavku – KoBSON. Radovi su pretraživani prema sledećim ključnim rečima i sintagmama: upravljanje rizikom u finansijskim institucijama, platni promet i rizik, gotovina i sigurnost, izvori rizika u platnom prometu, vrste i intenzitet rizika u platnom prometu. Analizirane su studije na engleskom i srpskom jeziku.

Menadžment rizika u platnom prometu

Radi zaštite banke od svih rizika, uključujući i kreditni rizik, kapitalizacija banke se nameće kao njena trajna orijentacija uz diverzifikaciju porfelja. U svim bankama implementiran je sistem izveštavanja o procentu zastupljenosti rizika. Ovo izveštavanje može biti redovno i periodično. Upravljanje odnosima sa klijentima (engl. Customer relationship managmenet – CRM)(Mansfield-Devine, 2018) odnosno učestvovanjem u procesu odlučivanja kreditnog odbora banke, utvrđuje se potencijalna opasnost od postojanje rizika kod svakog pojedinačnog klijenta ili u grupi klijenata(Kovačević & Gajić, 2019). CRM utvrđuje opasnost od rizika u skladu sa zakonskom regulativom i sastavlja izveštaj na mesečnom nivou, koji se dostavlja članovima uprave banke. Na mesečnom nivou se uprava banke upoznaje i sa stepenom zastupljenosti rizika putem izveštaja o kvantitetu portfolia banke, koji se sastavlja pararelno sa tipom i zakonskim procentom ograničenja. Zbirni bruto bilans banke, zbirna tabela eksponiranosti i analitičke kartice klijenata predstavljaju osnovu za sačinjavanje izveštaja o kvantitetu portfolia banke. Takođe uprava banke daje smernice za otklanjanje konkretnih prekoračenja, upravljanje i kontrolu postojećih i potencijalnih rizika banke(Hull et al., 2019).

Prema ABRS metodologiji banke prate i analiziraju stepen izloženosti kreditnom riziku, koji obuhvata potraživanja po glavnici, kamatama, naknadama, obavezama prema pojedinačnom klijentu ili prema grupi klijenata. Stepen izloženosti kreditnom riziku u obliku izdatih garancija ne sme iznositi preko 100% iznosa osnovnog kapitala banke. Izloženost banke kreditnom riziku prema pojedinačnom klijentu ili prema grupi klijenata ne sme iznositi preko 40% iznosa osnovnog kapitala banke. Osnovni kapital banke, odnosno maksimalna izloženost kreditnom riziku strukturirana je prema sledećim ograničenjima(Živković, 2019):

- Do 5% iznosa osnovnog kapitala banke gde nije kreditni rizik pokriven kolateralom;

- Od 5% do 25% iznosa osnovnog kapitala banke gde je kreditni rizik pokriven kolateralom;
- Preko 25% iznosa osnovnog kapitala banke gde je kreditni rizik pokriven kvalitetnim utrživim zalogom čija je vrednost viša od vrednosti kolaterale.
- Do 20% iznosa osnovnog kapitala banke, ako je kreditni rizik u obliku izdatih garancija, osim garancija za dobro izvršenje posla.

Akreditivi i garancije iskazane u novčanim vrednostima ne uključuju se u ukupnom izlaganju kreditnom riziku do iznosa njihovog pokrića. Ukoliko je ukupna izloženost banke kreditnom riziku prema pojedinačnom klijentu ili prema grupi klijenata viša od 15% iznosa osnovnog kapitala banke smatra se da je izlaganje banke kreditnom riziku velika. Zbir svih velikih izlaganja banke kreditnom riziku ne sme da pređe iznos od 300% iznosa osnovnog kapitala banke(Zhao et al., 2018).

U savremenom svetu, pod uticajem modernizacije tehnologije i elektronskog načina komunikacije, poslovanje banke je pod većim rizikom. Smanjena sposobnost banke da efikasno posluje i da jača svoju poslovnu i finansijsku poziciju, nestalnost zarađivanja i smanjenje kapitala predstavljaju osnovne karakteristike banke koja je izložena riziku. Kako bi banka zadržala svoju solventnost, ona mora da poseduje kapital, koji će pokriti potencijalne gubitke nastale usled nestalnosti zarađivanja. Takođe, neophodno je da banka upravlja svojim rizicima, naročito većim rizicima kojima je izložena.

Razlikujemo dve vrste rizika koji mogu uticati na nestalnost zarađivanja: finansijske i nefinansijske rizike. Finansijski rizici su direktno povezani sa ulogom finansijskog principala i posrednika, dok nefinansijski rizici nastaju kao posledica neadekvatnih procedura, usled eksternih i ljudskih faktora. U finansijske rizike ubrajamo kreditne, tržišne i ALM (engl. Asset-liabiilty management). Operativni, poslovni, reputacioni, strateški, zakonski i drugi rizici smatraju se nefinansijskim rizicima.

Kao vid sigurnosti i obezbeđenje garancije od izloženosti riziku, neophodno je da banke izdvajaju posebni kapital, koji bi služio kao pokriće za potencijalne gubitke prouzrokovane finansijskim i nefinansijskim rizicima. Izuzev identifikacije rizika, njihovog praćenja i kontrole, neophodno je da banke uspostave i sistem kvantifikacije izloženosti riziku odnosno sistem merenja(Li et al., 2019). Primenom sistema identifikacije, praćenja, kontrole i merenja rizika od strane banke, može se reći da je uspostavljen efikasan sistem upravljanja rizicima. Na osnovu Bazelskog komiteta za bankarski nadzor i međunarodnih sporazuma banke razvijaju sofisticirane modele za kvantifikaciju izloženosti riziku. U zavisnosti od izabranog modela, pravi se razlika između očekivanih i neočekivanih gubitaka. Očekivani gubici su oni za koje postoji

stepen verovatnoće da će nastati i oni su poznati banci. Oni se procenjuju i za njihovo pokriće se izdvajaju rezerve. Za razliku od očekivanih gubitaka, neočekivane gubitke nije moguće predvideti. Na njih se primenjuje sistem merenja rizika, putem precizne kvantifikacije rizika i izdvajanja kapitala od strane banke u cilju pokrića(Griffiths et al., 2017).

Da bi banka uvek bila solventna i imala mogućnost da se zaštiti od eventualnih gubitaka u određenom periodu, ona mora da vodi računa o veličini ekonomskog kapitala banke. S obzirom da je ekonomski kapital, veliki trošak za banku, potrebno je da njegova veličina bude usaglašena za rizičnim profilom banke(Mihajlović et al., 2020). On predstavlja meru ukupnog rizičnog profila banke, kao i meru promena njenih rizika u vremenu. Koristi se prilikom izračunavanja procenta zarade banke u odnosu na stepen izloženosti riziku. Služi za komparaciju različitih vrsta rizika.

Bilo koja neizvesna situacija u bankarskom poslovanju, odnosno postojanje verovatnoće gubitaka usled obavljanja određenih bankarskih aktivnosti predstavlja rizik. Svaka banka posluje sa manjim ili većim brojem rizika, pozicionirajući se između dva ekstrema: apsolutno prihvatanje rizika i apsolutno neprihvatanje rizika(Vićić, 2016). Nepohodno je da stepen prihvatanja rizika bude proporcionalan sposobnosti banke da pokrije nastale gubitke, kao i da ostvari prihvatljivu stopu prinosa. Ostvarivanje viših prinosa je moguće ukoliko banka uspostavi efikasnu identifikaciju, merenje i upravljanje rizicima poslovanja.

Sigurnost platnog prometa gotovinom

U platnom prometu gotovinom predmeti narušavanja sigurnosti platnog prometa dele se na subjekte i objekte narušavanja sigurnosti. Radnici i klijenti bankarskih institucija čine subjekte narušavanja sigurnosti, dok imovina tj. novac i poslovni procesi predstavljaju objekte narušavaja sigurnosti u platnom prometu gotovinom.

Po prirodi nastanka izvori narušavanja sigurnosti u platnom prometu gotovinom mogu biti prirodni, društveni i tehničko-tehnološki. Nosioci narušavanja sigurnosti proizlaze iz vrste izvora. U prirodne izvore ubrajamo prirodne sile i pojave, dok u društvene izvore ubrajamo pojedince, kriminalne ili terorističke organizacije i nedovoljnu organiziranost društva. Među tehničko-tehnološkim izvorima izdvajamo neorganizovanost poslovanja institucije i/ili društva, nemar i nebrigu(Mirković et al., 2022).

Oblici narušavanja sigurnosti proizlaze iz izvora narušavanja sigurnosti. Pljuskovi, grmljavina, zemljotresi i poplave su oblici narušavanja sigurnosti karakteristični za prirodne izvore. Njih nije moguće predvideti i nastaju kao

posledica prirodnih sila(Papp et al., 2019). Teroristički napadi, provale, krađe i protesti su oblici narušavanja sigurnosti karakteristični za društvene izvore. U cilju sprečavanja nastanka takvih pojava, postoji mogućnost njihovog utvrđivanja učestalosti prikupljanjem i analizom informacija, definisanjem mera zaštite i odbrane. Pad informacionih sistema, kvar ili otkazivanje uređaja su oblici narušavanja sigurnosti karakteristični za tehničko-tehnološke izvore. Sprečavanje ovakvih negativnih posledica postiže se redovnim održavanjem i obezbeđivanjem zamenskih delova.

Izvori narušavanja sigurnosti koriste se i za izbor sredstava za realizaciju oblika narušavanja sigurnosti. Prirodni izvori se koriste kao sredstava narušavanja sigurnosti za prirodne pojave za koje se zna da se mogu u budućnosti dogoditi, ali se ne zna u kom trenutku će se dogoditi. Platni promet gotovinom je najviše narušen društvenim izvorima narušavanja sigurnosti npr. napadi na banke, provale i krađe(Raskin, 2017). Sredstva narušavanja sigurnosti koja se mogu koristiti iz društvenih izvora su oružje, noževi, palice i drugo. Sredstva narušavanja sigurnosti mogu biti i iz tehničko-tehnoloških izvora kao što su vatra, električna struja i drugo.

Takođe metode narušavanja sigurnosti platnim prometom gotovine se razlikuju u odnosu na izvore narušavanja sigurnosti. Potresima i poplavama smatraju se metode narušavanja sigurnosti nastale iz prirodnih izvora. Provale, napadi i krađe smatraju se metodama narušavanja sigurnosti nastale iz društenih izvora. Tehničko-tehnološke metode narušavanja sigurnosti nastale su iz tehničko-tehnoloških izvora.

Za izvore i metode narušavanja sigurnosti vezan je vremenski period narušavanja. Vremenski period narušavanja sigurnosti iz prirodnih izvora je trajniji zbog nepredvidljivosti. Vremenski period narušavanja sigurnosti iz društvenih izvora povezuje se sa izvorom narušavanja sigurnosti. Vremenski period narušavanja sigurnosti napadom na finansijske institucije traje tokom vremena boravka zaposlenih u samim objektima finansijskih institucija, zatim prilikom prenosa i transporta novca sa jedne lokacije na drugu.

Iz izvora narušavanja sigurnosti proizilazi i intezitet narušavanja. On takođe zavisi od faze poslovnog procesa upravljanja gotovinom. U zavisnosti od izvora intezitet narušavanja sigurnosti može biti jakog i slabog inteziteta.

Posledice narušavanja sigurnosti platnog prometa gotovinom zavise od načina primene odbrambeno-zaštitnih funkcija institucije. Mogu se klasifikovati po predmetu koji ima za posledicu narušavanje sigurnosti(Avakumović, et al., 2021):

- osoba (smrt, teža ili lakša telesna povreda, psihički slom);

- imovina (gubitak i oštećenje novca);
- poslovni proces (trajni ili privremeni prekid poslovanja).

Analizom napada na finansijske institucije, posmatrajući period u proteklih pedeset godina, evidentan je stalan rast. Međutim ukoliko se posmatra napad na finansijske institucije prilikom transporta gotovine, može se reći da je zabeležen pad. To se opravdava činjenicom da se prilikom transporta gotovine, sistem zaštite stalno implementira i usložava, što dovodi do toga da je napadačima potrebna adekvatnija priprema.

Da bi se sprovela odbrambeno-zaštitna funkcija, potrebno je u njoj uvrstiti one mere koje pružaju mogućnost eleminisanja elemenata koji dovode do narušavanja sigurnosti i opasnosti. Te mere moraju da budu sastavni deo institucije i izvođenja radnog procesa(Stanojević & Milunović, 2020). Primenom propisanih pravila i sprovođenjem mera o zaštiti na radu, zaštiti od požara, zaštiti zivotne sredine i zaštiti zaposlenih uspostavlja se zadovoljavajući stepen sigurnosti. Cilj sprovođenja mera sigurnosti je sprečavanje povreda na radu, profesionalnih bolesti, drugih bolesti u vezi s radom, zaštita radne okoline i zaštita lica i imovine. Odbrambeno-zaštitna funkcija prikazana je prirodnom, društvenom i političkom funkcijom. Prirodna funkcija se ostvaruje spontano i sastavni je deo očuvanja života. Društvena funkcija doprinosi očuvanju društvenih vrednosti i postiže se zajedničkim interesom društva. Politička funkcija čuva političku vlast i postiže se političkim interesom i delovanjem. Odbrambeno-zaštitna funkcija ima dvojaku ulogu. Prva uloga je zaštita, koja preventivno deluje i definiše se kao otpornost prema narušavanju sigurnosti i opasnosti. Druga uloga je odbrana, direktno usmerena na pružanje otpora napadu izvora i nosioca narušavanja sigurnosti. Odbrana predstavlja sposobnost reagiranja na nadvladavanje narušavanju sigurnosti i opasnosti s ciljem uspostavljanja stanja sigurnosti(Elghaish, et al., 2020).

Uslov za sigurno i normalno poslovanje u platnom prometu gotovinom podrazumeva neophodnost posedovanja obučenog ljudstva za sprovođenje funkcije sigurnosti. Da bi se sprovela funkcija sigurnosti i da bi se njome uspešno upravljalo, potrebno je da se itegrišu različite norme u postojećim zakonskim propisima.

Izvori i intenzitet rizika u platnom prometu gotovinom

Zakonom o privatnoj zaštiti regulisane su mere zaštite i odbrane koje samostalno mogu da sprovede finansijske institucije, a njegovim podzakonskim aktima detaljnije je uređena privatna zaštita. Takođe pitanje procene izloženosti riziku, način zaštite lica i imovine, način rada lica koja sprovode zaštitu i nadzor

nad njihovim radom regulisani su Zakonom o privatnoj zaštiti(Cartwright, et al., 2019).

Skup aktivnosti kojima se štite lica i njihova imovina od protivpravnih radnji posredstvom sredstava tehnike predstavljaju vid tehničke zaštite. Tehnička zaštita zahteva procenu izloženosti riziku. Ukoliko se štiti objekat kao deo imovine, zahteva se svrstavanje objekta u kategoriju koja sadrži obavezne mere zaštite(Abdul-Rahman, 2014). Pravno lice, koje ima odobrenje za obavljanje poslova privatne zaštite, ima mogućnost da izgradi dojavni centar sistema tehničke zaštite, u kojem će primati signal za intervenciju. Ovakav vid intervencije po dojavnom signalu vrši ekipa koja se sastoji od najmanje dva lica koja poseduju oružje. Za razliku od tehničke zaštite, telesna zaštita obuhvata lično nadgledanje lica i njihove imovine, koja se štiti, bez potrebe korišćenja sredstava tehnike. Telesna zaštita se obavlja na osnovu radnog naloga poslodavca, koji je popunjen u skladu sa propisima (Zekić, Brajković, 2022). Lica koja sprovode telesnu zaštitu imaju mogućnost da upotrebe silu, ali samo u onom trenutku kada je neophodno da bi se zadovoljio cilj.

Narušavanje sigurnosti u platnom prometu podstaknuto je rizicima tj. aktivnostima koje imaju posledice nastanka nekih nuspojava. Izvori narušavanja sigurnosti mogu biti prirodni, društveni i tehničko-tehnološki. Nosioci narušavanja sigurnosti se mogu klasifikovati na interne i eksterne. Klasifikacija je izvršena prema mestu odakle se uočava narušavanje sigurnosti. Interni nosioci su oni koji nastaju u okviru poslovnog procesa finansijskih institucija. Karakterišu se kao nedefinisani poslovni procesi, nastali usled neorganizovanosti institucije (npr. ne sprovode se mere zaštite radi interesa zaposlenih i interesa uslužnih delatnosti), neodgovornog ponašaja zaposlenih i neispravnosti objekta sredstava i opreme(Ristić et al., 2021). Za razliku od internih nosioca, eksterni nosioci narušavanja sigurnosti nastaju van poslovnog procesa kao što su kriminalne radnje, prirodne sile, tehnološke katastrofe i drugo.

U skladu sa Zakonom o minimalnim merama zaštite sprovodi se procena narušavanja sigurnosti u platnom prometu, koja obuhvata analizu kaznenih radnji protiv slobode i prava čoveka, protiv života čoveka i iz koristoljublja. Za razliku od kaznenih radnji, kriminalne radnje se odnose na krađe, razbojništva, otmice, ucene, iznude i vandalizam.

Vremenski period narušavanja sigurnosti dovodi se u vezu sa izvorima i metodama. Vremenski period narušavanja sigurnosti, koja je prouzrokavana pretnjom izvršenja napada na finansijske institucije traje tokom radnog vremena finansijskih institucija, a naročito u uslovima prenosa i transporta gotovine. U izuzetnim slučajevima, kada je u pitanju pretnja provalom, vremenski period

narušavanja sigurnosti traje van radnog vremena finansijskih institucija(Ciarko & Paluch-Dybek, 2022).

Intezitet narušavanja sigurnosti zavisi od stepena rizika i oscilira u zavisnosti od: izvora narušavanja sigurnosti, predviđanja adekvatnih situacija za napad na finansijsku instituciju, rizika kažnjavanja, broja lica koja se nalaze u objektu i broja osposobljenih lica, lokacije, faze poslovnog procesa, vremena i mera zaštita koje se sprovode. Može biti različitog inteziteta i dovodi do posledica koje zavise i od sprovedenih aktivnosti odbrambeno-zaštitne funkcije.

Sankcije za napade na bankarske institucije, kao i narušavanje sigurnosti slobode i prava čoveka i njegove društvene vrednosti, zagarantovano je Ustavom Republike Srbije i međunarodnim pravom. Upotreba sile, pretnja licu smrću, ili bilo kojim drugim načinom koji ima za posledicu da lice strahuje za svoj život, oduzimanje licu pokretnih stvari i protivpravno prisvajanje istih su osnovna obeležja krivičnih dela pri napadu na finansijske institucije(Jestrović, & Jovanović, 2022). Poslednjih godina u zemljama Evropske unije, ova obeležja dovedena su u vezu sa iznudom, gde se kod izvršenja napada na finansijske institucije, kao što je na primer otmica članova porodice visokih funkcionera institucije ili postavljanje eksplozivne naprave zahteva od finansijske institucije da izdvoji novčana sredstva i da ih dostavi počiniocima krivičnog dela. Na taj način se silom i pretnjom stvara prinuda da lice koje je zaposleno u finansijskoj instituciji, protivno svojoj volji počini krivično delo, što inače ne bi ni uradilo.

Sprovedena istraživanja u poslednjih deset godina, istakla su da se napadi na finansijske institucije uglavnom dešavaju u velikim gradovima, gde je velika gustina naseljenosti, a time i veća mogućnost za skrivanje počinioca krivičnih dela. Obično se napad sprovodi od strane mlađih osoba, preciznije muškaraca, kako zbog svojih fizičkih sposobnosti, tako i zbog nezrelosti i želje za bogastvom. Napadi na finansijske institucije se mogu razlikovati u zavisnosti da li je napad izvršen u finansijskoj instituciji ili pri prenosu i transportu gotovine. Ukoliko je napad izvršen u finansijskoj instituciji, on može biti napad koji je izvršen u bankama, poštama, menjačnicama, poslovnicama finansijskih agencija, kladionicama i kockarnicama. Napadi na finansijske institucije izvršeni pri prenosu gotovine, uglavnom se dešavaju kad se gotovina prenosi u nepropisanim vrećama ili torbama i bez primene propisanih mera zaštite. Napadi izvršeni pri transportu gotovine su povezani sa napadom pri prenosu gotovine, jer se uglavnom napadi sprovode prilikom utovara i istovara gotovine. Pored napada na finansijske institucije koje se bave platnim prometom gotovine, u poslednje vreme je sve više zastupljenija krađa kreditnih ili bankovnih kartica koje služe za podizanje gotovine na bankomatima. Zabeležne su i krađe

gotovine iz bankomata od strane lica koji vrše njihovo punjenje. Krivična dela krađe gotovine u finansijskim institucijama pri prenosu i transportu gotovine, koja su bila medijski pokrivena poslednjih godina, zabeležena su u Holandiji, Brazilu i Sloveniji.

Zaključak

Kako bi se u jednoj finansijskoj instituciji koja se bavi platnim prometom gotovine ostvario uspešan poslovni rezultat neophodno je da se uspostavi adekvatan sistem upravljanja potencijalnim gubitkom i štetom. Neizostavno je da sistem upravljanja rizikom u platnom prometu gotovinom i obezbeđenje sigurnosti budu integrisani u poslovanje finansijske institucije.

Obezbeđenje sigurnosti podrazumeva stanje u kojem se rizici identifikuju, procenjuju, smanjuju ili eleminišu. Neophodno je da se izvrši procena stepena narušavanja sigurnosti, njihovih izvora i vrsta, kritičnih mesta, posledica i primenjenih mera kako bi se obezbedio adekvatan sistem sigurnosti.

Procena stepena narušavanja sigurnosti podrazumeva procenu odnosno sud mogućih opasnosti i pretnji po osobe, gotovinu i poslovne procese. Osnovni cilj procene stepena narušavanja sigurnosti je utvrđivanje izvora i vrste narušavanja sigurnosti, prepoznavanje uzorka i vrste opasnosti, utvrđivanje stepena rizika i njegovo smanjivanje putem primene određenih mera zaštite i jačanja odbrambene moći. Sigurnost svakog poslovnog sistema mora biti uspostavljena na taj način da su njom predviđene moguće štete i rizici koji mogu nastati. Treba voditi računa da se mere za procenu stepena narušavanja sigurnosti i analize rizika utvrde na najobektivniji način. Uspostavljanjem takvog sistema sigurnosti obezbeđuje se efikasnost poslovanja, s jedne strane, dok sistem iziskuje velike troškove, s druge strane.

Literatura

1. Abdul-Rahman, H., Kho, M., Wang, C. (2014). Late payment and nonpayment encountered by contracting firms in a fast-developing economy, J. Prof. Issues Eng. Educ. Pract., 140(2), 04013013, , https://doi.org/10.1061/(ASCE)EI.1943-5541. 0000189.
2. Avakumović, J., Obradović, L., & Božić, G. (2021). Menadžment i organizacija timskog rada u funkciji održivog razvoja. *Održivi razvoj*, *3*(2), 69-80. https://doi.org/10.5937/OdrRaz2102069A
3. Cartwright, E. , Hernandez Castro, H. , Cartwright, A. (2019). To pay or not: game the- oretical models of Ransomware. J. Cybersecur. 5 (1), 1–12 .

4. Ciarko, M., & Paluch-Dybek, A. (2022). Efektivnost unutrašnje kontrole u jedinicama lokalne samouprave. *Društveni horizonti*, *2*(3), 75-84. https://doi.org/10.5937/drushor2203075C
5. Elghaish, F., Abrishami, S., Hosseini, M.R. (2020). Integrated project delivery with blockchain: an automated financial system, Autom. Constr. 114,103182, https://doi.org/10.1016/j.autcon.2020.103182.
6. Griffiths, R., Lord, W., Coggins, J. (2017). Project bank accounts: the second wave of security of payment? J. Financ. Manag. Prop. Constr. 22 (3), 322–338, https://doi. org/10.1108/jfmpc-04-2017-0011.
7. Hull, G. , John, H. , Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Sci. 8 (2), 1–22.
8. Jestrović, V., & Jovanović, V. (2022). Uloga korporativnog rukovođenja u održivom razvoju. *Održivi razvoj*, *4*(1), 43-53. https://doi.org/10.5937/OdrRaz2201043J
9. Kovačević, M., & Gajić, T. (2019). Instrumenti platnog prometa. *Vojno delo*, *71*(6), 371-379. https://doi.org/10.5937/vojdelo1906371K
10. Li, J., Greenwood, D., Kassem, M. (2019). Blockchain in the built environment and construction industry : A systematic review, conceptual models and practical use cases, Autom. Constr. 102, 288–307, https://doi.org/10.1016/j.autcon.2019.02.005.
11. Mansfield-Devine, (2018). The malware arms race. Comput. Fraud Secur. 2018 (2), 15–20 .
12. Mihajlović, M., Nikolić, S., & Tasić, S. (2020). Održivost ekonomskog modela savremene privrede. *Održivi razvoj*, *2*(2), 7-13. https://doi.org/10.5937/OdrRaz2002007M
13. Mirković, P., Prokopović, I., & Petrović, I. (2022). Pravni odnosi između subjekata u akreditivu sa osvrtom na ulogu i značaj banaka u strukturi finansijskog sektora u Srbiji. *Pravo - teorija i praksa*, *39*(2), 65-79. https://doi.org/10.5937/ptp2202065M
14. Papp, J. , Smith, B. , Wareham, J. , Wu, Y. (2019). Fear of retaliation and citizen willing- ness to cooperate with police. Polic. Soc. 29 (6), 623–639 .
15. Raskin, M. (2017). The law and legality of smart contracts, Georg. Law Technol. Rev. 305, 305–341, https://doi.org/10.2139/ssrn.2842258.
16. Ristić, K., Miljković, Lj. & Milunović, M. (2021). Investment in the banking sector as a basis for money laundering. Akcionarstvo, 27(1), 55-70
17. Stanojević, S. & Milunović, M. (2020). Okončanje postupka državne revizije. Akcionarstvo, 26(1), 35-48
18. Vićić, M. (2016). Elektronski novac u platnom prometu Republike Srbije. *Pravo i privreda*, *54*(4-6), 386-401.

19. Zhao, J.Y. , Kessler, E.G. , Yu, J. (2018). Impact of trauma hospital ransomware attack on surgical residency training. J. Surg. Res. 232, 389–397 .
20. Zekić M., Brajković B., (2022). Uloga finansijskog menadžmenta u preduzeću, Finansijski savetnik, Vol. 27, No. 1, str. 7-24
21. Živković, A. (2019). Kvalitet upravljanja operativnim rizicima u finansijskim institucijama. Akcionarstvo, 25(1), 5-32

MANAGEMENT OF ORGANIZATIONAL PAYMENT SECURITY

Ilija Životić[20], Kristijan Ristić[21], Snežana Krstić[22], Srboljub Nikolić[23], Bruno Đuran[24]

Review paper

Abstract

Risk management in payment transactions includes identifying, measuring and managing risks. That is why it is necessary to establish its effective function in payment transactions. In the last ten years, the development of risk management in countries in transition is evident. Bearing these facts in mind, the aim of this research study is to analyze the risks in payment transactions, with special reference to the analysis of cash management. The results of this overview study show that each bank operates with a smaller or larger number of risks, positioning itself between two extremes: absolute risk acceptance and absolute risk non-acceptance. It is necessary that the level of risk acceptance be proportional to the bank's ability to cover the resulting losses, as well as to achieve an acceptable rate of return. Achieving higher returns is possible if the bank establishes effective identification, measurement and management of business risks. The carriers of security breaches arise from the types of sources from which forms of security breaches will later arise. In order to carry out the defense and protection function, it is necessary to include those measures that provide the possibility of eliminating elements that lead to the violation of security and danger. Those measures must be an integral part of the institution and the execution of the work process. The condition for safe and normal operations in cash payment transactions implies the necessity of having trained personnel for the implementation of the security function. In order to implement

[20] PhD Ilija Životić, assistant professor, Union University "Nikola Tesla", Faculty of Engineering Management, Bulevar vojvode Mišića 43, Belgrade, R. Serbia, email: ilijazivotic@gmail.com

[21] PhD Kristijan Ristić, associate professor, University of MB, Faculty of Business Law, Knez Mihajlova 33, Belgrade, Serbia, E-mail: kristijanristic.fpim@yahoo.com

[22] Ph.D. Snežana Krstić, associate professor, University of Defense, Military Academy, Veljka Lukića Kurjaka 33, Belgrade, Serbia, email: snezanakrstic17@gmail.com

[23] PhD Srboljub Nikolić, assistant professor, University of Defense, Military Academy, Veljka Lukića Kurjaka 33, Belgrade, Serbia, email: srboljub.nikolic@yahoo.com

[24] PhD Bruno Đuran, associate professor, University of Business Studies, Jovana Dučića 23a, Banaja Luka, Bosnia and Herzegovina, email: ups@univerzitetps.com

the security function and manage it successfully, it is necessary to integrate various norms in the existing legal regulations.

Keywords: *risk management, payment transactions, cash and security.*

JEL: *E42, E49.*

Introduction

Due to the globalization of the population, the economy and politics, the growth of foreign investments and cross-border transfers, the integration of stock markets into a single system and the growth of their placements, the abolition of redundant financial processes through the reduction of the influence of the state on financial activities, the establishment of modern technology, the fluctuation of exchange rates and prices of strategic products, comes to increased risk in business for all participants in the financial market. Risk is present in all institutions operating on the market. We define risk as the percentage of probability of occurrence of negative events, which have negative consequences on business. Its main characteristic is constancy. It exists in all institutions to a greater or lesser extent, it is not possible to eliminate it, but it is possible to reduce it.

Traditional financial institutions are exposed to liquidity risk, credit risk, interest rate risk, foreign exchange risk, concentration risk, operational risk and strategic risk. Central banks are also exposed to the same risks, but with a higher degree of protection because their portfolio consists of high security placements. Unlike traditional financial institutions, central banks are non-profit institutions, established with the aim of ensuring the safety of public funds.

Analyzing the relevant literature, in the last ten years, the tendency of central bank risk management, their identification and the development of instruments for risk assessment, i.e. their measurement, is present.

The goal of the work

Given that in recent years there has been a growing trend of attacks on institutions dealing with payment transactions, primarily cash, the aim of this research study is to look at the risks in payment transactions, with special reference to the analysis of cash management.

Method of work

A systematic review of the literature was performed through a search in the databases PubMed, Google Scholar Advanced Search and the Consortium of Serbian Libraries for Unified Procurement - KoBSON. Papers were searched

according to the following key words and phrases: risk management in financial institutions, payment traffic and risk, cash and security, sources of risk in payment traffic, types and intensity of risk in payment traffic. Studies in English and Serbian were analyzed.

Risk management in payment transactions

In order to protect the bank from all risks, including credit risk, the bank's capitalization is imposed as its permanent orientation along with portfolio diversification. A system of reporting on the percentage of risk representation has been implemented in all banks. This reporting can be regular or periodic. Customer relationship management (CRM) (Mansfield-Devine, 2018), i.e. participation in the decision-making process of the bank's credit committee, determines the potential danger of risk in each individual client or in a group of clients (Kovačević & Gajić, 2019). CRM determines the danger of the risk in accordance with the legal regulations and prepares a report on a monthly level, which is submitted to the members of the bank's management. On a monthly basis, the bank's management is informed about the level of risk representation through a report on the quantity of the bank's portfolio, which is compiled in parallel with the type and legal percentage of restrictions. The aggregated gross balance of the bank, the aggregated table of exposure and the analytical cards of the clients are the basis for the preparation of the report on the quantity of the bank's portfolio. Also, the bank's management provides guidelines for eliminating specific excesses, management and control of existing and potential risks of the bank (Hull et al., 2019).

According to the ABRS methodology, banks monitor and analyze the degree of exposure to credit risk, which includes claims for principal, interest, fees, liabilities to an individual client or to a group of clients. The degree of exposure to credit risk in the form of issued guarantees may not exceed 100% of the amount of the bank's core capital. The bank's exposure to credit risk to an individual client or to a group of clients must not exceed 40% of the amount of the bank's core capital. The basic capital of the bank, i.e. the maximum exposure to credit risk is structured according to the following restrictions (Živković, 2019):

- Up to 5% of the amount of the bank's core capital where the credit risk is not covered by collateral;
- From 5% to 25% of the amount of the bank's core capital where the credit risk is covered by collateral;
- Over 25% of the amount of the bank's core capital where the credit risk is covered by a high-quality marketable pledge whose value is higher than the value of the collateral.

- Up to 20% of the amount of the bank's core capital, if the credit risk is in the form of issued guarantees, except guarantees for good performance.

Letters of credit and guarantees expressed in monetary values are not included in the total exposure to credit risk up to the amount of their coverage. If the bank's total exposure to credit risk to an individual client or to a group of clients is higher than 15% of the amount of the bank's core capital, it is considered that the bank's exposure to credit risk is high. The sum of all the bank's large exposures to credit risk must not exceed 300% of the bank's core capital (Zhao et al., 2018).

In the modern world, under the influence of modernizing technology and electronic means of communication, bank operations are at greater risk. Reduced ability of the bank to operate efficiently and to strengthen its business and financial position, instability of earnings and reduction of capital represent the basic characteristics of a bank that is exposed to risk. In order for a bank to maintain its solvency, it must have capital, which will cover potential losses caused by the volatility of earnings. Also, it is necessary for the bank to manage its risks, especially the larger risks to which it is exposed.

We distinguish between two types of risks that can affect the volatility of earnings: financial and non-financial risks. Financial risks are directly related to the role of the financial principal and intermediary, while non-financial risks arise as a result of inadequate procedures, due to external and human factors. Financial risks include credit, market and ALM (asset-liability management). Operational, business, reputational, strategic, legal and other risks are considered non-financial risks.

As a form of security and guarantee against risk exposure, it is necessary for banks to set aside special capital, which would serve as cover for potential losses caused by financial and non-financial risks. In addition to risk identification, their monitoring and control, it is necessary for banks to establish a risk exposure quantification system, i.e. a measurement system (Li et al., 2019). By applying the system of identification, monitoring, control and measurement of risks by the bank, it can be said that an effective risk management system has been established. Based on the Basel Committee on Banking Supervision and international agreements, banks are developing sophisticated models for quantifying risk exposure. Depending on the chosen model, a distinction is made between expected and unexpected losses. Expected losses are those for which there is a degree of probability that they will occur and they are known to the bank. They are assessed and reserves are set aside to cover them. Unlike expected losses, unexpected losses cannot be predicted. A system of risk measurement is applied to them, through precise risk quantification and

allocation of capital by the bank for the purpose of coverage (Griffiths et al., 2017).

In order for the bank to always be solvent and have the ability to protect itself from possible losses in a certain period, it must take into account the size of the bank's economic capital. Given that economic capital is a large expense for the bank, it is necessary that its size be adjusted to the bank's risk profile (Mihajlović et al., 2020). It represents a measure of the bank's overall risk profile, as well as a measure of changes in its risks over time. It is used when calculating the percentage of the bank's earnings in relation to the degree of exposure to risk. It serves to compare different types of risks.

Any uncertain situation in banking business, i.e. the existence of the probability of losses due to the performance of certain banking activities represents a risk. Each bank operates with a smaller or larger number of risks, positioning itself between two extremes: absolute acceptance of risk and absolute non-acceptance of risk (Vićić, 2016). It is necessary that the level of risk acceptance be proportional to the bank's ability to cover the resulting losses, as well as to achieve an acceptable rate of return. Achieving higher returns is possible if the bank establishes effective identification, measurement and management of business risks.

Security of cash payments

In the case of cash payment transactions, cases of violation of the security of payment transactions are divided into subjects and objects of security violation. Workers and clients of banking institutions are the subjects of security breaches, while property, i.e. money and business processes are objects of security violations in cash payment transactions.

According to the nature of the occurrence, the sources of security violations in cash payment transactions can be natural, social and technical-technological. Carriers of security breaches arise from a variety of sources. Natural sources include natural forces and phenomena, while social sources include individuals, criminal or terrorist organizations, and insufficient organization of society. Among the technical-technological sources, we single out the disorganized operation of the institution and/or society, negligence and carelessness (Mirković et al., 2022).

Shapes security breaches arise from sources of security breaches. Showers, thunderstorms, earthquakes and floods are forms of disruption of security characteristic of natural sources. They cannot be predicted and arise as a result of natural forces (Papp et al., 2019). Terrorist attacks, burglaries, thefts and protests are forms of breach of security characteristic of social sources. In order

to prevent the occurrence of such phenomena, there is a possibility of determining their frequency by collecting and analyzing information, defining protection and defense measures. The failure of information systems, breakdown or failure of devices are forms of breach of security characteristic of technical-technological sources. Prevention of such negative consequences is achieved by regular maintenance and provision of replacement parts.

Sources of security breaches are also used for the selection of means for the realization of forms of security breach. Natural resources are used as failsafes for natural phenomena that are known to occur in the future, but do not know when they will occur. Cash payment transactions are most affected by social sources of security violations, i.e. attacks on banks, burglaries and thefts (Raskin, 2017). Resources security breaches that can be used from social sources are guns, knives, clubs and more. Means of breaching security can also be from technical-technological sources such as fire, electric current and others.

Also, the methods of breaching the security of cash payment transactions differ in relation to the sources of breach of security. Earthquakes and floods are considered to be methods of disrupting security arising from natural sources. Burglary, assault and theft are considered methods of breaching security originating from social sources. Technical-technological methods of breaching security arose from technical-technological sources.

The time period of the breach is related to the sources and methods of security breaches. The time period of security breaches from natural sources is more permanent due to unpredictability. The time period of the breach of security from social sources is associated with the source of the breach of security. The time period of breaching security by attacking financial institutions lasts during the time employees stay in the facilities of the financial institutions themselves, then during the transfer and transport of money from one location to another.

The intensity of the violation also comes from the source of security violations. It also depends on the stage of the cash management business process. Depending on the source, the intensity of the security breach can be strong or weak.

The consequences of violating the security of cash payment transactions depend on the way the institution's defense and protection functions are applied. They can be classified according to the subject that has the effect of violating security (Avakumović, et al., 2021):

- person (death, serious or minor physical injury, mental breakdown);
- property (loss and damage to money);

- business process (permanent or temporary business interruption).

Analyzing attacks on financial institutions, looking at the period of the past fifty years, a constant growth is evident. However, if we look at the attack on financial institutions during the transport of cash, it can be said that there has been a decline. This is justified by the fact that when transporting cash, the protection system is constantly being implemented and complicated, which means that attackers need more adequate preparation.

In order to implement the defense and protection function, it is necessary to include those measures that provide the possibility of eliminating elements that lead to the violation of security and danger. Those measures must be an integral part of the institution and the execution of the work process (Stanojević & Milunović, 2020). By application prescribed rules and the implementation of measures on occupational safety, fire protection, environmental protection and employee protection establish a satisfactory level of safety. The goal of implementing safety measures is to prevent injuries at work, occupational diseases, other work-related diseases, protection of the working environment and protection of persons and property. The defense-protective function is shown as a natural, social and political function. The natural function is realized spontaneously and is an integral part of preserving life. The social function contributes to the preservation of social values and is achieved by the common interest of society. Political function preserves political power and is achieved through political interest and action. The defensive-protective function has a dual role. The first role is protection, which acts preventively and is defined as resistance to the violation of security and danger. The second role is defense, directly aimed at resisting the attack of the source and carrier of the security breach. Defense represents the ability to react to overcoming security violations and threats with the aim of establishing a state of security (Elghaish, et al., 2020).

Condition for safe and normal business operations in cash payments implies the necessity of having trained personnel to implement the security function. In order to implement the security function and manage it successfully, it is necessary to integrate various norms in the existing legal regulations.

Sources and intensity of risk in cash payment transactions

The law on private protection regulates protection and defense measures that financial institutions can implement independently, and its by-laws regulate private protection in more detail. Also, the issue of risk exposure assessment, the way to protect people and property, the way of work of persons who carry

out protection and the supervision of their work are regulated by the Law on Private Protection (Cartwright, et al., 2019).

A set of activities that protect persons and their property from illegal actions by means of technical means is a form of technical protection. Technical protection requires risk exposure assessment. If the object is protected as part of the property, it is required to classify the object into a category that contains mandatory protection measures (Abdul-Rahman, 2014). A legal entity, which is authorized to perform private security services, has the possibility to build a notification center of the technical protection system, where it will receive a signal for intervention. This type of intervention following a warning signal is carried out by a team consisting of at least two persons who possess weapons. Unlike technical protection, physical protection includes personal monitoring of persons and their property, which is being protected, without the need to use technical means. Physical protection is performed on the basis of the employer's work order, which is completed in accordance with the regulations (Zekić, Brajković, 2022). Persons who carry out physical protection have the possibility to use force, but only at that moment when it is necessary to satisfy the goal.

Violation of security in payment transactions is encouraged by risks, i.e. activities that have the consequences of some side effects. Sources of security violations can be natural, social and technical-technological. The carriers of security breaches can be classified into internal and external. The classification was made according to the place from where the violation of security is observed. Internal carriers are those that arise within the business process of financial institutions. They are characterized as undefined business processes, caused by the disorganization of the institution (e.g. protection measures are not implemented for the interests of employees and the interests of service activities), irresponsible behavior of employees and malfunctioning of facilities and equipment (Ristić et al., 2021). Unlike internal carriers, external carriers of security breaches occur outside the business process, such as criminal acts, natural forces, technological disasters, and others.

In accordance with the Law on Minimum Protection Measures, an assessment of the violation of security in payment transactions is carried out, which includes the analysis of criminal actions against human freedom and rights, against human life and for self-interest. Unlike criminal acts, criminal acts refer to theft, robbery, kidnapping, blackmail, extortion and vandalism.

The time period of the security breach is related to the sources and methods. The time period of breach of security, which is caused by the threat of an attack on financial institutions, lasts during the working hours of financial institutions, especially in the conditions of transfer and transport of cash. In exceptional

cases, when it comes to the threat of a break-in, the time period of the security breach lasts outside the working hours of financial institutions (Ciarko & Paluch-Dybek, 2022).

The intensity of the security breach depends on the degree of risk and fluctuates depending on: the source of the security breach, the prediction of adequate situations for an attack on the financial institution, the risk of punishment, the number of persons in the facility and the number of trained persons, location, stage of the business process, time and measures protection that are implemented. It can be of different intensity and lead to consequences that also depend on the implemented activities of the defense-protective function.

Sanctions for attacks on banking institutions, as well as the violation of the security of freedom and rights of man and his social values, are guaranteed by the Constitution of the Republic of Serbia and international law. The use of force, the threat of death to a person, or any other way that causes a person to fear for his life, confiscation of movable property from a person and illegal appropriation of the same are the basic characteristics of criminal acts in the attack on financial institutions (Jestrović, & Jovanović, 2022). In recent years, in the countries of the European Union, these characteristics have been linked to extortion, where when carrying out attacks on financial institutions, such as kidnapping family members of high officials of the institution or planting an explosive device, the financial institution is required to allocate funds and deliver them to the perpetrators of the crime. In this way, coercion is created by force and threat, so that a person who is employed in a financial institution, against his will, commits a criminal act, which otherwise he would not have done.

Researches conducted in the last ten years have pointed out that attacks on financial institutions mostly take place in big cities, where there is a high population density, and thus a greater possibility for the perpetrators of criminal acts to hide. Usually, the attack is carried out by younger persons, more specifically men, both because of their physical abilities, and because of their immaturity and desire for wealth. Attacks on financial institutions can differ depending on whether the attack is carried out at a financial institution or during the transfer and transport of cash. If the attack was carried out in a financial institution, it can be an attack carried out in banks, post offices, exchange offices, branches of financial agencies, betting shops and casinos. Attacks on financial institutions carried out during the transfer of cash, mostly occur when the cash is transferred in non-prescribed sacks or bags and without the application of prescribed protection measures. Attacks carried out during the transport of cash are related to the attack during the transfer of cash, because

mainly the attacks are carried out during the loading and unloading of cash. In addition to attacks on financial institutions that deal with cash payments, the theft of credit or bank cards used to withdraw cash from ATMs has become more common recently. Thefts of cash from ATMs by the persons filling them have also been recorded. Crimes of theft of cash in financial institutions during the transfer and transport of cash, which have been covered by the media in recent years, have been recorded in the Netherlands, Brazil and Slovenia.

Conclusion

In order to achieve a successful business result in a financial institution dealing with cash payments, it is necessary to establish an adequate management system for potential loss and damage. It is essential that the risk management system in cash payment transactions and security assurance be integrated into the operations of the financial institution.

Ensuring security means the state in which risks are identified, assessed, reduced or eliminated. It is necessary to assess the degree of security breaches, their sources and types, critical places, consequences and applied measures in order to ensure an adequate security system.

The assessment of the degree of security breach implies an assessment, i.e. a judgment of possible dangers and threats to persons, cash and business processes. The main goal of assessing the degree of security breach is to determine the source and type of security breach, identify the pattern and type of danger, determine the degree of risk and reduce it through the application of certain protection measures and strengthening of defense power. The security of every business system must be established in such a way that it foresees possible damages and risks that may arise. Care should be taken to determine the measures for assessing the degree of security breach and risk analysis in the most objective way. By establishing such a security system, business efficiency is ensured, on the one hand, while the system requires large costs, on the other hand.

Literature

1. Abdul-Rahman, H., Kho, M., Wang, C. (2014). Late payment and nonpayment encountered by contracting firms in a fast-developing economy, J. Prof. Issues Eng. Educ. Pract., 140(2), 04013013, https://doi.org/10.1061/(ASCE)EI.1943-5541. 0000189.
2. Avakumović, J., Obradović, L., & Božić, G. (2021). Management and organization of teamwork in the function of sustainable development.

Sustainable development, 3 (2), 69-80. https://doi.org/10.5937/OdrRaz2102069A
3. Cartwright, E., Hernandez Castro, H., Cartwright, A. (2019). To pay or not: game the theoretical models of Ransomware. J. Cybersecur. 5 (1), 1–12.
4. Ciarko, M., & Paluch-Dybek, A. (2022). Effectiveness of internal control in local self-government units. *Social horizons, 2* (3), 75-84. https://doi.org/10.5937/drushor2203075C
5. Elghaish, F., Abrishami, S., Hosseini, MR (2020). Integrated project delivery with blockchain: an automated financial system, Autom. Construction 114,103182, https://doi.org/10.1016/j.autcon.2020.103182 .
6. Griffiths, R., Lord, W., Coggins, J. (2017). Project bank accounts: the second wave of security of payment? J. Financ. Manag. Prop. Construction 22 (3), 322 – 338, https://doi. org/10.1108/jfmpc-04-2017-0011.
7. Hull, G., John, H., Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Sci. 8 (2), 1–22.
8. Jestrović, V., & Jovanović, V. (2022). The role of corporate leadership in sustainable development. *Sustainable development, 4* (1), 43-53. https://doi.org/10.5937/OdrRaz2201043J
9. Kovačević, M., & Gajić, T. (2019). Instruments salary traffic. *Military work, 71* (6), 371-379. https://doi.org/10.5937/vojdelo1906371K
10. Lee, J., Greenwood, D., Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases, Autom. Construction 102, 288 – 307, https://doi.org/10.1016/j.autcon.2019.02.005 .
11. Mansfield-Devine, (2018). The malware arms race. Comput. Fraud Secur. 2018 (2), 15–20.
12. Mihajlović, M., Nikolić, S., & Tasić, S. (2020). Sustainability of the economic model of the modern economy. *Sustainable development, 2* (2), 7-13. https://doi.org/10.5937/OdrRaz2002007M
13. Mirković, P., Prokopović, and., & Petrović, and. (2022). Legal relations between subjects in letter of credit with in retrospect on the role and meaning banks in structure financial sector in to Serbia. *Law - theory and practice, 39* (2), 65-79. https://doi.org/10.5937/ptp2202065M
14. Papp, J., Smith, B., Wareham, J., Wu, Y. (2019). Fear of retaliation and citizen willingness to cooperate with police. Police. Soc. 29 (6), 623–639.
15. Raskin, M. (2017). The law and legality of smart contracts, Georg. Law Technol. Rev. 305, 305 – 341, https://doi.org/10.2139/ssrn.2842258 .
16. Ristić, K., Miljković, Lj. & Milunović, M. (2021). Investment in the banking sector as a basis for money laundering. Aksionarstvo, 27(1), 55-70

17. Stanojević, S. & Milunović, M. (2020). Completion of the state audit procedure. Aksionarstvo, 26(1), 35-48
18. Vićić, M. (2016). Electronic money in the payment system of the Republic of Serbia. *Right and economy, 54* (4-6), 386-401.
19. Zhao, JY, Kessler, EG, Yu, J. (2018). Impact of trauma hospital ransomware attack on surgical residency training. J. Surg. Res. 232, 389–397.
20. Zekić M., Brajković B., (2022). Uloga finansijskog menadžmenta u preduzeću, Finansijski savetnik, Vol. 27, No. 1, str. 7-24
21. Živković, A. (2019). Quality of operational risk management in financial institutions. Aksionarstvo, 25(1), 5-32

Datum prijema (Date received): 12.08.2022.
Datum prihvatanja (Date accepted): 24.10.2022.