UNIVERZITET CRNE GORE
ELEKTROTEHNIČKI FAKULTET PODGORICA

Ana Ivanović

INFORMACIONE TEHOLOGIJE U SLUŽBI IDENTIFIKACIJE, PROCJENE I KONTROLE RIZIKA PO BEZBJEDNOST INFORMACIJA SA PRIMJEROM IMPLEMENTACIJE

MASTER RAD

Podgorica, 2019. godine

UNIVERZITET CRNE GORE
ELEKTROTEHNIČKI FAKULTET PODGORICA

Ana Ivanović

INFORMACIONE TEHOLOGIJE U SLUŽBI IDENTIFIKACIJE, PROCJENE I KONTROLE RIZIKA PO BEZBJEDNOST INFORMACIJA SA PRIMJEROM IMPLEMENTACIJE

MASTER RAD

Podgorica, 2019. godine

PODACI I INFORMACIJE O MAGISTRANDU

Ime i prezime	**Ana Ivanović**
Datum i mjesto rođenja	**16.08.1977. godine, Podgorica**
Naziv završenog osnovnog studijskog programa i godina završetka studija	**Elektronika, Telekomunikacije i Računari, 2004**

INFORMACIJE O MAGISTARSKOM RADU

Naziv postdiplomskog studija	**Elektronika, Telekomunikacije i Računari**
Naslov rada	**Informacione tehnologije u službi identifikacije, procjene i kontrole rizika po bezbjednost informacija sa primjerom implementacije**
Fakultet/Akademija na kojem je rad odbranjen	**Elektrotehnički fakultet, Podgorica**

UDK, OCJENA I ODBRANA MAGISTARSKOG RADA

Datum prijave magistarskog rada	**04.06.2018.**
Datum sjednice vijeća na kojoj je prihvaćena tema	**26.10.2018**.
Komisija za ocjenu teme i podobnosti magistranda	**Prof. dr Budimir Lutovac** **Prof. dr Miloš Daković** **Prof. dr Irena Orović**
Mentor	**Prof. dr Miloš Daković**
Komisija za ocjenu rada	**Prof. dr Budimir Lutovac** **Prof. dr Miloš Daković** **Prof. dr Irena Orović**
Komisija za odbranu rada	**Prof. dr Budimir Lutovac** **Prof. dr Miloš Daković** **Prof. dr Irena Orović**
Datum odbrane	**31.01.2020**.
Datum promocije	__.__.____.

Predgovor

Sa stalnim napretkom informacionih tehnologija, javila se tendencija da u svim segmentima poslovanja što je moguće više poslovnih procesa dobije adekvatnu informatičku podršku odnosno da bude pokriveno odgovarajućima aplikativnim softverom. Iz tog razloga, uspješnost funkcionisanje poslovne organizacije je značajno zavisna od efikasnosti funkcionisanja informacionog sistema kojim su automatizovani poslovni procesi u toj organizaciji. Posljedično, informacioni sistemi su postali meta čestih napada. Skoro svakodnevno, oni su izložni ozbiljnim pretnjama koje, korišćenjem poznatih i nepoznatih ranjivosti, mogu ugroziti organizacione operacije i imovinu, kao i pojedince. Krajnji cilj ovih upada je dolaženje do informacija iz pogođenog sistema. Posmatrano sa tog aspekta, informacija je svojevrsna poslovna imovina čiji gubitak može dovesti do značajne i dugoročne štete po poslovanje organizacije. Zbog toga je očuvanje bezbjednosti informacije suštinski važno za svaku organizaciju. S obzirom da postoje prijetnje po bezbjednost informacija koje je nemoguće izbjeći, očuvanje bezbjednosti informacije svodi se na to da se rizik drži pod kontrolom odnosno na prihvatljivom nivou. Proučavanje ove teme motivisano je težnjom da se koncipira model za izradu informacionog sistema koji bi omogućio što efikasnije evidentiranje i obradu podataka neophodnih za upravljanje rizikom.

Izvod rada

U tezi je prikazan razvoj informacionog sistema za upravljanje rizikom po bezbjednost informacija, kroz sve faze, od faze analize i kreiranja specifikacije, pa sve do faze uvođenja u upotrebu. Razvijenim sistemom je sprovedena automatizacija poslovnih procesa koji čine upravljanje rizikom po bezbjednost informacija u Centralnoj banci Crne Gore.

Najprije je kreiran model informacionog sistema koji omogućava da se proces vrednovanja informacijskih resursa, kao i proces procjene i klasifikacije rizika sprovodi automatski u skladu sa usvojenim standardima kroz razvrstavanje, klasifikovanje i kategorizaciju informacijskih resursa i grupisanje prijetnji i ranjivosti koje se mogu javiti za određenu kategoriju resursa u realnom poslovnom sistemu. Koncepcija modela je takva da je njegov ključni dio, koji se odnosi na podatke o rizicima po identifikovane informacijske resurse, povezan sa šifarnicima u kojima su smješteni podaci vezani za regulativu upravljanja rizicima i šifarnicima sa popisom identifikovanih resursa, kategorija resursa i za njih definisanih prijetnji i ranjivosti.

Modeliranjem registra rizika u obliku dokumenta koji se oslanja na niz šifarnika, postignuta je primjenjivost modela za razne regulative odnosno opštost modela. Pošto u Centralnoj banci Crne Gore postoji Glavni bankarski sistem, koji automatizuje ključne poslovne procesa, razvijeni informacioni sistem za upravljanje rizicima, integrisan je sa postojećim aplikativnim sistemom. Sprovedena integracija je nametnula upotrebu postojećih šifarnika Glavnog bankarskog sistema kao “izvora” identifikovanih informacijskih resursa.

Zahvaljujući upotrebi izgrađenog informacionog sistema, sve samostalne organizacione jedinice Centralne banke Crne Gore formiraju sopstvene registre rizika po bezbjednost informacija, u skladu sa jedinstvenom metodologijom i koristeći podatke iz jedinstvenih šifarnika. Ne manje važna je činjenica da se na osnovu podataka evidentiranih u registrima, dobijaju svi neophodni izvještaji za analizu rizika. Na taj način je postignuto efikasno i uređeno upravljanje rizicima po bezbjednost informacija za Centralnu banku kao cjelinu.

Ključne riječi: bezbjednost informacija, informacijski resursi, informacioni sistem za upravljanje rizikom, automatizacija, registar rizika.

Abstract

This thesis describes the development of an information security risk management information system, through all phases, from the analysis and specification phases to the implementation phase. The developed system has implemented the automation of business processes that make managing information security risk in the Central Bank of Montenegro.

First, an information system model was created that allows the information resource evaluation process as well as the risk assessment and classification process to be performed automatically in accordance with the adopted standards by sorting, classifying and categorizing information resources and grouping threats and vulnerabilities that may occur for a particular resource category in a real business system. The conception of the model is such that its key part, related to the risk information on the identified information resources, is related to the codebooks containing the data related to the risk management regulation and the codebooks with a list of identified resources, resource categories and threats defined for them and vulnerabilities.

The applicability of the model to various regulations and the generality of the model was achieved by modeling the risk register in the form of a document that relies on a series of codebooks. Since there is a Core Banking System in the Central Bank of Montenegro, which automates key business processes, the developed risk management information system is integrated with the existing application system. The implementation of the integration imposed the use of existing codes of the Core Banking System as a "source" of identified information resources.

Thanks to the use of the developed information system, all independent organizational units of the Central Bank of Montenegro form their own risk registers for information security, in accordance with a unique methodology and using data from unique codes. Equally important is the fact that, all the necessary reports for risk analysis are obtained based on the data recorded in the registers. In this way, effective and orderly information security risk management was achieved for the Central Bank as a whole.

Key words: information security, information resources, risk management information system, automation, risk register.

Indeks pojmova i slika

Indeks pojmova

IT – Information Technology
ICT – Information and communications technology
CIA – C – Confidentiality, I – Integrity, A - Availability
EMP – Electromagnetic pulse
DRP – Dissaster Recovery Plan
IRP – Incident response plan
API – Application programming interface
AES – Advanced Encription Standard
ISMS – Information Security Management System
ISO/IEC – Information Security Management/International Electrotechnical Commission
GDPR – General Data Protection Regulation
ER – Entity Relationship
SSA – Structured Systems Analysis
SUBP – Sistem za upravljanje bazom podataka
OJ – Organizaciona jedinica
ANN – Artifical Neural Networks
LSI – Large Scale Integration
VLSI – Very Large Scale Integration
TLU – Threshold Logic Unit

Indeks slika

Sadržaj

1. Uvod

Percepcija bilo kojeg događaja ili situacije, odluke koje se donosimo, kao i odnos prema određenom pitanju, pored ličnih principa i znanja koja posjedujemo, u velikoj mjeri zavise od informacija koje su nam u tom trenutku dostupne. Nedostatak informacija o nekom problemu, može dovesti do nemogućnosti potpunog razumijevanja tog problema izazivajući izvođenje pogrešnih zaključaka o uzrocima njegovog nastanka, a time i umanjujući mogućnosti uspješnog rješavanja. Samo ako raspoložemo preciznim informacijama o određenom problemu, taj problem možemo uspješno sagledati i analizirati. Dakle, posjedovanje preciznih i potpunih informacija utiče na sve sfere života tako što u velikoj mjeri utiče na našu sposobnost da odgovorimo raznim izazovima.

Uticaj dostupnosti preciznih informacija posebno je uočljiv u poslovnom svijetu gdje odluke često moraju biti donošene jako brzo, a mogu imati dugoročne posljedice. Nagli razvoj informacionih tehnologija, a to podrazumijeva tehnologije koje omogućavaju prikupljanje, obrađivanje, zaštitu i čuvanje informacija, omogućio je ogroman protok informacija u svim smjerovima. Naročito, razvoj interneta je doveo do toga da se gotovo može reći da samo neko ko nije dovoljno zainteresovan ne može doći do neke informacije. Koliko je ova pojava pozitivna u smislu olakšane razmjene informacija, toliko je negativna jer znači da sa podjednakom vjerovatnoćom informacija može biti dostupna onome kome je namijenjena kao i nekome ko ima namjeru da tu informaciju zloupotrijebi. Formiranje informacionog društva, kao i razvoj i ekspanzija informaciono komunikacione tehnologije omogućili su ispunjenje dugogodišnjeg cilja da informacija bude što brže dostupna. U skladu sa novonastalim problemom potencijalne zloupotrebe informacije, iskristalisao se novi cilj - spriječiti neovlašćeno raspologanje informacijama. U osnovi sprečavanja zloupotrebe informacija diferenciraju se dva oprečna, a podjednako važna zadatka - istu informaciju učiniti dostupnom korisniku kome je namijenjena, a nedostupnom svim ostalim korisnicima.

Razvoj informaciono-komunikacionih tehnologija doveo je do toga da, bez obzira na to što se na svim aplikativnim i infrastrukturnim nivoima informacionog sistema konstantno unapređuju softverske i hardverske kontrole, postoji stalna opasnost od zloupotrebe informacija. U tom smislu, informacija je

poslovna imovina koju karakterišu tri osobine: povjerljivost, integritet i dostupnost. Narušavanje bilo koje od njih stvara veliku štetu poslovnoj organizaciji. Očuvanje ovih osobina informacije zapravo znači očuvanje bezbjednosti informacije. Bezbjednost informacija je zahtjev koji mora biti u što je moguće većoj mjeri zadovoljen da poslovanje bilo koje organizacije ne bi bilo ozbiljnije ugroženo.

Naime, bezbjednost informacija je proces smanjenja rizika ili vjerovatnoće nastajanja štete. Proces smanjenja rizika obuhvata identifikaciju prijetnji i ranjivosti koje se mogu javiti za određenu kategoriju informacijskih resursa, zatim ocjenu i klasifikaciju rizika i na kraju, izradu plana tretmana rizika, kroz odabir opcija za modifikaciju rizika. Informacijski resursi su sva ona sredstva koja sadrže informaciju, prenose informaciju, kreiraju informaciju, koriste informaciju ili su informacija sama za sebe. Bezbjednost informacija je zaštita informacija od velikog broja prijetnji radi osiguranja kontinuiteta poslovanja, smanjenja poslovnog rizika i povećanja prihoda od investicija i poslovnih prilika. Bezbjednost informacija postiže se primjenom odgovarajućeg skupa kontrola, uključujući politike, procese, procedure, organizacijske strukture i softverske i hardverske funkcije.

Značajna učestanost pojavljivanja događaja koji predstavljaju prijetnju bezbjednosti informacija uslovila je da ova tema bude veoma aktuelna. Zbog toga sam razvila informacioni sistem koji predstavlja adekvatnu informatičku podršku poslovnim procesima koji čine osnovu očuvanja bezbjednosti informacija. Detaljan opis razvoja tog informacionog sistema, od faze snimanja postojećeg stanja, preko kreiranja modela, pa do uvođenja u upotrebu je predmet ove teze. U tezi će postojati dvije cjeline – teorijski dio i dio koji se odnosi na razvoj informacionog sistema.

U teorijskom dijelu teze (Glava 2, 3) će biti data teorijska podloga za uvođenje pojma bezbjednosti informacija, kao i detaljno objašnjenje samog pojma. U glavi 2 će biti uvedeni i objašnjeni pojmovi koji su u vezi sa bezbjednošću informacija, a to su informacija, informacione tehnologije, sistemi i informaciono društvo. Glava 3 će biti posvećena pojmu bezbjednosti informacija - definiciji, oblastima zastupljenosti, kao standardima za upravljanje bezbjednošću informacija, uz poseban osvrt na Opštu uredbu o zaštiti podataka.

Naredne tri glave magistarske teze (Glava 4, 5, 6) će se baviti informacionim sistemom čiji je razvoj tema teze. U Glavi 4 će biti detaljno opisano projektovanje informacionog sistema. S obzirom da je razvijeni informacioni sistem uveden u upotrebu u Centralnoj banci Crne Gore, u istoj glavi će biti

opisana misija Centralne banke, način osiguravanja bezbjednosti informacija u njoj, opis stanja prije razvoja aplikativnog rješenja, kao i integracija sa postojećim informacionim sistemom. U Glavi 5 će biti navedene i objašnjene funkcionalnosti razvijenog aplikativnog rješenja. U Glavi 6 će biti nabrojane prednosti razvijenog aplikativnog rješenja uz smjernice za budući razvoj. U istoj glavi će biti riječi i o neuralnim mrežama čija upotreba omogućava značajno poboljšanje procesa upravljanja rizikom po bezbjednost informacija.

2. Informacione tehnologije, sistemi i društvo

2.1. Informacija

U savremenom dobu skoro da nema naučne discipline koja ne upotrebljava koncept informacije u kontekstu koji je njoj svojstven. U vezi sa tim, postoje mnoge koncepcije informacije. Navedene koncepcije ugrađene su u manje ili više eksplicitne teorijske strukture.

U toku prošlog vijeka pojam informacije se mnogo proučavao. Kao rezultat toga, informacija se definisala na razne načine, a veliki broj tih definicija su postavili filozofi. Filozof Ursul je definisao informaciju na sljedeći način: „Informacija predstavlja preslikavanje stanja jednog subjekta u stanje drugog subjekta. Pri tome ovo preslikavanje na drugi subjekt ne mora da bude istovjetno kod svih subjekata", [18], [20]. Ova definicija informacije se mnogo koristi i primjenjiva je na razne kontekste definisanja informacije. Navedena definicija pojma informacije ističe vezu informacije sa procesom prenošenja, odnosno komuniciranja između subjekata. Napomenimo da subjekt u procesu komuniciranja može biti čovjek, mašina, i slično. U procesu komunikacije uspostavlja se veza između subjekata koji komuniciraju, [19]. Načini ostvarivanja te veze mogu biti različiti - posredstvom govora, muzike, pisma, slika. Na osnovu navedenog zaključujemo da proces komuniciranja sačinjavaju tri komponente: informacioni izvor (koji šalje informacije), prijemnik (koji prima informacije) i kanal veze (preko koga se informacije prenose), [19].

2.1.1. Pojam informacije

Pojam informacije se prvi put pominje još u Staroj Grčkoj, kada je Aristotel govorio o informacijama i njihovom prenošenju. Dalje, u srednjem vijeku proučavanjem informacije i definisanjem njenih osnovnih osobina bave se ljudi koji su bili ispred svog vremena, najviše filozofi, [20].

Riječ informacija potiče iz latinskog jezika i nastala je od riječi *informatio* koja označava obavještenje, obavještavanje, uputstvo, podučavanje. Imajući u vidu etimološki aspekt riječi, informacija označava

činjenice koje se o nekoj stvari mogu saznati, saopštiti i prenijeti nekom drugom, [20]. Postoje različiti pristupi fenomenu informacije, a u skladu sa tim, i različita tumačenja pojma informacije.

Prema [31], informacija postoji između čovjeka i čovjeka, čovjeka i mašine, mašine i čovjeka, ali i između mašine i mašine. S druge strane, u [32] nailazimo na tvdnju da informacija postoji samo u relaciji čovjek – čovjek iz koje slijedi da su ljudi i tvorci i nosioci informacija. Pristup koji je iznešen u [31] je kibernetski pristup koji je širi i prihvatljiviji. U skladu sa tim pristupom, pojam informacija označavao bi slanje, prenošenje i primanje podataka ili opštenje pomoću znakova između čovjeka i čovjeka, čovjeka i mašine, mašine i čovjeka i mašine i mašine. Šire gledano, a u skladu sa [31], informacija predstavlja svaki uticaj nekog sistema S1 na bilo koji drugi sistem S2. Prema [33], informacija ukida neodređenost - entropiju. Entropija je mjera neodređenosti – haosa sistema u smislu prelaska u jedno od mogućih stanja. Imajući u vidu prethodno navedeno, informacija je kvantitativno jednaka entropiji kojom je sistem bio okarakterisan prije njenog pojavljivanja. Iz tog razloga, informacija se naziva i negentropija [33]. U literaturi, [20], nailazimo i na tumačenje pojma informacija kao namjenski usmjerenog znanja sa ciljem da pripremi odgovarajuće ponašanje. Prema [34], informacija je pored materije i energije osnovni resurs univerzuma. Zbog toga je vrlo važno ovladati upotrebom informacionih resursa da bi na najbolji mogući način upotrebljavali energetske i materijalne resurse.

U ovom trenutku informacija je postala toliko bitna da se može smatrati ključnim resursom u svim oblastima čovjekovog djelovanja. Takođe, informacija se može smatrati osobenom vrstom robe, [20]. Nevezano za teorijsko objašnjenje pojma informacija, važno je uvidjeti da se u savremenom društvu informacija smatra resursom. Ovakvo shvatanje informacije je veoma rasprostranjeno i njegova suština je u tome da se značaj informacije kao resursa izjednačava sa značajem tradicionalnih resursa, a to su novac, hardverske komponente, zaposleni i materijal. Ishodište shvatanja informacije kao resursa jeste u tome da je kompletna i pravovremena informacija resurs koji je neprikosnoveno važan prilikom odlučivanja. Još jedan aspekt tumačenja informacije dobijamo imajući u vidu da je primarni koncept savremenog društva upravljanje znanjem, a u osnovi znanja stoji informacija, [20]. Jedna od definicija znanja jeste da ono podrazumijeva količinu informacija, opažanja ili razumijevanja koje posjeduje neka osoba. Jasno je da viši nivo znanja omogućava smanjenje neizvjesnosti odvijanja procesa [20].

2.1.2. Neke definicije informacije

Kao što je već objašnjeno u prethodnom tekstu, postoji mnogo definicija i tumačenja informacije. U ovom poglavlju biće dat pregled najčešće korišćenih definicija, [20]. Najopštija definicija informacije je da je informacija odraz realnog svijeta, dok je najuža, specijalizovana definicija da je informacija podatak koji je podložan obradi.

Informacija je kompletnost podataka o svim mogućim objektima, pojavama ili procesima, [20]. Ona se može predstaviti u obliku crteža, teksta, zvučnih i svjetlosnih signala, energetskih i nervnih impulsa i slično. Posmatrano u odnosu na način nastanka, uočavamo elementarne informacije koje oslikavaju procese i pojave iz mrtve prirode, biološke informacije koje opisuju procese u životinjskom i biljnom svijetu i socijalne koje izražavaju procese u ljudskom društvu. Informacije koje kreira i upotrebljava čovjek mogu biti masovne, kao što su društveno-političke, naučno-popularne i slično, specijalne, u koje spadaju naučne, tehničke, ekonomske i slično i lične. Informacija je podatak koji ima određeno značenje, odnosno znanje koje je moguće prenijeti verbalno, pismeno, elektronski ili na neki drugi način, [18]. Peter Drucker, utemeljivač teorije savremenog menadžmenta, smatra da je informacija resurs današnjice i budućnosti, ali da nije poput materije ili energije jer se ne troši upotrebom, niti se smanjuje raspodjelom. Fascinantna su njegova razmišljanja o dijeljenju znanja: „Ako nešto znam mogu naučiti druge, a da sam ništa pri tome ne gubim. Primjenjujući to što sam saznao, ne samo da ne gubim korišćeno znanje, već ga oplemenjujem praksom", [20].

Informacija je svaki oblik komunikacije koja primaocu pruža razumljivo i korisno znanje, a sastoji se od podataka koji za primaoca imaju značenje. Informacija je često rezultat upita ili obrade, a odlike su joj: upotrebljivost, što znači da se može primijeniti za neku aktivnost ili u neku svrhu, zatim, razumljivost, odnosno da je data u razumljivom obliku i na kraju pravovremenost, što znači da je primljena u vrijeme i na način koji omogućava ispunjenje njene namjene, [21]. Šire gledano, pod informacijom podrazumijevamo svaku vijest koja za primaoca predstavlja novost.

2.1.3. Podatak i informacija

U literaturi, kao i u verbalnoj komunikaciji, pojmovi podatak i informacija se upotrebljavaju kao sinonimi. Međutim, takva upotreba nije potpuno korektna jer ovi pojmovi, zapravo, nemaju isto značenje.

Podaci su evidentirane činjenice o nekom događaju u realnom sistemu. Oni se sakupljaju i evidentiraju da bi se mogli upotrijebiti, [22]. Informacija je protumačeni podatak odnosno znanje koje se može dobiti iz podatka. Pod informacijom se podrazumijeva grupa podataka tako organizovanih i obrađenih da predstavljaju obavještenje, [22]. Podatak prerasta u informaciju tek kada se na odgovarajući način obradi i prezentira korisniku koji će moći da ga upotrijebi pri rješavanju problema ili prilikom donošenja odluke.

Postoji još jedna suštinska razlika između podatka i informacije. Podatak je objektivna kategorija. S druge strane, informacija zavisi od načina tumačenja prezentovanog podatka, što je čini subjektivnom.

Imajući u vidu značaj informacionih sistema za optimalno funkcionisanje poslovnih procesa u savremenom društvu, treba se osvrnuti i na definicije pojma informacije i podatka sa aspekta informacionih sistema. U osnovi infrastrukture informacionog sistema je računar. Računar se sastoji od elektronskih kola koja se mogu naći u jednom od dva stanja: kada kroz kolo protiče struja ili kada kroz kolo ne protiče stuja. Prvom stanju odgovara cifra 1, a drugom stanju cifra 0.

Imajući u vidu da raspolažemo samo sa dvije cifre, svaki podatak koji se čuva u računaru mora biti predstavljen kao određena kombinacija nula i jedinica. Zapis sastavljen od nula i jedinica naziva se binarni zapis. Prevođenje podataka u nizove nula i jedinica naziva se kodiranje. Kroz informacioni sistem podaci se prenose pomoću signala. Signali predstavljaju namjerno izazvane određene fizičke procese u kojima je sadržana poruka.

2.2. Istorija nastanka i definicije informacionog društva

Već nekoliko decenija informaciono društvo je jedan od ključnih pojmova koji se koriste za opis današnjeg društva, [36]. Nailazimo na raznoliku upotrebu ovog pojma – on se pojavljuje kao socijalni, kulturni, ekonomski i tehnički koncept, [38]. Opšti smisao u kojem se najčešće koristi odnosi se na servisno orjentisano društvo okarakterisano brzim razvojem visoke tehnologije, materijalnim bogatstvom, u kojem je informacija dominantni resurs, prije nego sirovina ili energija, [35]. Sve navedene osobine vode ka društvu koje se karakteriše tendencijom ka što većem zadovoljenju individualnih ljudskih potreba i očuvanju ekološke ravnoteže.

Ovaj pojam se odnosi na društvo koje omogućava velikom broju svojih članova da učestvuju u produktivnim poduhvatima za koje je potrebno posjedovanje značajne količine znanja, koji su

motivisani znanjem i zasnovani na znanju, [39]. Takođe, on podrazumijeva društvo koje ima komunikacionu mrežu kojom slobodno kruže informacije tako da se informacije konzistentno, djelotvorno i efikasno koriste prilikom donošenja odluka, [39]. Informaciono društvo ima sposobnost da upravlja uvijek prisutnim sukobom između konzervativnih struja i struja koje se zalažu za promjene, koristeći argumente koji se zasnivaju na racionalnom razmišljanju i razumijevanje utemeljeno na posjedovanju znanja, a ne tradicionalnim načinom koji uključuje emocije i, katkad, upotrebu sile, [39].

U smislu svoje zavisnosti od informacije, društvo je uvijek bilo informaciono, [39]. U skladu sa tim, oduvijek je postojala osnovna infrastruktura. Hiljadama godina zavisnost društva od informacija nije bila očigledna zbog toga što je količina informacija bila dovoljno mala tako da se mogla pamtiti i prenositi govorom. Najraniji pisani tragovi u svim kulturama su popisi, zakoni i priče - osnovni mnemonički alati za očuvanje društva. Čak i pisana literatura je imala svrhu da podstakne pamćenje, a da se značenje ne prenese direktno. Kada je količina informacije postala prevelika da bi se pamtila, društvo je kreiralo metod sličan pamćenju koji je služio za čuvanje informacija, [39]. Informacije su i dalje percipirane kao pasivne, potčinjene načinu zapisivanja, a ne kao dinamičan resurs. Uprkos tome, ljudi koji su upravljali i bavili se profitabilnim poslovima, zasigurno su znali vrijednost informacije kao dinamičnog resursa, [35]. Zbog toga su koristili informacije i kontrolisali ih što su više mogli. Sve od srednjeg do devetnaestog vijeka, vlade evropskih država su kontrolisale kanale informisanja kontrolišući novine i trgovinu knjigama, a obrazovanje je bilo dostupno samo članovima bogatih porodica koje su svakako kontrolisale profitabilne poslove.

U devetnaestom vijeku, dolazi do određenih promjena – s jedne strane, vlade mnogih država su postale liberalnije, a s druge strane, ljudi koji su se bavili industrijom postali su svjesni da su im potrebni radnici sa boljim obrazovanjem, [35]. To je dovelo do objavljivanja sve veće količine informacija, zatim do unapređenja opšteg obrazovanja i na kraju do formiranja univerziteta. Sve ove promjene izazvale su značajni ekonomski razvoj. Navedeni događaji u kombinaciji sa naučnim otkrićima iz osamnaestog vijeka, doveli su do toga da se, krajem devetnasetog vijeka percepcija cijelog društva, kao i upotreba informacije i znanja, promijene iz temelja, [39]. Rezultati tih promjena postali su evidentni sredinom dvadesetog vijeka. Nastanak informacionog društva posmatran je kao prirodni razvoj evropske liberalne tradicije ili američkog tehnološkog moderniteta, [38].

Imajući u vidu istoriju koja je prethodila njegovom nastanku, informaciono društvo označava najnoviju fazu ekonomski razvijenog društva, čije se ključne aktivnosti i institucije zasnivaju na upotrebi i razvoju informacionih i komunikacionih tehnologija, [39]. Definicija informacionog društva bazirana je na pojmovima komunikacija i informacije iz čega proizilaze dvije osnovne dimenzije ovog pojma - društvena, vezana za komunikacijski aspekt i intelektualna, vezano za informacioni aspekt.

2.3. Osnovni principi informacionog društva

Informaciono komunikacione tehnologije (ICT - Information and communications technology) predstavljaju za današnje društvo ono što su industrijske mašine predstavljale tokom industrijske revolucije – one su preinačile način rada, transformisale ekonomiju, imali nepovratan uticaj na način života ljudi i tako oblikovale novo informaciono društvo, [35], [36]. S jedne strane, prepoznata je fundamentalna uloga ICT u društvu orjentisanom ka posjedovanju informacija i sticanju znanja, a s druge strane, činjenica da postoji nejednakost u pristupu informacijama i distribuciji i dijeljenje ovih tehnologija, [36]. Iz ove dvije oprečne pojave, iskristalisao se prvi i najvažniji princip za informaciono društvo, a to je univerzalni servis, [37].

U okruženju u kojem su informacije i znanje postali ključni faktori za društveni i ekonomski razvoj, javila se potreba da se pristup informacijama i sredstvima koja omogućavaju upotrebu tih informacija proširi na što je moguće više korisnika. Iz tog razloga, obezbjeđivanje univerzalnog pristupa ili univerzalnog servisa predstavlja osnovnu tačku za sve deklaracije o informacionom društvu, [37]. Implementacija koncepta univerzalnog servisa podrazumijeva omogućavanje dostupnosti komunikacijskih uređaja svima – na individualnom nivou ili na nivou domaćinstva. Ovaj koncept je posebno istaknut u regulatorno - zakonodavnom okviru koji ukazuje na obavezu telekomunikacionih operatora da pruže svoje usluge čitavoj populaciji, [36]. Koncept univerzalne usluge je dopunjen konceptom univerzalnog pristupa. Početak implementacije ovog koncepta zahtijevao je inovativne pristupe, uključujući povezivanje zajednice i uspostavljanje javnih pristupnih tačaka, [35]. Uspostavljanje javnih pristupnih tačaka je omogućilo korisnicima pristup informacijama i znanju sa minimalnim troškovima u područjima koja nijesu imala servis [36]. U skladu sa prethodno navedenim, nameće se zaključak da je prvi korak ka univerzalnom servisu napravljen uspostavljenjem javnih tačaka pristupa. Neophodnost univerzalnog pristupa informacijama je navedena u nekoliko deklaracija, [35], [36], naglašavajući da svima i svuda treba omogućiti da učestvuju u globalnom informacionom društvu.

S obzirom da koncept univerzalnog pristupa može imati različite konotacije, kao što su sociološka, ekonomska i kulturna, treba naglasiti da se u ovom kontekstu on tumači kao materijalni i fizički pristup informacijskoj infrastrukturi i servisima, [36].
Razmatrajući potrebne uslove za dalji razvoj informacionog društva, uvidjelo se da je fizičko postojanje infrastrukture esencijalno, ali nije dovoljno, [35], [36]. Uočena je potreba da sve države promovišu jednake mogućnosti svojim građanima, a posebno da podstiču učešće slabijih kategorija na upotrebu ICT – a, [37]. Pored toga, upotreba glasovnih i touch screen aplikacija omogućila je većem broju ljudi da koristi ICT. Dalje, razvijanje aplikacija prilagođenih lokalnim potrebama dovela je do većeg interesovanja za upotrebu ICT - a. Na taj način je omogućeno stanovništvu da u što većem broju učestvuje u informacionom društvu.

Pored prethodno navedenog, sadržaj je osnovni element za korišćenje ICT-a, [35], [38]. Razvoj lokalnog sadržaja na internetu je sredstvo za obezbjeđivanje kulturno i lingvistički raznovrsnog sajberprostora, [38]. ICT pružaju nove kanale za izražavanje ove raznolikosti i za širenje lokalno stvorenog sadržaja širom svijeta. Plasiranje odgovarajućeg sadržaja aktueliziralo je još jedan aspekt informacionog društva - upotrebu ICT-a u obrazovne svrhe. Kvalitet i raznovrsnost sadržaja je od velikog značaja za podsticanje ljudi da se priključe online aktivnosti. U tom smislu su značajne aplikacije koje su korisne za različite jezike, kao što je, na primjer, prevod. Izrada lokalnog, nacionalnog i regionalnog sadržaja na maternjim jezicima, i smještanje tog sadržaja na regionalne servere, takođe može pomoći u racionalizaciji pristupa lokalnom i regionalnom saobraćaju i promovisanju njegove razmjene preko najrazvijenije magistrale, [36].

Jedan od važnih principa informacionog društva jeste sloboda izražavanja i sloboda pristupa. U informacionom društvu, komunikacije su sredstvo za primjenu principa slobode izražavanja. Za stvaranje globalnog informacionog društva neophodno je očuvati pluralizam mišljenja.

2.4. Informacione tehnologije i sistemi

Informaciono društvo je koncept koji naglašava upotrebu informacija i informacione tehnologije u praktično svakom društvu. Ono ne postoji bez informacionih i komunikacionih tehnologija jer su to sredstva za širenje i intenziviranje upotrebe informacija. Sagledavajući savremeno društvo, nameće se zaključak da je poslednjih godina takozvani tehnološki pritisak glavna pokretačka snaga za razvoj, [36].

U skladu sa tim, informaciono društvo zavisi od kompleksa elektronske informacione i komunikacione mreže i značajan dio svojih resursa opredjeljuje za aktivnosti informisanja i komunikacije. Postojanje informacione tehnologije samo po sebi nije dovoljno za postojanje informacionog društva. Međutim, postojanje svijesti o značaju posjedovanja i upotrebe informacija, kao i o sticanju znanja, u kombinaciji sa postojanjem informacionih tehnologija vodi ka razvoju informacionog društva. U obrazovnim sistemima mnogih država, od škola do univerziteta, tehnološka infrastruktura informacionog društva se upotrebljava za automatizaciju raznih poslovnih procesa, a istovremeno služi kao predmet proučavanja, [20].

Termin informacione tehnologije (IT – Information Technology) označava sve forme tehnologija koje učestvuju u procesu evidentiranja, obrade, čuvanja, zaštite i razmjene svih oblika podataka. U ovom obliku, termin je prvi put upotrijebljen u članku koji je 1985.godine objavljen u Harvard Business Review-u, sa ciljem da se napravi i istakne razlika između mašina posebne namjene predviđenih da izvršavaju ograničeni opseg funkcija i računarskih mašina za opštu namjenu koje mogu biti programirane da izvršaju različite operacije, [40]. Prema [40], informaciona tehnologija, na koju se odnosi ovaj članak, sastoji od tri osnovna dijela: računarske obrade podataka, podrške odlučivanju i poslovnog softvera.

Vremenski okvir, koji počinje objavljivanjem pomenutog članka, označio je početak IT-a kao zvanično definisanog područja poslovanja. Od sredine dvadesetog vijeka, IT industrija je značajno napredovala zahvaljujući tome što su pri proizvodnji elektronskih kola u računarima počeli da se upotrebljavaju tranzistori, a zatim i da se od njih izrađuju integrisana kola, [35]. Ovakav način proizvodnje računara doveo je do napretka sa dva aspekta. Na prvom mjestu, značajno su se poboljšale performanse računara – smanjilo se vrijeme potrebno za izvršavanje instrukcije, smanjila se njihova potrošnja energije i proizvodili su se računari manjih dimenzija. S druge strane, smanjili su se i troškovi njihove proizvodnje, što je rezultiralo smanjenjem cijene računara.

Informaciona tehnologija, prema Američkoj asocijaciji za informacione tehnologije, obuhvata proučavanje, projektovanje, razvoj, primjenu, podršku ili upravljanje informacionim sistemima zasnovano na računarima, posebno softverskih aplikacija i računarskog hardvera, [20]. U evropskim državama se naročito ističe komunikaciona komponenta informacione tehnologije, pa se upotrebljava naziv informaciono – komunikaciona tehnologija (ICT - Information and Communications Technology),

[20]. IT koriste računare i računarske programe da pretvaraju, čuvaju, štite, procesuiraju i, sa zadovoljavajućim stepenom bezbjednosti, šalju i primaju informacije. Termin informaciona tehnologija često obuhvata i mnogo veće područje u oblasti tehnologije, [39]. Pod tim se podrazumijevaju kompletne aktivnosti koje realizuju IT profesionalci, počevši sa instalacijom aplikativnih softvera, preko umrežavanja i inženjeringa računarskog hardvera, dizajniranja softvera i baza podataka, pa sve do projektovanja kompleksnih računarskih mreža i informacionih sistema, upravljanja informacionim sistemom i vođenja njegove administracije, [39].

Informacione tehnologije su relativno nova naučna disciplina koja postoji od kraja dvadesetog vijeka. Njeno pojavljivanje je koincidiralo sa prelaskom društva iz industrijskog u informaciono. Postavljanje raznih praktičnih zahtjeva vezanih za automatizaciju poslovnih procesa u organizacijama, dovela je do toga da se ova disciplina vrlo brzo razvija. Posmatrajući informacione tehnologije kao naučnu disciplinu, primjećujemo da ona više proučava tehnologije nego informacije, za razliku od informacionih sistema. U savremenom poslovnom svijetu, gotovo sve organizacije upotrebljavaju sisteme koji su bazirani na informacionim tehnologijama, tako da poslovanje u raznim sferama zavisi u velikoj mjeri od informacionih tehnologija.

Informaciono komunikacione tehnologije objedinjavaju računarske i komunikacione tehnologije i mikroelektroniku i na taj način obezbjeđuju povećanje efikasnosti i produktivnosti, dijeljenje i čuvanje informacija čime poboljšavaju i unapređuju komunikaciju, dovode do bržeg sticanja znanja, kao i njegovog širenja i primjene.

Prema [17], informacioni sistem možemo definisati na više načina. Informacioni sistem predstavlja sistem koji sakuplja, smješta, čuva, procesuira i isporučuje informacije koje su važne za neku organizaciju i obezbjeđuje njihovu dostupnost i upotrebljivost za sve osobe koje imaju pravo pristupa. Informacionim sistemom se smatra i skup ljudi i tehničkih sredstava koji po utvrđenim pravilima i metodologiji sprovode prikupljanje, memorisanje, obradu i daju na korištenje podatake i informacije. Pored toga, informacioni sistem je određeni skup metoda, postupaka i resursa, organizovanih da doprinesu dostizanju postavljenog cilja. Informacioni sistem u okviru neke organizacije, omogućava da organizacija ima unutrašnju i spoljašnju komunikaciju. Dakle, uslov opstanka bilo koje organizacije je da raspolaže podobnim informacionim sistemom, u kojem su razrađeni postupci informacionih aktivnosti. U nekim ogranizacijama te postupke obavljaju ljudi, a u drugima se koristi moderna

informaciona tehnologija. Iz toga zaključujemo da informacioni sistem može biti manuelan ili podržan informacionom tehnologijom, odnosno kompjuterizovan. On ne mora biti napravljen upotrebom informacionih tehnologija.

Informacioni sistem podržan informacionom tehnologijom je informacioni sistem koji podrazumijeva upotrebu računara. Treba napomenuti da je pojam informacionog sistema sveobuhvatniji od pojmova računara i računarske obrade podataka, [19]. To znači da informacioni sistem obuhvata i kompjuterizovani i nekompjuterizovani dio informacionih aktivnosti, odakle slijedi da informacioni sistem može da postoji i bez računarske podrške.

Informacioni sistem je kompleksan organizacioni sistem, a kompleksnost se odnosi i na strukturu elemenata i na strukturu veza u okviru sistema, kao i veza sa okruženjem, [15]. Sistem treba da bude postavljen tako da način na koji se upotrebljava bude jasan svim korisnicima, da jasno prikazuje informacije, da njegov rad bude pouzdan i da omogućava isporuku obrađenih informacija u vrlo kratkim vremenskim intervalima, [19].

Prvi veliki mehanički informacioni sistem bila je mašina koja omogućila tabelarni prikaz podataka iz popisa stanovištva, koju je izumio Herman Hollerith, [42]. Ova mašina je predstavljala veliki korak u automatizaciji, kao i inspiraciju za razvoj računarskih informacionih sistema.

3. Bezbjednost informacija i standardi za upravljanje bezbjednošću informacija

3.1. Bezbjednost informacija – definicija i ciljevi

Bezbjednost informacija (Information security - Infosec) je skup strategija za upravljanje procesima, alatima i politikama neophodnim za sprečavanje, otkrivanje, dokumentovanje i protivljenje prijetnji digitalnim i ne-digitalnim informacijama, [41]. Domen odgovornosti bezbjednosti informacija obuhvata uspostavljanje skupa poslovnih procesa koji će zaštititi informacijske resurse nezavisno od toga kako su informacije formatirane, da li su u procesu prenošenja ili ne, obrađujuju li se ili su u stanju mirovanja, [41].

Informacijski resursi su cjeline znanja koje su organizovane u obliku jednog entiteta i kojima se na takav način i upravlja, [42], [43], [45]. Kao i sva druga imovina organizacija, tako i informacijski resursi imaju svoju finansijsku vrijednost, [41], [42]. Finansijska vrijednost informacijskog resursa je direktno proporcionalna broju ljudi koji mogu koristiti taj informacijski resurs, [42]. S obzirom da informacije mogu imati kratak životni ciklus, vrijednost informacijskog resursa se vremenom smanjuje, kao i vrijednost mnogih drugih vrsta resursa jedne organizacije, [43]. Brzina kojom informacijski resurs gubi vrijednost zavisi od vrste informacija koje resurs predstavlja, kao i od toga koliko tačne informacije mogu ostati s vremenom. U nekim organizacijama, informacije koje se ne mogu koristiti se smatraju obavezom.

Informacijski resursi se mogu klasifikovati upotrebom različitih kriterijuma, ne samo prema relativnom značaju resursa ili prema učestanosti njegove upotrebe, [41], [42]. Na primjer, podaci se mogu razvrstati na osnovu sadržaja, vremena kreiranja, mjesta kreiranja, zaposlenog ili dijela organizacije koji ih najviše koriste. Sistem klasifikacije podataka može se implementirati tako da bi se informacijski resursi organizacije što lakše pronalazili, dijelili i održavali, [47], [48].

U odnosu na to ko ima pristup podacima, podaci se dijele na javne, interne, povjerljive i tajne, [47]. Pristup javnim podacima je neograničen. U ovu klasu podataka spadaju podaci koji se dobijaju od javnih servisa za pružanje informacija. Pristup internim podacima dozvoljen je samo pojedinim grupama korisnika, [47]. Ukoliko dođe do objavljivanja ove vrste podataka, to nije od kritične važnosti. Podaci u razvojnim grupama, kao i radne verzije dokumenata i projekata spadaju u interne podatke, [47]. Povjerljivi podaci su podaci koji su unutar određene grupe zaštićeni od neovlašćenog pristupa. Takvi su podaci o zaposlenima, podaci o zaradama zaposlenih, projektna dokumentacija, kao i razni računovodstveni podaci i povjerljivi ugovori. Šteta koja se nanosi organizaciji objavljivanjem ove vrste podataka je značajna, [47], [48]. Neovlašteni pristup tajnim podacima je strogo zabranjen. Mali broj korisnika ima ovlašćenje za pristup dokumentima koji sadrže tajne podatke. U ovu grupu podataka spadaju podaci o većim novčanim transakcijama, podaci koji su u vezi sa vojnim djelovanjem, podaci koji imaju značaj na državnom nivou i slično, [47], [48].

Metodologije vezane za bezbjednost informacija se temelje na osnovnim ciljevima CIA trojstva (C – Confidentiality, I – Integrity, A - Availability), a to su održavanje povjerljivosti, integriteta i dostupnosti IT sistema i poslovnih podataka, [21]. CIA trojstvo je model dizajniran da bude zvijezda vodilja za osmišljavanje politike za bezbjednost informacija unutar organizacije. Smatra se da su elementi trojstva tri suštinske komponente na kojima se temelji bezbjednost informacija. U tom smislu, povjerljivost je skup pravila koji ograničavaju pristup informacijama, integritet je garancija da su informacije pouzdane i tačne, a dostupnost je garancija pouzdanog pristupa informacijama za ovlašćene korisnike, [21]. Ovi ciljevi osiguravaju da se osjetljive informacije objelodanjuju samo ovlašćenim korisnicima (povjerljivost), sprečavaju neovlašćenu izmjenu podataka (integritet) i garantuju dostupnost podataka ovlašćenim korisnicima na upit (dostupnost), [21].

Povjerljivost je približno ekvivalentna privatnosti, [21]. Mjere koje se uvode da osiguraju povjerljivost su osmišljene tako da spriječe neovlašćene korisnike da dođu do osetljivih informacija, a da istovremeno obezbijede da ovlašćeni korisnici imaju nesmetan pristup informacijama, [21]. Usvojena je praksa da se podaci sortiraju prema količini i vrsti oštećenja koja bi mogla nastati ukoliko podaci dospiju do neadekvatne osobe, [23], [24]. U skladu sa tako formiranim kategorijama se implementiraju više ili manje stroge mjere. Ponekad očuvanje povjerljivosti podataka može uključiti i posebnu obuku za osobe koje imaju ovlašćenja za rad sa povjerljivim dokumentima, [23], [24], [25]. Takva vrsta obuka uključuje razmatranje sigurnosnih rizika koji bi mogli ugroziti ove informacije. Ovlašćene osobe se, sprovođenjem

obuke, upoznaju sa faktorima rizika i mogućim načinima zaštite podataka, [25]. Dalji aspekti obuke mogu uključiti jake lozinke i najbolje prakse vezane za lozinku, kao i informacije o metodama socijalnog inženjerstva, u cilju sprečavanja deformisanja usvojenih pravila za rukovanje podacima, [25]. Uobičajeni metod za obezbjeđivanje povjerljivosti je enkripcija podataka. Enkripcija je sistem kodiranja nekog sadržaja upotrebom odgovarajućeg algoritma, [49], [50]. Pored toga, procedura postojanja korisničke šifre i lozinke prilikom bilo kojeg pristupa podacima, koji nijesu javni, predstavlja standardnu proceduru, [51]. U savremenom društvu standard postaje i dvostruka autentifikacija – nešto što znaš i nešto što imaš, [53]. U tu svrhu se koriste sigurnosni žetoni, tokeni ili kartice. Upotrebljava se i mogućnost biometrijske verifikacije, [53]. Ovlašćeni korisnici mogu preduzeti dodatne mjere sigurnosti u smislu smanjenja broja ponavljanja informacije i broja prenosa informacije prilikom izvršavanja određene transakcije, [53]. U slučaju dokumenata koji su posebno osjetljivi po pitanju pristupa, koriste se pojačane mjere opreza kao što je čuvanje dokumenata samo na kompjuterima koji su fizički teško dostupni ili na odvojenim uređajima za čuvanje podataka, [48]. Za dokumente sa najvišim stepenom tajnosti praktikuje se i čuvanje samo u štampanom obliku, [48].

Integritet podrazumijeva održavanje konzistentnosti, tačnosti i pouzdanosti podataka tokom cijelog životnog ciklusa, [21]. Tokom prenosa podaci ne smiju biti podložni promjeni i u tom smislu se moraju preduzeti neophodne mjere koje obezbjeđuju da korisnici koji nemaju ovlašćenja ne mogu mijenjati podatke (na primjer, u povredi povjerljivosti), [46]. Ove mjere obuhvataju dozvolu pristupa fajlovima i kontrolu pristupa korisnika. U cilju sprečavanja pogrešnih izmjena sadržaja ili slučajnog brisanja dokumenata od strane autorizovanih korisnika upotrebljava se i kontrola verzija dokumenata, [46]. Pored toga, na raspolaganju moraju biti sredstva koja su potrebna da bi se otkrile bilo kakve promjene u podacima koji mogu nastati kao rezultat događaja koji nisu izazvani ljudskim faktorom, kao što je elektromagnetski impuls (EMP) ili pad sistema servera. Neki podaci mogu biti organizovani tako da uključuju kontrolne korake, čak i kriptografske kontrolne korake, za provjeru integriteta, [25]. Da bi mogao da se sprovede oporavak oštećenih podataka, neophodno je da postoje rezervne kopije podataka (backup). U tom smislu je izuzetno važno redovno generisanje rezervnih kopija podataka.

Dostupnost se najsigurnije obezbjeđuje redovnim održavanjem cjelokupnog hardvera, blagovremenim sprovođenjem potrebnih popravki i održavanjem ispravnog funkcionisanja okruženja operativnog sistema bez konflikata softvera koji pod njim funkcionišu, [21]. Neophodno je i biti u toku sa svim nadogradnjama sistema koje je potrebno uraditi. Podjednako je važno i obezbeđivanje adekvatnog

propusnog opsega komunikacije i sprečavanje pojave uskih grla. Ukoliko dođe do hardverskih problema redundantnost servera, failover i klasteri velike dostupnosti mogu ublažiti ozbiljne posledice, [54]. Kada se radi o najgorim scenarijima, brzi i adaptivni oporavak od katastrofa je od suštinskog značaja. Sposobnost oporavka mnogo zavisi od postojanja kompletnog i preciznog plana oporavka od katastrofa (DRP - Dissaster Recovery Plan), [26]. Pri kreiranju plana oporavka treba se usredsrediti na osmišljavanje načina za uspostavljanje aktivnosti na glavnoj lokaciji poslije dešavanja katastrofe. Svaka vrsta zaštite od gubljenja podataka ili prekida veze kojom se podaci prenose mora uključivati nepredvidljive događaje kao što su prirodne katastrofe i požari. Da bi se spriječio gubitak podataka u takvim slučajevima, rezervna kopija bi morala biti čuvana na geografski izolovanoj lokaciji, možda čak i u sefu koji je otporan na vodu i vatru. Dodatna bezbjedonosna oprema i programi kao što su firewall i proksi serveri se koriste kao zaštita od zastoja u radu sistema i nedostupnosti podataka izazvanih zlonamjernim akcijama kao što je izazivanje prekida u radu servisa i upadi u mrežu, [26].

Mnoge velike organizacije zapošljavaju grupu ljudi koji su posvećeni bezbjednosti informacija i zaduženi su za implementaciju i održavanje programa vezanih za bezbjednost informacija organizacije, [51]. Generalno, ova grupa je odgovorna za sprovođenje upravljanja rizicima po bezbjednost informacija, a to je proces u kome se neprekidno procenjuju ranjivosti i pretnje informacijskim resursima organizacije, a nakon toga utvrđuju i primjenjuju odgovarajuće zaštitne kontrole, [53]. Vrijednost organizacije leži u njenim informacijskim resursima, pa je očigledno da je čuvanje njihove bezbjednost od ključnog značaja za poslovanje, kao i za zadržavanje kredibiliteta i povjerenje klijenata.

Prijetnje osjetljivim i privatnim informacijama mogu se pojaviti se u različitim oblicima, kao što su zlonamjerni programi i phishing napadi, krađa identiteta i ransomvare. U cillju odvraćanja potencijalnih napadača i ublažavanja ranjivosti u različitim tačkama, vrši se implementacija višestrukih sigurnosnih kontrola, koje se koordiniraju kao dio slojevite strategije odbrane, [25]. Navedena koncepcija bi trebalo da minimizira uticaj napada. Da bi bili spremni da reaguju u slučaju kršenja bezbjednosti, grupe zaposlenih zadužene za bezbjednost treba da imaju plan po kome se postupa u slučaju incidenta (IRP – Incident response plan), [46]. Pri kreiranju IRP – treba se usredsrediti na osmišljavanje načina trenutnog reagovanja u slučaju incidenta. Postojanje ovog plana bi trebalo da omogući kontrolisanje i ograničavanje štete, uklanjanje uzroka i primjenu poboljšanih kontrola, [46].

Politika bezbjednosti informacija i procesi vezani za njeno sprovođenje obuhvataju fizičke i digitalne mjere bezbjednosti u cilju zaštite podataka od neovlašćenog pristupa, korišćenja, replikacije ili uništavanja. Primjeri fizičkih mjera zaštite su upotreba prostorije sa dvoje vrata, pri čemu se jedna otključavaju i otvaraju samo dok su druga zatvorena i zaključana (mantrap) i upravljanje šifrovanjem ključeva. Sistemi za otkrivanje upada u mrežu, primjena politike lozinke i poštovanje propisa predstavljaju digitalne mjere zaštite. Da bi se procijenila sposobnost organizacije da održava sisteme bezbjednosti u odnosu na set utvrđenih kriterijuma, vrši se revizija bezbjednosti informacija.

3.2. Oblasti zastupljenosti bezbjednosti informacija

Bazirano na izlaganjima iz [41], bezbjednosti informacija se pojavljuje kao:

- *Bezbjednosti aplikacija* koja pokriva softverske ranjivosti u veb i mobilnim aplikacijama i interfejsima aplikativnog softvera (API – Application programming interface). Kod pomenutih aplikacija ranjivosti se mogu pojaviti prilikom autentifikacije ili autorizacije korisnika, u integritetu programskog koda i konfiguraciji, kao i u stepenu razvijenosti politika i procedura. Slabosti aplikacija mogu stvoriti ulazne tačke za značajna kršenja bezbjednosti informacija. Očuvanje bezbjednost aplikacija je važan dio odbrane za očuvanje bezbjednosti informacija.
- *Bezbjednost Cloud-a* se fokusira na kreiranje i postavljanje zaštićenih aplikacija na cloud okruženje i njihovu bezbjednu upotrebu za korisnike. Cloud znači da se aplikacija pokreće u zajedničkom okruženju. Organizacije koje koriste cloud moraju biti sigurne da postoji adekvatna izolacija između različitih procesa koji se odvijaju u zajedničkom okruženju.
- *Kriptovanje podataka* prilikom prenosa ili u mirovanju doprinosi očuvanju njihove povjerljivosti i integriteta. Kako bi se potvrdila autentičnost podataka, u kriptografiji se obično koriste digitalni potpisi. Kriptografija i enkripcija postaju sve važniji. Dobar primjer upotrebe kriptografije je Advanced Encription Standard (AES). AES je simetrični algoritam koji se je u SAD - u usvojen kao federalni standard za enkripciju podataka i korišćen je u komunikacijama Američke vlade.
- *Bezbjednost infrastrukture* se bavi zaštitom mreža, laboratorija, data centara, servera, desktopa i mobilnih uređaja.
- *Odgovor na incident* je funkcija koja prati i istražuje potencijalno zlonamjerno ponašanje. Prilikom pripreme za slučaj kršenja bezbjednosti, zaposleni treba da naprave plan za slučaj pojavljivanja incidenta u cilju kontrolisanja prijetnje i uspostavljanja mreže. Pored toga, plan

treba da obuhvati kreiranje sistema za očuvanje dokaza za forenzičku analizu i potencijalno gonjenje. Ovi podaci mogu pomoći u sprečavanju daljeg kršenja bezbjednosti i pomoći zaposlenima da otkriju napadača.

- *Upravljanje ranjivostima* je proces skeniranja okruženja za slabe tačke. Razlozi pojavljivanja novih ranjivosti mogu biti različiti. Jedan od razloga pojavljivanja ranjivosti jeste dodavanje aplikacija, korisnika i infrastrukture u cjelokupni sistem. Imajući u vidu da se to u velikom broju organizacija često dešava, važno je utvrditi vremenski period sprovođenja skeniranja sistema za potencijalne ranjivosti. Pronalaženje ranjivosti i predviđanje potencijalnih prijetnji koje su vezane za te ranjivosti predstavlja suštinu upravljanja rizicima po bezbjednost informacija.

3.3. Standardi za upravljanje bezbjednošću informacija

Da bi organizacije mogle da smanje rizik po bezbjednost informacija i da obezbijede kontinuitet poslovanja nezavisno od eventualne promjene zaposlenih, morao je biti utvrđen formalni set smjernica za očuvanje bezbjednosti informacija - Sistem za upravljanje bezbednošću informacija (ISMS - Information Security Management System), [26]. Ovaj set smjernica i procesa je kreiran da bi pomogao organizacijama u ostvarivanju cjelishodnog postupanja u slučaju da dođe do kršenja bezbjednosti informacija. ISMS je sistematski pristup upravljanju osjetljivijim informacijama organizacije tako da bude zadovoljena bezbjednost informacija, [26]. Pomenuti pristup uključuje ljude, procese i IT sisteme primjenom procesa upravljanja rizicima po bezbjednost informacija.

Dobro poznata specifikacija ISMS – a je standard ISO/IEC 27001 koji pripada familiji standarda ISO/IEC 27000, [26]. Pomenuta familija obuhvata više od dvanaest standarda, a najpoznatiji je ISO/IEC 27001 koji propisuje uslove za uspostavljanje, implementaciju, održavanje i kontinuirano unapređenje sistema upravljanja informacijama u kontekstu organizacije, [26]. Pored navedenog, standard uključuje i zahtjeve za procjenu i tretman rizika po bezbjednost informacija prilagođenih potrebama organizacije. Uslovi koji su postavljeni u standardu su generički i mogu se primijeniti na bilo koju organizaciju, nezavisno od njene vrste, veličine ili prirode, [44]. Neki od uslova koji su definisani standardom su usklađenost sa zakonima, sistematska zaštita od zlonamjerne upotrebe kompjutera, sajber kriminala i drugih negativnih uticaja, uzdizanje svog ugleda kod zaposlenih, klijenata i partnerskih organizacija,

unaprijeđena prodaja usluga, praktične odluke u vezi sa bezbjedonosnim tehnikama i razvojna rješenja, postojanje odgovornosti za bezbjednost informacija od strane svih i na svim nivoima u organizaciji, smanjenje troškova koji nastaju usled zloupotrebe informacija, [52]. Standard propisuje tehničke mjere zaštite (lozinke, programsko šifrovanje, prava pristupa i sl.), administrativne (sigurnosne politike, pravilnike, procedure) i fizičke mjere (video nadzor, zaštita prostorija, fizička kontrola pristupa itd.), [52].

Organizacije čiji sistem za upravljanje bezbjednošću informacija funkcioniše prema standardu ISO/IEC 27001 imaju mogućnost da izvrše sertifikaciju tog sistema u skladu sa standardom ISO/IEC 27001, [44]. Treba napomenuti da sertifikacija nije obavezna. Neke organizacije odlučuju da implementiraju standard kako bi imali koristi od najbolje prakse koja je ustanovljena standardom, dok druge žele da sprovedu procedure sticanja sertifikata, koji, kao dokaz o primjeni, predstavlja garanciju da je standard na odgovarajući način primijenjen u konkretnoj organizaciji.

3.4. Opšta uredba o zaštiti podataka

Kada se govori o bezbjednosti informacija, neophodno je pomenuti Opštu uredbu o zaštiti podataka (GDPR - General Data Protection Regulation). Uredba je usvojena u aprilu 2016. godine od strane Evropskog parlamenta i Savjeta Evrope, a stupila je na snagu 25.maja 2018. godine, [55], [56]. Period pripreme koji je trajao dvije godine, omogućio je organizacijama i javnim organima na koje se regulativa odnosi da spovedu potrebne izmjene kako bi se uskladile sa regulativom.

Opšta uredba o zaštiti podataka je zakonska regulativa Evropske unije za zaštitu ličnih podataka njenih građana, tako da sve organizacije koje obrađuju podatke građana Evropske unije, nezavisno od toga da li posluju u Evropskoj uniji ili van nje, podliježu pravilima uredbe, [55], [56]. Svrha uredbe je, ne samo kontrola upotrebe ličnih podataka, nego i promjena pristupa pri njihovoj upotrebi, [55], [56]. Organizacije u svakom trenutku moraju znati gdje su koji podaci, kao i u koju svrhu se smiju koristiti. Isto tako, u slučaju da neko odluči da povuče dozvolu za upotrebu svojih ličnih podataka, organizacije moraju biti u mogućnosti da u traženom roku to i sprovedu. Subjekti koji koriste podatke će tako moći da potvrde pravo na skupljanje podataka, a pravila o privatnosti će precizno definisati kako se podaci čuvaju i upotrebljavaju. Pored toga, uredba predviđa da fizičko lice u bilo kojem trenutku može pristupiti podacima, ispraviti ih ili obrisati iz sistema neke organizacije, [55], [56]. Osnovni zahtjevi koje

uredba postavlja organizacijama je da imaju program upravljanja podacima, da imenuju službenika za zaštitu podataka, da zahtijevaju saglasnost korisnika za obradu podataka, da izvrše popisivanje i mapiranje podataka, da obezbijede legitimne osnove za obradu podataka, da sprovedu analizu rizika i procjenu uticaja na podatke, da omoguće ostvarivanje prava vezanih za podatke, da pruže obavještenja o kršenju zaštite podataka i da podatke učine anonimnima u smislu privatnosti.

Kršenje pravila uredbe se sankcioniše izricanjem novčanih kazni sa maksimalnom kaznom od 4% ukupnog godišnjeg prihoda organizacije ili 20 miliona eura, u zavisnosti od toga koja je vrijednost veća, [55],[56].

4. Projektovanje informacionog sistema za upravljanje rizicima po bezbjednost informacija u Centralnoj banci Crne Gore

4.1. Uloga Centralne banke Crne Gore

U skladu sa referencom [27], zadatak Centralne banke je da stimuliše i čuva stalnost finansijskog sistema, uključujući stimulisanje i očuvanje vitalnog bankarskog sistema i pouzdanog i uspješnog platnog prometa.

Osnovne funkcije Centralne banke, [27], su da:

- brine o očuvanju ustaljenosti cjelokupnog finansijskog sistema i vezano za to utvrđuje regulativu;
- dozvoljava rad banaka i finansijskih institucija i sprovodi kontrolu njihovog rada;
- izvršava stečajni i likvidacioni postupak banaka i finansijskih institucija u skladu sa zakonom;
- reguliše platni promet u zemlji i sa inostranstvom i vrši kontrolu njegovog funkcionisanja;
- ima mogućnost da bude vlasnik i operater platnog sistema i participant u drugom platnom sistemu;
- ukoliko nije operater nekog platnog sistema, ispostavlja dozvolu za njegov rad i nadgleda funkcionisanje platnih sistema;
- rukovodi međunarodnim rezervama;
- prema određenim međunarodnim finansijskim institucijama izvršava poslove platnog i/ili fiskalnog agenta i može predstavljati državu Crnu Goru u međunarodnim finansijskim institucijama;
- sprovodi makroekonomske analize i Vladi države Crne Gore upućuje preporuke vezano za ekonomsku politiku;
- prepoznaje faktore koji mogu uticati na cjelokupni finansijski sistem i analizira ih;
- sakuplja podatke i informacije koji su bitni za njeno funkcionisanje , a zatim ih statistički tretira i objavljuje;
- konstituiše informacioni sistem koji podržava njeno uspješno funkcionisanje;

- izvršava prenose na državnom i inostranom finansijskom tržištu;
- prihvata depozite banaka, državnih organa i organizacija i finansijskih institucija i drugih subjekata, poštujući propise;
- formira račune banaka i finansijskih institucija, državnih organa i organizacija, stranih banaka, centralnih banaka, međunarodnih finansijskih institucija, organizacija koje doniraju sredstva državnim organima i organizacija i drugih lica poštujući zakon i propise i sprovodi platni promet po tim računima;
- utvrđuje propise i mjere iz djelokruga svog zakonskog ovlašćenja;
- izvršava i druge poslove propisane zakonima.

4.2. Metodologija za upravljanje rizicima po bezbjednost informacija u Centralnoj banci Crne Gore

Kao što je već navedeno u prethodnom tekstu, informacija je poslovna imovina i kao takva ima suštinski značaj za svaku organizaciju. Stoga se nameće zaključak da je očuvanje bezbjednosti informacija poslovna potreba. Očuvanje bezbjednosti informacija predstavlja postizanje ciljeva poslovanja na bezbjedan način, u kojem su zadovoljeni regulatorni i bezbjedonosni zahtjevi kroz ugradnju odgovarajućih kontrola, upravljanje rizicima, kao i kroz podizanje svijesti o bezbjednosti informacija u organizaciji.

Iskustvo je pokazalo da je većina bezbjednosnih incidenata u organizacijama izazvana određenim djelovanjem zaposlenih. Veliki procenat takvih incidenata nije izazvan namjerno, nego usljed nedostatka znanja iz oblasti bezbjednosti informacija. Na osnovu toga, nameće se zaključak da je izuzetno važno da se zaposleni obučavaju o tome šta sve može biti rizično po poslovanje organizacije i kako treba reagovati u tom slučaju, [29].

U vezi sa tim, Centralna banka Crne Gore je donijela Politiku i Pravila bezbjednosti informacija. Politika bezbjednosti informacija je dokument koji je u potpunost usklađen sa međunarodnim standardima bezbjednosti informacija iz ISO/IEC 27000 familije, sa jedne strane, i usaglašen sa zakonskom regulativom u Crnoj Gori, kao i sa konceptom bezbjednosti informacija Evropske unije, sa druge strane. Dokument Pravila bezbjednosti informacija predstavlja dopunu Politici, u smislu razrade pojedinih stavki, [29]. Prema [29], svi zaposleni u Centralnoj banci Crne Gore, na svim nivoima u

organizaciji, su odgovorni za očuvanje bezbjednosti informacija. Posljedično, svaki zaposleni mora biti u potpunosti svjestan svoje uloge u sistemu bezbjednosti informacija.

U Centralnoj banci Crne Gore postoji utvrđena Metodologija za upravljanje rizicima po bezbjednost informacija Centralne banke Crne Gore (u daljem tekstu Metodologija). Metodologija podrazumijeva da se upravljanje rizicima sprovodi kroz identifikaciju i vrednovanje informacijskih resursa u Centralnoj banci Crne Gore, grupisanje identifikovanih resursa u određene kategorije, identifikaciju i ocjenu ranjivosti i prijetnji koje se mogu pojaviti za određenu kategoriju resursa, kao i procjenu rizika i izradu plana tretmana rizika, [28]. Metodologija se primjenjuje na sve poslovne procese, organizacione jedinice, lokacije u kojima se obavljaju poslovni procesi kao i sve resurse Centralne banke.

Prema [28], Direkcija za upravljanje operativnim rizikom, bezbjednošću informacija i kontinuitetom poslovanja (u daljem tekstu: Direkcija) koordinira proces procjene i obrade rizika, a proces sprovode zaduženi zaposleni iz samostalnih organizacionih jedinica, za informacijske resurse koji su u vlasništvu tih organizacionih jedinica. Samostalne organizacione jedinice izvještavaju Direkciju o sprovođenju planiranih tretmana rizika. Na osnovu dostavljenih izvještaja organizacionih jedinica, Direkcija izvještava rukovodstvo o identifikovanim rizicima po bezbjednost informacija, kao i o realizaciji predviđenih tretmana za rizike. Drugim riječima, primjena Metodologije iziskuje kreiranje Registra i Plana tretmana rizika po bezbjednost informacija (u daljem tekstu Registar rizika po bezbjednost informacija) za poslovne procese koji se odvijaju u Centralnoj banci Crne Gore.

Metodologija propisuje da se procedura procjene i obrade rizika po bezbjednost informacija sprovodi na sljedeći način: Svaka samostalna organizaciona jedinica u Centralnoj banci vrši procjenu i obradu rizika za svoje poslovne procese. Najprije se izvrši popis poslovnih procesa i na osnovu toga se identifikuju informacijski resursi. Identifikovanim resursima se dodjeljuju vlasnici u skladu sa zahtjevima standarda ISO/IEC 27001, po kojem je vlasnik resursa pojedinac ili entitet kome je dodijeljena odgovornost od strane menadžmenta za kontrolisanje proizvodnje, razvoja, održavanja, upotrebe i bezbjednosti resursa. Identifikovani resursi se svrstavaju u neku od sljedećih kategorija:

- Informacije
- Softver
- Fizičke vrijednosti
- Servisi

- Ljudi
- Nematerijalne vrijednosti.

Resursi se vrednuju u skladu sa CIA metodom, [28]. Za svaki identifikovani resurs, parametri C, I i A se pojedinačno vrednuju nekim od brojeva od 1 do 4, u zavisnosti od značaja za Centralnu banku, u skladu sa tabelama definisanim u Metodologiji, pri čemu većoj brojčanoj vrijednosti parametra odgovara veći značaj. Dalje, poslije vrednovanja prametara C, I i A, za svaki resurs se izračunava proizvod C x I x A, koji može iznositi najmanje 1, a najviše 64. Procjena vrijednost resursa se vrši zbog toga što se samo za resurse čija je pocijenjena vrijednost 12 ili više, utvrđuju ranjivosti kojima su oni izloženi i prijetnje koje mogu iskoristiti te ranjivosti. Za svaki resurs posebno, identifikovane ranjivosti i prijetnje se upisuju u Registar i plan tretmana rizika.

Nakon identifikacije ranjivosti i prijetnji, slijedi njihovo vrednovanje u smislu utvrđivanja vjerovatnoće pojavljivanja prijetnje, stepena ranjivosti i stepena uticaja ranjivosti na određeni resurs, a u skladu sa tim, i na cjelokupno poslovanje Centralne banke. Metodologijom su definisane tabele sa mogućim brojčanim vrijednostima, klasifikacijom i pripadajućim opisima za vjerovatnoću pojavljivanja prijetnje, stepena ranjivosti i stepena uticaja ranjivosti. Moguće vrijednosti su brojevi od 1 do 3, pri čemu manjem broju odgovara niža klasifikacija.

Sljedeći korak jeste formiranje ocjene rizika. Ocjena rizika je veličina koja omogućava da se procijeni moguća šteta koja će se nanijeti Centralnoj banci i da se sagleda značaj uticaja ranjivosti i prijetnji na poverljivost, integritet i raspoloživost njenih resursa. Ova veličina zavisi od opsega vrijednosti u kojem se nalazi vrijednost rizika. Na vrijednost rizika utiče vrijednost samog resursa, kao i vrijednost za vjerovatnoću prijetnje, stepen ranjivosti, stepen uticaja ranjivosti, te se ona izračunava prema formuli:

$$Rizik = Vrijednost\ resursa + Vjerovatnoća\ prijetnje \times Stepen\ ranjivosti \times Stepen\ uticaja.$$

Imajući u vidu moguće vrijednosti za veličine na osnovu kojih se izračunava vrijednost rizika, uočavamo da je minimalna vrijednost rizika $R_{min} = 1 + 1 \times 1 \times 1 = 2$, dok je maksimalna $R_{max} = 64 + 3 \times 3 \times 3 = 91$. Metodologijom su definisane tabele u kojima je tačno određeno koja ocjena, nivo rizika i opis odgovaraju različitim rasponima vrijednosti rizika. Na osnovu izračunate vrijednosti rizika, u skladu sa tabelom definisanom Metodologijom, određuje se ocjena rizika i nivo rizika, odnosno vrši se

klasifikacija rizika. Ocjena rizika može uzeti vrijednost od 1 do 4, pri čemu ocjeni 1 odgovara nivo rizika *Veoma visok*, a ocjeni 4 *Nizak*.

Cilj klasifikacije rizika jeste da pokaže kakav stav treba zauzeti prema identifikovanom riziku. Ukoliko je nivo rizika nizak, on se ne razmatra, niti tretira, ukoliko je nivo srednji mora se do nekog prihvatljivog roka napraviti plan tretmana tog rizika, a ukoliko je visok ili veoma visok plan tretmana mora biti hitno napravljen i primijenjen. Metodologija takođe definiše i moguće opcije za treman rizika. Cijeli postupak, za posmatrani period, zaokružuje se ocjenom efektivnosti primijenjenih kontrola.

4.3. Način vođenja Registra rizika prije uvođenja informacionog sistema za upravljanje rizicima

U prethodnom poglavlju opisana je Metodologija koja predstavlja regulativu za upravljanje rizicima po bezbjednost informacija u Centralnoj banci. Praktična implementacija regulative, prije uvođenja aplikativnog rješenja, podrazumijevala je da svaka samostalna organizaciona jedinica Centralne banke kreira po jedan dokument sa spiskom svojih resursa, za njih identifikovanih prijetnji i ranjivosti i planom tretmana rizika, u obliku excel fajla, te da pomenuti fajl, putem email servisa dostavlja Direkciji. Direkcija bi zatim sprovodila kontrolu podataka za svaki pristigli fajl. Proces kontrole podataka je obuhvatao kontrolu unosa podataka, u smislu usklađenosti unijetih vrijednosti sa Metodologijom, utvrđivanja da li su informacijski resursi ispravno identifikovani i kategorisani, utvrđivanja da li su prijetnje i ranjivosti pravilno identifikovane, kao i kontrolu ispravnosti procjene nekog resursa, vrednovanja vjerovatnoće prijetnje, stepena ranjivosti i stepena uticaja ranjivosti. Direkcija bi, ukoliko ima primjedbe, kontaktirala zadužene zaposlene iz organizacionih jedinica, i davala im uputstva za potrebne izmjene prije ponovnog slanja fajla.

Nedostaci opisanog načina vođenja Registra rizika po bezbjednost informacija su bili brojni i vrlo ozbiljni, [57]. Nije postojala jedinstvena baza za čuvanje podataka o rizicima po bezbjednost informacija u Centralnoj banci. Podaci su čuvani u obliku excelovih fajlova na radnoj stanici ovlašćenog lica iz Direkcije. U skladu sa tim, nije postojala konzistentnost podataka, niti bilo kakva mogućnost automatskog generisanja izvještaja na osnovu evidentiranih podataka. Dalje, nije postojala katalogizacija niti unificiranost informacijskih resursa, kategorija resursa, prijetnji i ranjivosti. Prilikom unosa, svaka organizaciona jedinica je evidentirala pomenute pojmove onako kako ih je ona percipirala. Ovakvim

načinom evidencije, moglo se desiti da dvije različite samostalne organizacione jedinice isti informacijski resurs, kao i za njega vezane ranjivosti i prijetnje, potpuno drugačije evidentiraju, tako da se prilikom analize pojave kao dva različita resursa. Takođe, moglo se desiti da se na spisku nađe nešto što se uopšte ne može identifikovati kao informacijski resurs. Dalje, spisak mogućih prijetnji i ranjivosti definisanih na takav način je bio veoma dugačak. U tom smislu i evidentiranje je bilo prilično složeno, kao i posao pregleda i korekcije pomenutih podataka, a da ne govorimo o analizi dobijenih podataka i o kreiranju neophodnih izvještaja na osnovu njih.

Imajući u vidu značaj podataka o informacijskim resursima Centralne banke i potencijalnim rizicima po bezbjednost informacija, jasno je da je bilo neophodno napraviti informacioni sistem koji će omogućiti jednostavno evidentiranje, praćenje i izvještavanje o ovim rizicima. Poseban izazov predstavljalo je integrisanje razvijenog informacionog sistema za upravljanje rizicima po bezbjednost informacija sa postojećim informacionim sistemom Centralne banke Crne Gore, Glavnim bankarskim sistemom, koji predstavlja informatičku podršku drugim poslovnim procesima.

4.4. Model informacionog sistema za upravljanje rizicima po bezbjednost informacija

Razvoj informacionog sistema je kompleksan i dugotrajan proces koji se realizuje kroz niz faza i aktivnosti, [16], [17], [18]. Postoje različiti modeli razvoja informacionog sistema i svaki od njih ima svoje prednosti i nedostatke, [3]. U skladu sa konkretnim zahtjevom za razvoj informacionog sistema, bira se model koji po svojim karakteristikama najbolje odgovara. Imajući u vidu da su poslovni procesi koje treba da podrži informacioni sistem za upravljanje rizicima po bezbjednost informacija jasno definisani i da u toku realizacije neće biti izmjena u njihovom funkcionisanju, izabrala sam linearnu metodologiju razvoja zasnovanu na Vodopad modelu (*Waterfall*) životnog ciklusa. Osobenost ovog modela, [2], je da se faze razvoja informacionog sistema realizuju strogo po sekvencama i da se naredna faza može započeti tek pošto se tekuća završi. Greške iz prethodnih faza koje se otkriju u tekućoj fazi, moraju se otkloniti i dokumentovati vraćanjem u prethodne faze i prolaskom kroz sve prethodne faze. Primjenjujući ovaj model, razvoj informacionog sistema se realizuje se kroz pet faza, [4].

Prva faza je **analiza i specifikacija zahtjeva**. U okviru nje se sprovodi detaljno snimanje realnog sistema, proučava se zahtjev korisnika i analizira postojeće stanje, [3]. Identifikuju se zahtjevi koje informacioni sistem treba da zadovolji u smislu funkcionalnosti, performansi, jednostavnosti korišćenja i slično. Rezultat rada u ovoj fazi, [3] i [4], treba da bude dokument koji sadrži preciznu i detaljnu specifikaciju informacionih zahtjeva. Dokument treba da bude sažet i jasan i da sadrži opis funkcionalnosti koje informacioni sistem treba da ima, [4].

Prilikom razvoja informacionog sistema, koji je predmet ove teze, analizom je utvrđeno da, za svaku samostalnu organizacionu jedinicu, Registar rizika treba koncipirati kao dokument koji prolazi kroz različite statuse, tako da u svakom od statusa različiti tipovi korisnika imaju pravo pristupa dokumentu, kao i pravo da sprovode različite akcije nad dokumentom. Nakon kreiranja, dokument treba da bude u statusu *Evidentiran*. U ovom statusu dokument je "vidljiv" samo za zaposlene iz organizacione jedinice za koju je kreiran dokument i podaci u njemu se mogu ažurirati, [57]. Svaka samostalna organizaciona jedinica ima pristup samo dokumentima koje kreira njen ovlašćeni zaposleni, pri čemu svaka organizaciona jedinica može kreirati samo jedan dokument za jedan period izvještavanja, a to je kalendarska godina. Kad zaposleni, koji je kreirao dokument, smatra da je rad na njemu završen, on ga eksplicitnom akcijom prosljeđuje Direkciji, koja je nadležna za upravljanje rizikom po bezbjednost informacija, na uvid, dodjeljujući mu novi status. Direkcija treba da ima pristup dokumentima svih samostalnih organizacionih jedinica poslije prosljeđivanja, ali bez prava ažuriranja ili brisanja podataka. Ukoliko uvidom utvrdi da ima nekih nepravilnosti koje treba ispraviti, Direkcija ima mogućnost da eksplicitnom akcijom vrati dokument u prvobitni status, odnosno na doradu organizacionoj jedinici koja je dokument kreirala i proslijedila. O toj akciji treba da postoji mail notifikacija i da bude upućena onom licu iz organizacione jedinice koje je proslijedilo dokument. Dokument, koji predstavlja Registar rizika za samostalnu organizacionu jedinicu, kreira se u skladu sa Metodologijom. Postojeće stanje je podrazumijevalo vođenje evidencije o rizicima po bezbjednost informacija u obliku excel fajlova, kao što je objašnjeno u poglavlju 4.3.

Druga faza, **projektovanje informacionog sistema**, obuhvata logičko i fizičko projektovanje, [4].

Pod logičkim projektovanjem informacionog sistema podrazumijevamo modeliranje realnog sistema, [4]. Ishod treba da bude model primjenjiv za razne načine implementacija. Prilikom modeliranja, prema [14] i [15], projektant ima zadatak da identifikuje funkcije koje informacioni sistem treba da realizuje,

kao i sekvence u kojima se funkcije realizuju, zatim podatke koji treba da se skladište u bazi podataka i da se obrađuju u sistemu, i na kraju, informacije koje informacioni sistem treba da obezbijedi za potrebe korisnika. Dakle, realni sistem se modelira tako što se uoče ključne osobine sistema, a zatim se one predstavljaju modelom, [3]. Prema [4] i [5], logičko projektovanje obuhvata modeliranje podataka i modeliranje procesa.

Model podataka je strukturisani skup informacija o prošlosti i sadašnjosti sistema, potreban da bi se pod dejstvom budućih poznatih ulaza odredili budući izlazi iz sistema, [19]. Model podataka obuhvata definisanje podataka, veza između njih, njihovog značenja i ograničenja koja nad njima treba da postoje. Postoje razni modeli podataka. Prilikom modeliranja podataka u toku razvoja informacionog sistema za upravljanje bezbjednošću informacija korišćen je model entiteti – veze (ER – Entity Relationship) i kreirani model je prikazan grafički korišćenjem ER dijagrama. Karakteristika modela entiteti – veze je da prikazuje odnos (vezu) između podataka (1:1, 1:M, M:N), kao i grupe podataka – logičke cjeline. Opis skupa podataka u modelu je simbolički odnosno konceptualni i njegova šema je lako razumljiva i za projektanta i za korisnika, [7], [8], [9], [10], [11], [12], [13]. Prema [8] i [9], koncepti ovog modela su: entitet, koji za korisnika predstavlja „objekat" o kojem treba voditi podatke, atribut, koji opisuje svojstva pojedinog objekta i predstavlja sadržaj zapisa o objektu, veza, koja opisuje odnos između objekata, i zavisnost – (ne)samostalnost objekta.

Kreirani model podataka za razvoj informacionog sistema za upravljanje rizicima po bezbjednost informacija prikazan je na Slici 1. Entiteti su organizovani tako da se podaci o dokumentima smještaju u tabele rrb_zaglavlje, iz koje se spušta ključ u tabelu rrb_resurs, gdje se nalazi popis informacijskih resursa za samostalnu organizacionu jedinicu, a dalje se ključ spušta u tabelu rrb_rizik, gdje se za svaki resurs iz tabele rrb_resurs, upisuju prijetnje i ranjivosti koje definišu rizik. Dakle, imamo master detail vezu između tabela rrb_zaglavlje i rrb_resurs, kao i između tabela rrb_resurs i rrb_rizik. Tabela rrb_resurs ima spoljašnje ključeve na tabele rrb_dostupnost, rrb_integritet i rrb_povjerljivost, jer su to tabele u kojima su smještene vrijednosti za povjerljivost, integritet i dostupnost, definisane u Metodologiji, kao i prema tabeli rrb_kategorija_resursa, sa spiskom kategorija u koje se resursi mogu svrstati, takođe iz Metodologije. Tabela rrb_rizik ima spoljašnje ključeve prema tabelama rrb_prijetnje i rrb_ranjivosti, u kojima će biti smještani spiskovi mogućih prijetnji i ranjivosti koje su za određenu kategoriju resursa identifikovali ili Direkcija ili samostalna organizaciona jedinica. Na ovaj način bi se izvršila katalogizacija prijetnji i ranjivosti za određenu kategoriju resursa. Takođe, tabela ima spoljašnji

ključ prema tabeli rrb_opcija u koju će se smještati podaci o mogućim opcijama za tretman rizika, koje su definisane u Metodologiji.

Pod procesom podrazumijevamo skup aktivnosti koje su međusobno logički povezane tako da izazivaju promjene stanja u informacionom sistemu i na taj način na osnovu ulaznih podataka generišu izlaze iz sistema, [14] i [15]. Skup logički povezanih poslovnih procesa predstavlja poslovnu funkciju, [7]. Funkcije i procesi su nezavisni od organizacione strukture, [1]. Model procesa je instrument pomoću koga se opisuje dinamika sistema, odnosno uticaj ulaza na stanje i izlazne informacije preko programa nad definisanim modelom podataka, [19]. Model procesa opisuje niz elementarnih aktivnosti i tok podataka između njih, [19]. U ovoj magistarskoj tezi upotrijebljena je strukturna sistemska analiza (SSA - Structured Systems Analysis) za dekompoziciju procesa odnosno kreiranje modela procesa. Prema [6], SSA je metoda koja omogućava savladavanje kompleksnosti sistema putem hijerarhijske dekompozicije po unaprijed datom kriterijumu. Upotrebljava se za kreiranje strukturnog modela procesa sistema, [6], [12], [14]. SSA se realizuje kroz postupno razlaganje složenog sistema na skupove komponenti manje složenosti, zatim utvrđivanje međusobne zavisnosti komponenti, nezavisno kreiranje komponenti i, na kraju, integraciju komponenti u jedinstveni sistem. Kao ishod primjene SSA dobija se funkcionalna specifikacija, [4]. Drugim riječima, za izradu funkcionalne specifikacije potrebno je definisati funkciju odnosno procese. Svaka funkcija (proces) ima podfunkcije (podprocese), a ova svoje podfunkcije (podprocese), sve do elementarnih procesa koji nemaju svoje podprocese. Efekat dejstava podprocesa je postizanje ostvarenje funkcije u cjelini. SSA metoda je koncipirana tako da svaki proces obrade podataka mora da započinje nekim ulaznim tokom podataka, nakon čega se logički jasno i jednoznačno definiše obrada, što omogućava dobijajanje jednoznačno definisanih rezultata, [6]. To znači da SSA metod tretira informacioni sistem kao funkciju (proces obrade) koja, na bazi ulaznih, generiše izlazne podatke. Poslovni procesi koji upravljaju resursima realnog sistema i podaci u realnom sistemu su u potpunosti ispreplijetani što se jasno vidi prilikom njihovog modeliranja. Fizičko projektovanje, [5], podrazumijeva primjenu logičkog projekta na konkretne servere i bazu podataka. Na kraju ove faze kreira se projektna specifikacija sistema koja mora biti takva da zadovoljava zahtjeve definisane u prvoj fazi. Dekompozicija poslovnog procesa upravljanje rizicima po bezbjednost informacija prikazana je na Slici 2.

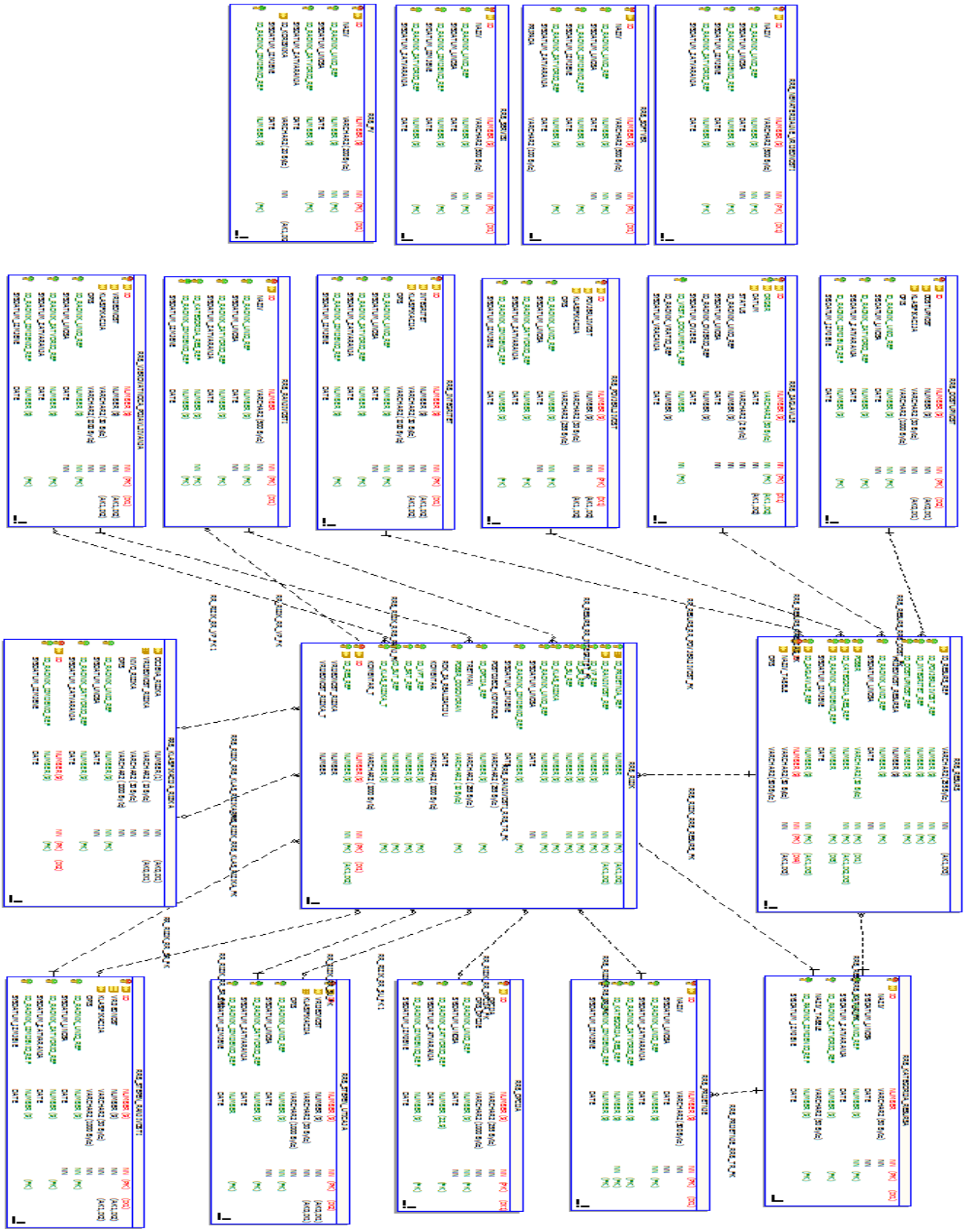
Programiranje i testiranje modula – obuhvata oblikovanje opisa šeme baze podataka u jeziku sistema za upravljanje bazom podataka (SUBP), pisanje programskog koda na osnovu projektne specifikacije i testiranje kreiranih modula, podešavanje fizičke organizacije baze podataka i postizanje zadovoljavajućih performansi, realizaciju i obezbjeđenje postupaka zaštite informacionog sistema, kao i izradu korisničke dokumentacije, [3]. Ako se otkriju greške u kodu pri testiranju modula, otkriva se što izaziva problem i ispravljaju se greške.

Testiranje sistema je treća faza i njoj se pristupa nakon generisanja programskog koda. Sistem testiraju krajnji korisnici i to sa dva aspekta, sa aspekta usaglašenosti postavljenog informacionog sistema sa postavljenim zahtjevima, kao i sa aspekta tačnosti rada ugrađenih funkcionalnosti. Takođe, u ovoj fazi korisnici mogu ispostaviti određene zahtjeve za doradu koji nijesu na početku traženi, ukoliko ti zahtjevi nijesu u koliziji sa postavljenom koncepcijom sistema.

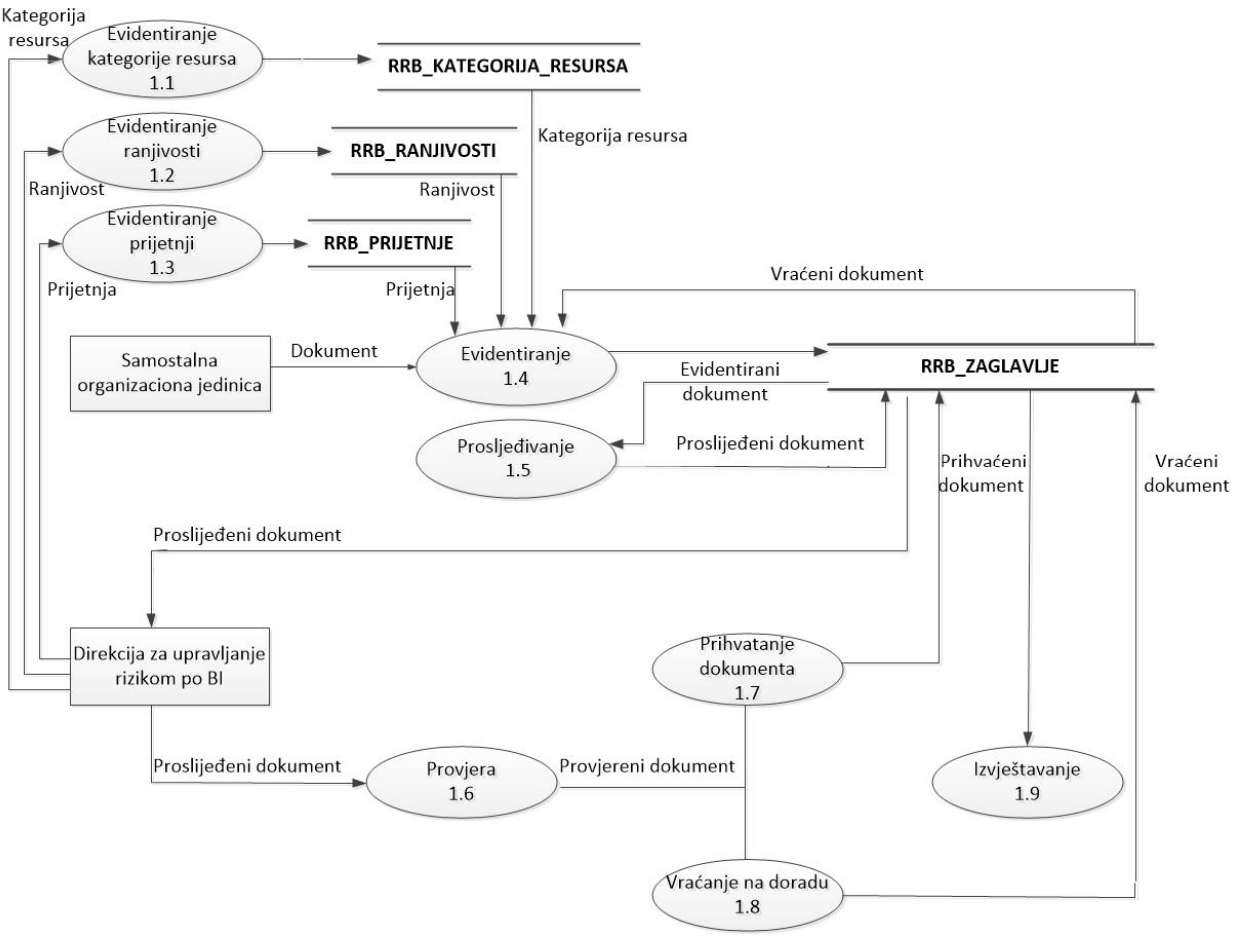
Faza **stavljanja u funkciju** slijedi nakon što se ustanovi da razvijeni informacioni sistem zadovoljava postavljene zahtjeve i da tačno funkcioniše.

Faza **održavanja sistema** obuhvata intervencije na sistemu nakon njegovog stavljanja u funkciju. Intervencije se odnose na otklanjanje zaostalih grešaka, unapređenje postojećih funkcionalnosti, kao i na uvođenje novih.

Da bi se iz informacionog sistema mogle dobiti informacije koje će biti relevantne za donošenje odluka, informacioni sistem treba koncipirati iz prespektive najvišeg nivoa odlučivanja, [1]. Takođe, informacioni sistem treba projektovati tako da u najmanjoj mogućoj mjeri zavisi od promjenjivih komponenti organizacije kakva je, na primjer, organizaciona struktura. Iz tog razloga, informacioni sistem se projektuje tako da omogućava informatičku podršku ključnim poslovnim procesima koji su konstantni za određeni domen poslovanja organizacije.



Slika 1: Logička šema baze podataka – ER dijagram



Slika 2: Dekompozicija procesa upravljanje rizicima po bezbjednost informacija

4.4.1. Ključni razlozi za primjenjivost modela za razne implementacije

U ovoj magistarskoj tezi je predložen jednostavan model za razvoj informacionog sistema za upravljanje rizicima po bezbjednost informacija. Podaci o informacijskim resursima, rizicima, tretmanima rizika i ocjeni efektivnosti kontrola smještaju se u tri tabele koje su u vezi master – detail – detail. Podaci koji se odnose na regulativu o upravljanju rizicima smještaju se u potreban broj tabela – šifarnika, na koje se prethodne tri tabele referenciraju. Ukoliko se model implementira u okruženju gdje su osnovni poslovni procesi već pokriveni informacionim sistemom, gore navedene tabele se referenciraju na postojeće tabele koje sadrže podatke o zaposlenima, radnim mjestima i organizacionoj strukturi. Dakle, sve tabele možemo podijeliti u tri grupe: tabele sa podacima koji se odnose na informacijske resurse, rizike i tretmane tih rizika, odnosno na podatke koji se stalno prikupljaju i ažuriraju, tabele sa podacima koji su vezani za regulativu upravljanja rizicima po bezbjednost informacija i na tabele koje sadrže podatke o osnovnim resursima organizacije. Na ovaj način je dobijen model koji se može upotrijebiti za

projektovanje informacionog sistema za upravljanje rizikom po bezbjednost informacija nezavisno od regulative kojim se uređuje upravljanje rizicima i organizacione strukture preduzeća.

4.5. Integracija razvijenog informacionog sistema za upravljanje rizicima po bezbjednost informacija u Centralnoj banci sa postojećim informacionim sistemom

S obzirom da u Centralnoj banci Crne Gore postoji aplikativni sistem, Glavni bankarski sistem, [30], pomoću koga su automatizovani ključni poslovni procesi u Centralnoj banci, informacioni sistem za upravljanje rizikom po bezbjednost informacija trebalo je modelirati tako da se integriše sa Glavnim bankarskim sistemom. Imajući u vidu da se u svaku tabelu baze podataka informacionog sistema koji se kreira, prilikom evidentiranja, ažuriranja ili zatvaranja zapisa upisuje zaposleni koji je bio prijavljen na aplikaciju prilikom sprovođenja tih akcija, kao i da se u neke tabele upisuje šifra organizacione jedinice i šifra radnog mjesta zaposlenog, pomenute tabele treba referencirati na postojeće tabele sa tim podacima. U skladu sa [30], integracija aplikativnih modula se realizuje na nivou baze podataka i na aplikativnom nivou. Primjenjujući model integracije aplikativnih modula koji je predložen u referenci [30], integracija na nivou baze podataka je sprovedena kreiranjem spoljašnjih ključeva prema tabelama ke_org, kl_radnik i ke_poslovi nad odgovarajućim atributima. U tabeli ke_org nalaze se zapisi o organizacionoj strukturi Centralne banke Crne Gore, u tabeli kl_radnik nalaze se zapisi o svim zaposlenim i drugim fizičkim licima koji su u vezi sa Centralnom bankom, a u tabeli ke_poslovi nalazi se spisak svih sistematizovanih radnih mjesta u Centralnoj banci. Integracija na aplikativnom nivou, kao u [30], izvršena je tako što se liste vrijednosti za radna mjesta, organizacione jedinice kao i za informacijske resurse, u zavisnosti od kategorije resursa, kreiraju od podataka koji su evidentirani kroz aplikacije Glavnog bankarskog sistema.

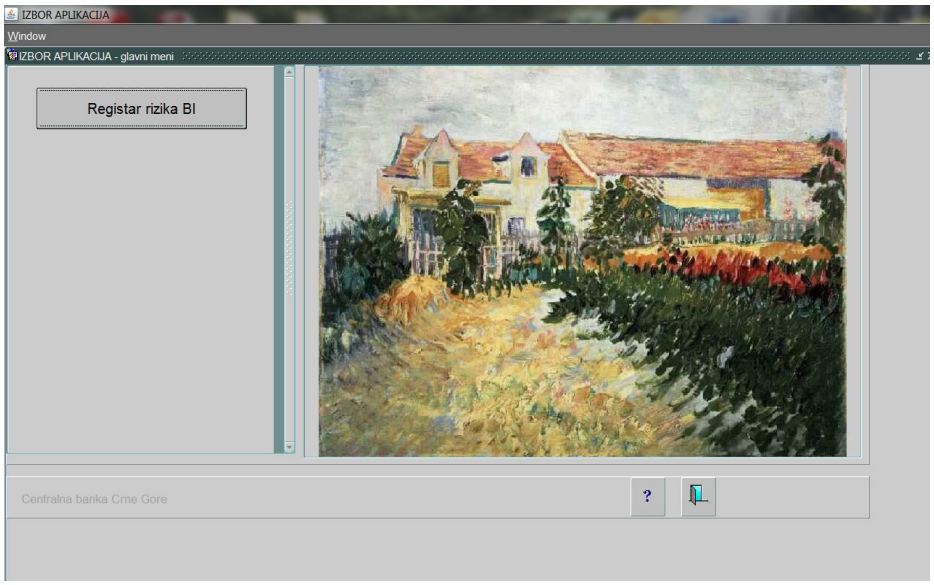
Dakle, u toku projektovanja informacionog sistema za upravljanje rizicima po bezbjednost informacija, osmišljena je i integracija tog informacionog sistema sa postojećim informacionim sistemom, Glavnim bankarskim sistemom. Time je omogućeno potpuno korišćenje svih postojećih podataka i prethodno automatizovanih poslovnih procesa.

5. Funkcionalnosti i značaj informacionog sistema za upravljanje rizicima po bezbjednost informacija u Centralnoj banci Crne Gore

Razvijeni informacioni sistem za upravljanje rizicima po bezbjednost informacija, nazvan Registar rizika BI, stavljen je u funkciju u Centralnoj banci Crne Gore i integrisan je sa postojećim Glavnim bankarskim sistemom (Slika 3). Registar rizika BI je namijenjen Direkciji za upravljanje operativnim rizikom, bezbjednošću informacija i kontinuitetom poslovanja (u daljem tekstu Direkcija), kao i svim samostalnim organizacionim jedinicama Centralne banke Crne Gore (u daljem tekstu samostalne OJ). Svaka samostalna OJ ima svog predstavnika koji je zadužen za dostavljanje podataka o rizicima po bezbjednost informacija za tu OJ, za zadati period.

Pritiskom na dugme, na ekranu se pojavljuje glavni meni informacionog sistema (Slika 4). Na glavnom meniju informacionog sistema su prikazane njegove funkcije :

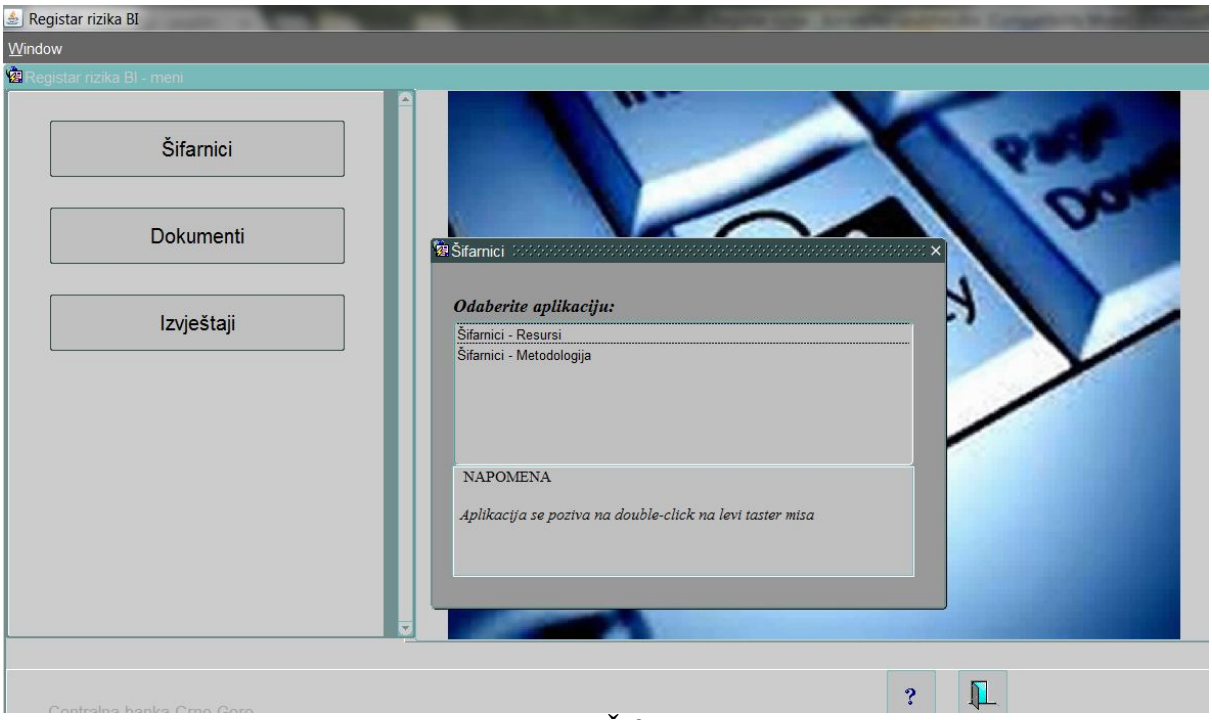
- **Šifarnici –** omogućava održavanje šifarnika;
- **Dokumenti –** omogućava evidentiranje i pregled dokumenata koji obuhvataju Registar rizika po bezbjednost informacija, kao i tretman tih rizika i ocjenu efektivnosti uvedenih kontrola, za svaku samostalnu OJ za period definisan Metodologijom za upravljanje rizicima po bezbjednost informacija Centralne banke Crne Gore (Metodologija);
- **Izvještaji –** izvještavanje na osnovu evidentiranih podataka u dokumentima koje su samostalne organizacione jedinice Centralne banke Crne Gore proslijedile Direkciji.



Slika 3: Informacioni sistem za upravljanje rizicima po bezbjednost informacija

Slika 4: Glavni meni informacionog sistema *Registar rizika BI*

5.1.Šifarnici



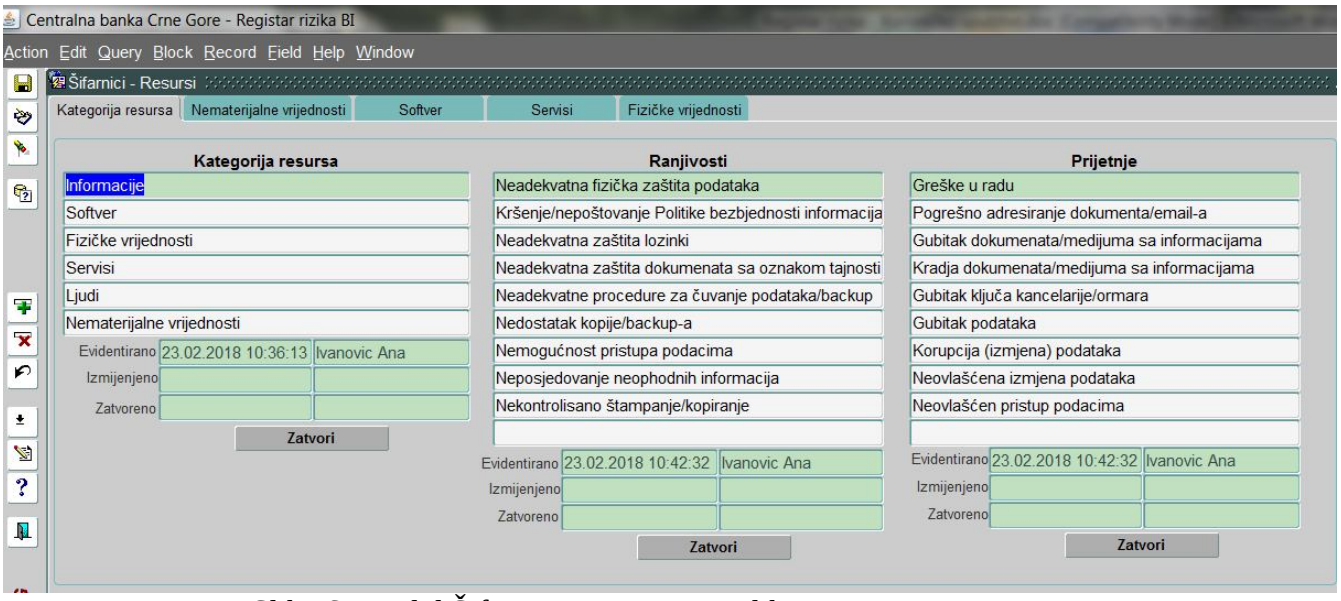
Slika 5: Šifarnici

Funkcija **Šifarnici** je namijenjena Direkciji. Predstavnici samostalnih OJ prilikom kreiranja dokumenta Registar i Plan tretmana rizika po bezbjednost informacija koriste liste vrijednosti sa podacima iz šifarnika. Ova funkcija podsistema se implementira kroz dva modula:

- **Šifarnici – Resursi**
- **Šifarnici – Metodologija**

5.1.1. Šifarnici – Resursi

Modul Šifarnici – Resursi je realizovan kao aplikativna forma podijeljena na više stranica sa posebnim aplikacijama. Na taj način ovaj modul omogućava evidentiranje više šifarnika. Dvostrukim klikom miša na modul ***Šifarnici – Resursi*** otvara se prozor modula (Slika 4). Na prvoj stranici (Slika 6) nalazi se aplikacija koja omogućava evidentiranje kategorija resursa, kao i definisanje određenog seta prijetnji i ranjivosti koje se mogu javiti za tu kategoriju resursa.



Slika 6: Modul Šifarnici – Resursi – aplikacija Kategorija resursa

Na njoj uočavamo polja:

- **Kategorija resursa**
- **Ranjivosti**
- **Prijetnje**

Ova polja su obavezna, tekstualna polja koja popunjava korisnik.

Na sljedećoj stranici nalazi se aplikacija koja omogućava evidentiranje resursa koji spadaju u kategoriju Nematerijalne vrijednosti (Slika 7). U ovoj aplikaciji uočavamo polja:

- **Naziv** – obavezno, tekstualno polje koje popunjava korisnik;

Na trećoj stranici nalazi se aplikacija koja omogućava evidentiranje resursa koji spadaju u kategoriju Softver (Slika 8). U ovoj aplikaciji uočavamo polja:

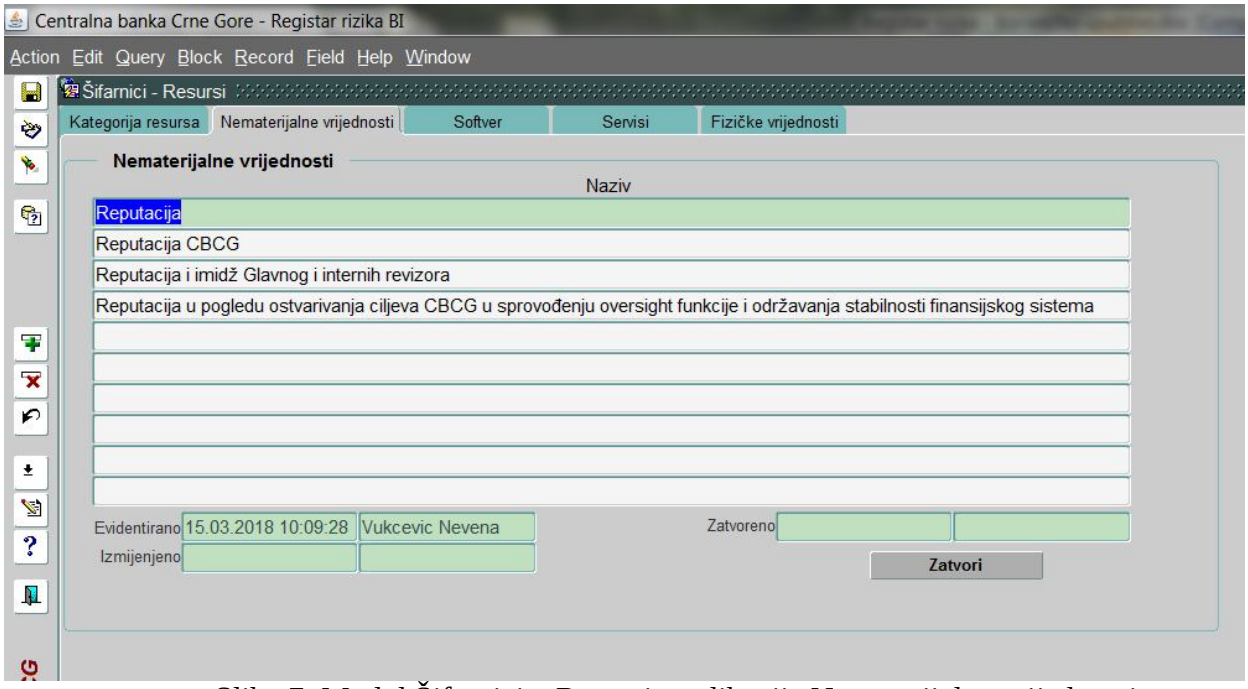
- **Naziv softvera** – obavezno, tekstualno polje koje popunjava korisnik;
- **Pripada** – neobavezno tekstualno polje koje popunjava korisnik, a popunjava se u slučaju kada je navedeni softver dio neke veće aplikativne cjeline;

Na četvrtoj stranici nalazi se aplikacija koja omogućava evidentiranje resursa koji spadaju u kategoriju Servisi (Slika 9). U ovoj aplikaciji uočavamo polja:

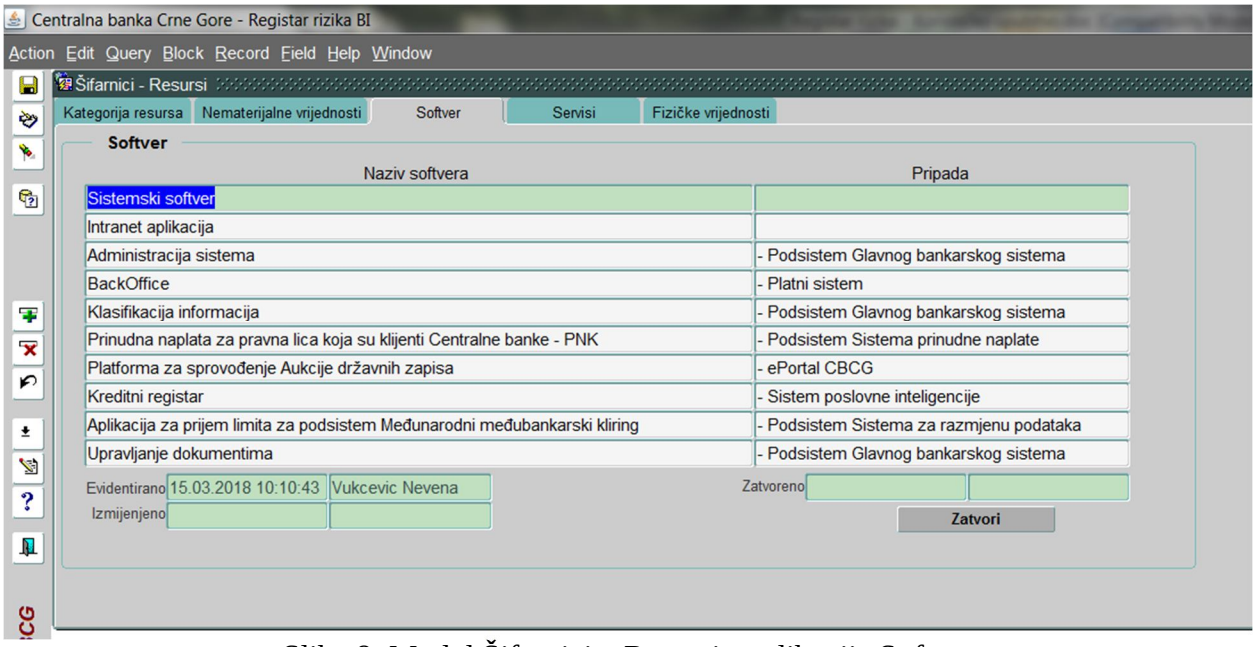
- **Naziv** – obavezno, tekstualno polje koje popunjava korisnik;

Na petoj stranici nalazi se aplikacija koja omogućava evidentiranje resursa koji spadaju u kategoriju Fizičke vrijednosti, a predstavlja dopunu resursima koji se uzimaju iz tabele Osnovna sredstva (Slika 10). U ovoj aplikaciji uočavamo polja:

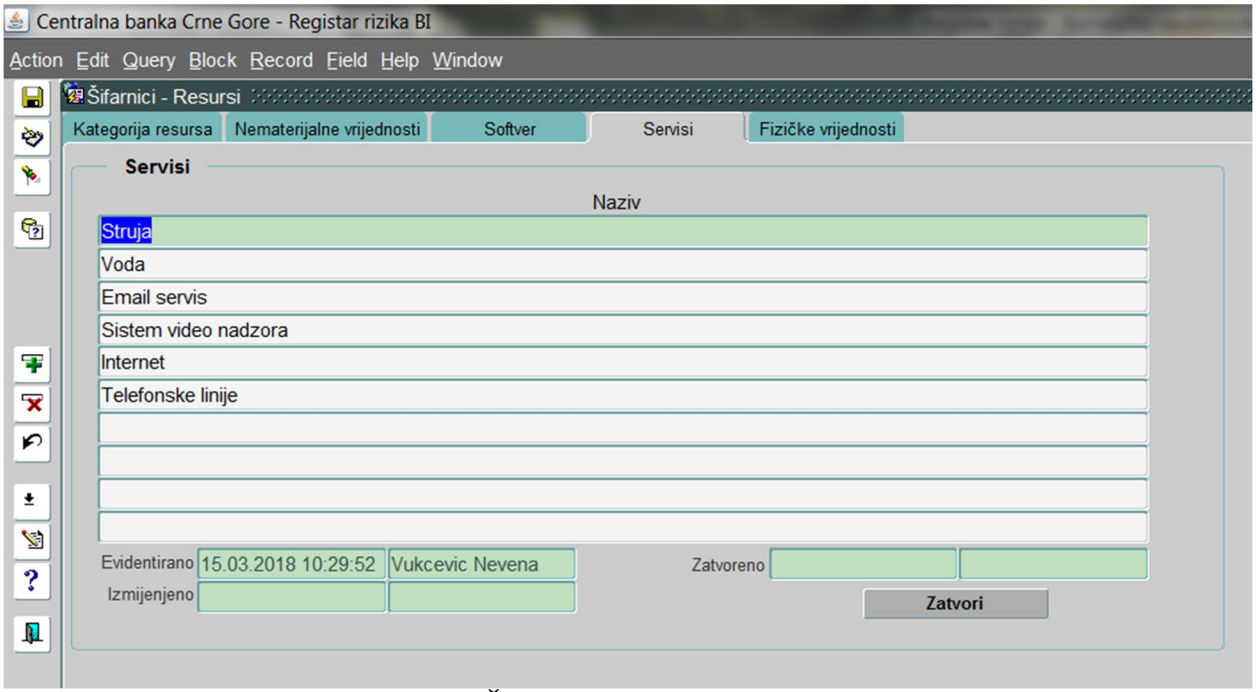
- **Šifra** – polje koje se popunjava automatski;
- **Naziv** – obavezno, tekstualno polje koje popunjava korisnik;



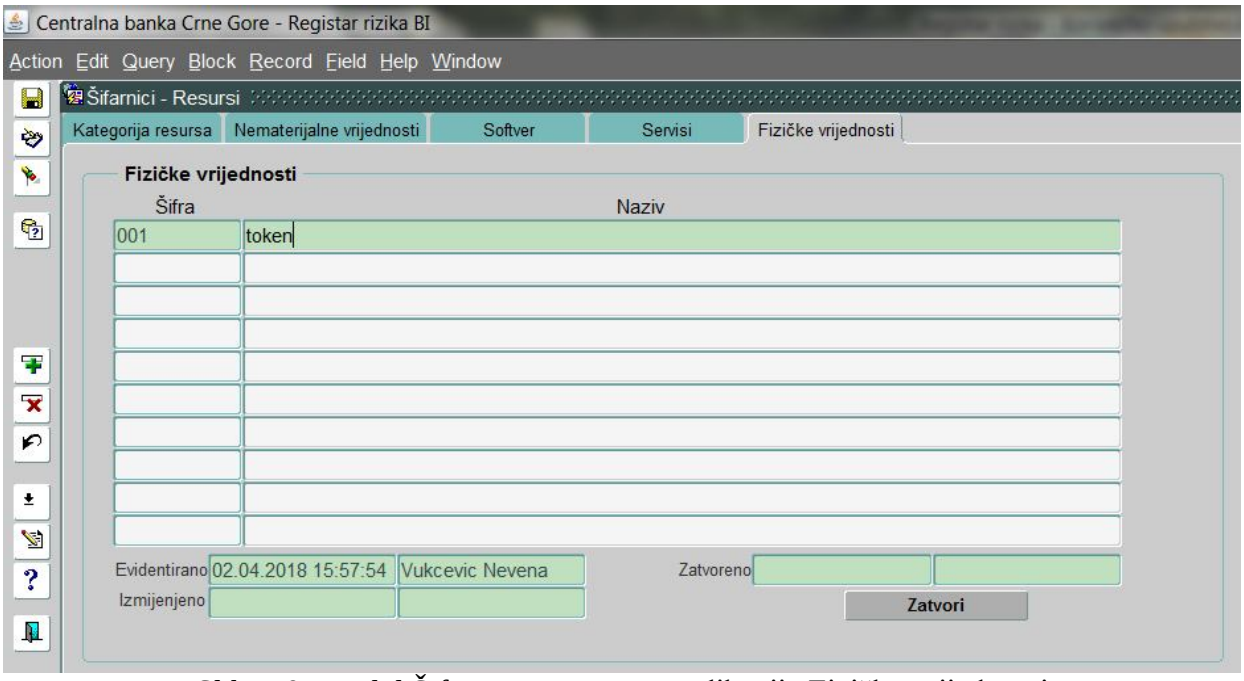
Slika 7: Modul Šifarnici – Resursi - aplikacija Nematerijalne vrijednosti



Slika 8: Modul Šifarnici – Resursi - aplikacija Softver



Slika 9: Modul Šifarnici – Resursi - aplikacija Servisi



Slika 10: Modul Šifarnici – Resursi - aplikacija Fizičke vrijednosti

Na svakoj stranici uočavamo polja:

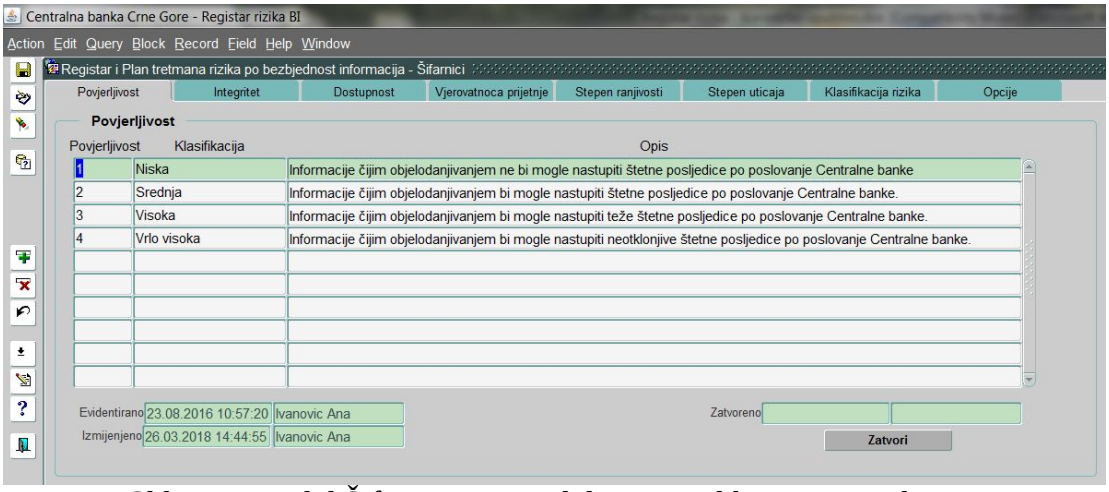
- **Evidentirano –** prilikom evidentiranja zapisa, ova polja se automatski popunjavaju sistemskim datumom i imenom zaposlenog koji je evidentirao;
- **Izmijenjeno –** prilikom ažuriranja zapisa, ova polja se automatski popunjavaju sistemskim datumom ažuriranja i imenom zaposlenog koji je ažurirao zapis;
- **Zatvoreno –** prilikom zatvaranja zapisa, ova polja se automatski popunjavaju sistemskim datumom zatvaranja i imenom zaposlenog koji je zatvorio zapis,

Kao i dugme

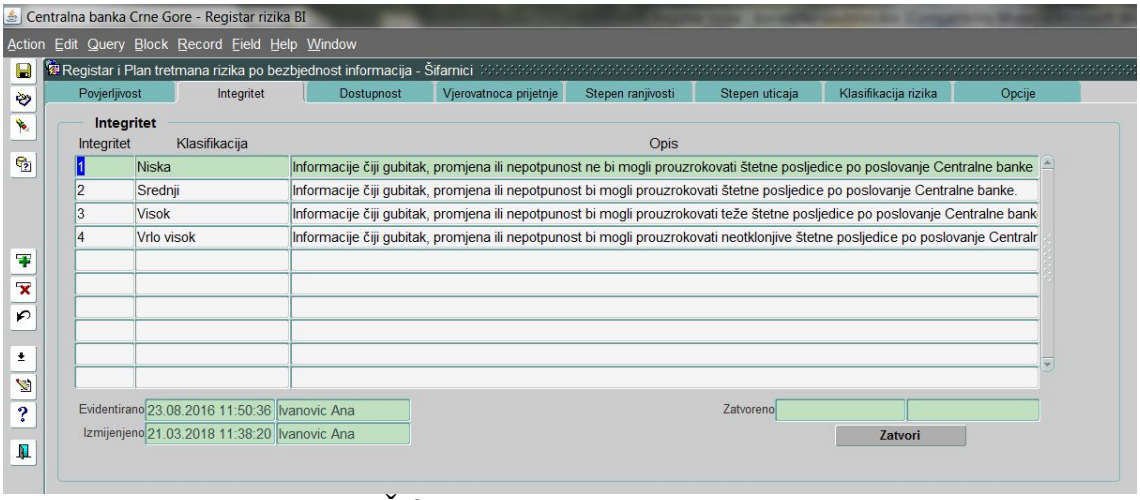
- **Zatvori –** pritiskom na ovo dugme zapis postaje neaktivan, iako je i dalje vidljiv na formi. Zatvoreni zapisi se ne vide u listama vrijednosti.

5.1.2. Šifarnici – Metodologija

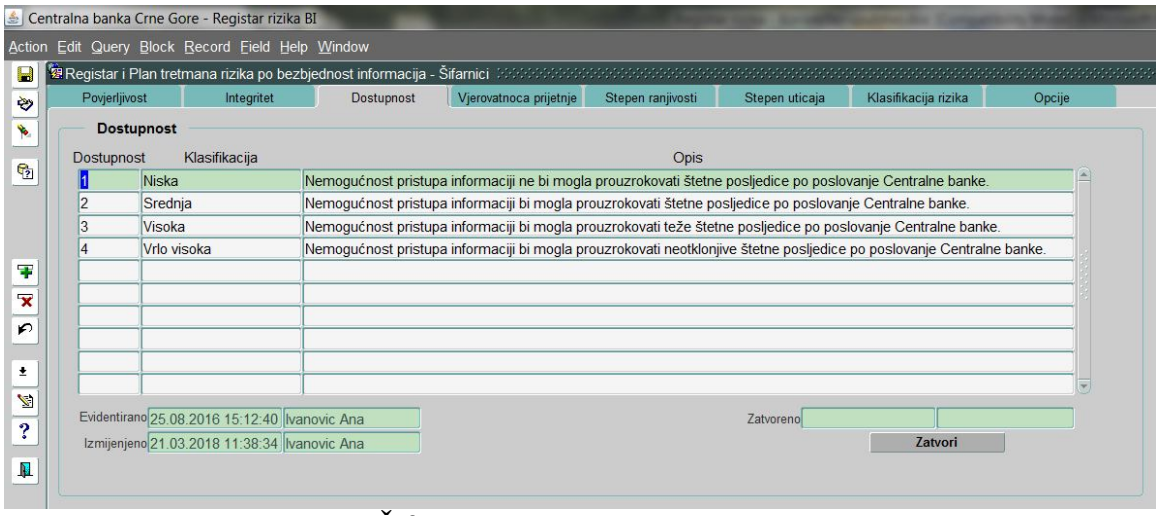
Modul Šifarnici – Metodologija je realizovana kao aplikativna forma podijeljena na više stranica sa posebnim aplikacijama. Na taj način ovaj modul omogućava evidentiranje više šifarnika koji su definisani u Metodologiji, a odnose se na procjenu vrijednosti resursa - šifarnik povjerljivosti, šifarnik integriteta i šifarnik dostupnosti, na vrednovanje ranjivosti i prijetnji - šifarnik vjerovatnoće pojavljivanja prijetnje, šifarnik stepena ranjivosti i šifarnik stepena uticaja, na vrednovanje rizika - šifarnik za klasifikaciju rizika, kao i na opcije za tretman rizika – šifarnik opcija. Dvostrukim klikom miša na modul ***Šifarnici – Metodologija*** otvara se prozor modula (Slika 11).



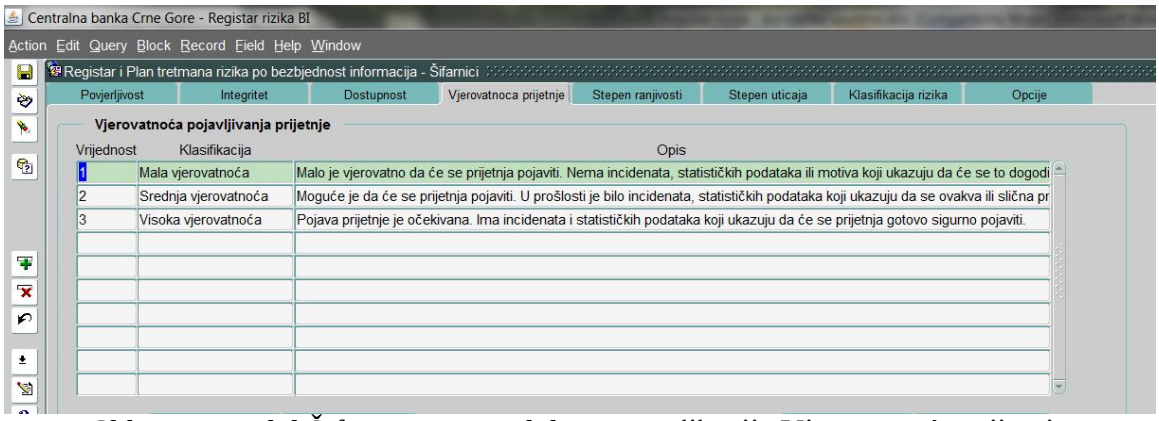
Slika 11: Modul Šifarnici – Metodologija - aplikacija Povjerljivost



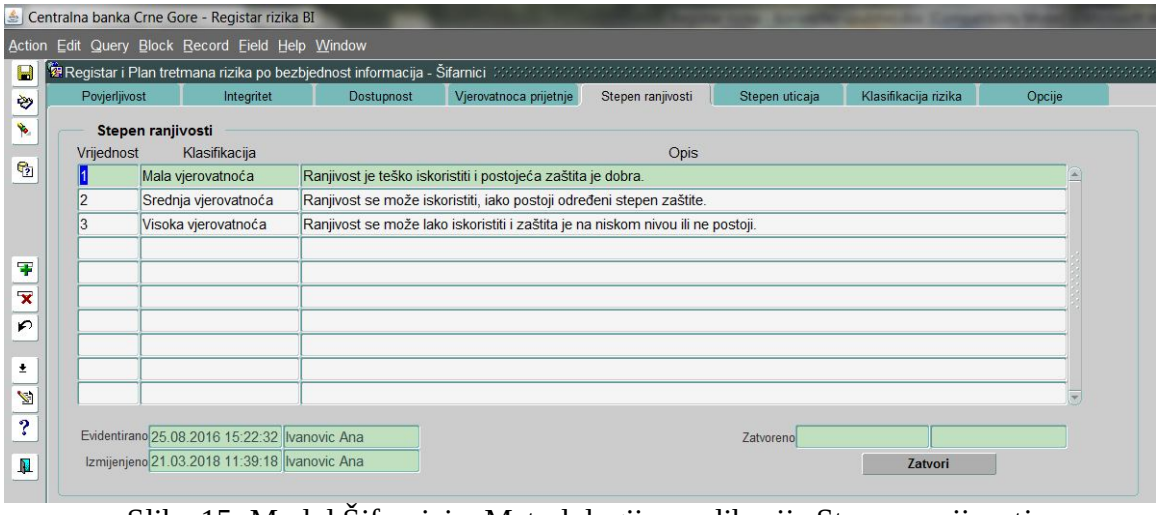
Slika 12: Modul Šifarnici – Metodologija - aplikacija Integritet



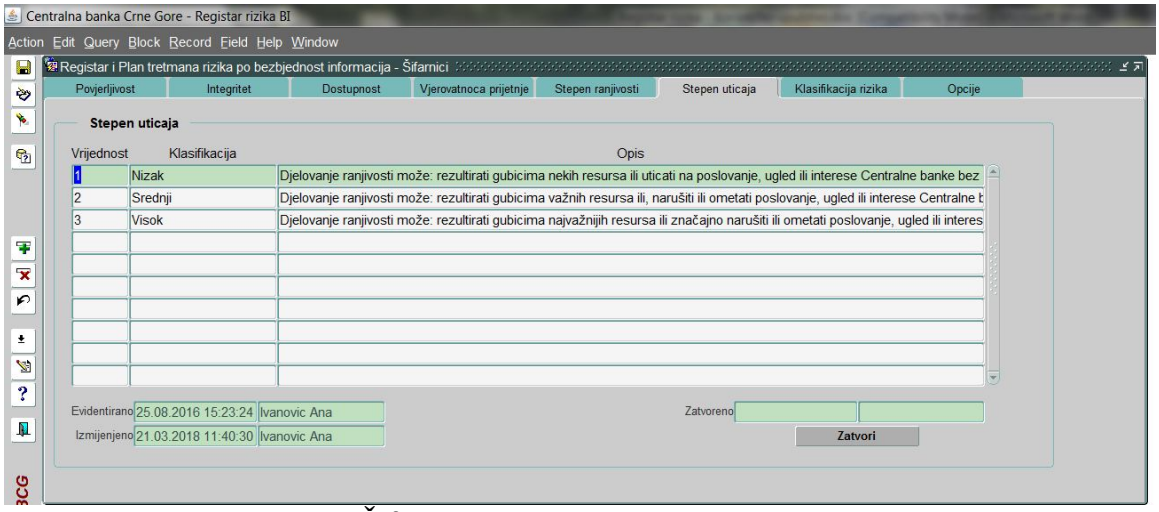
Slika 13: Modul Šifarnici – Metodologij***a*** - aplikacija Dostupnost



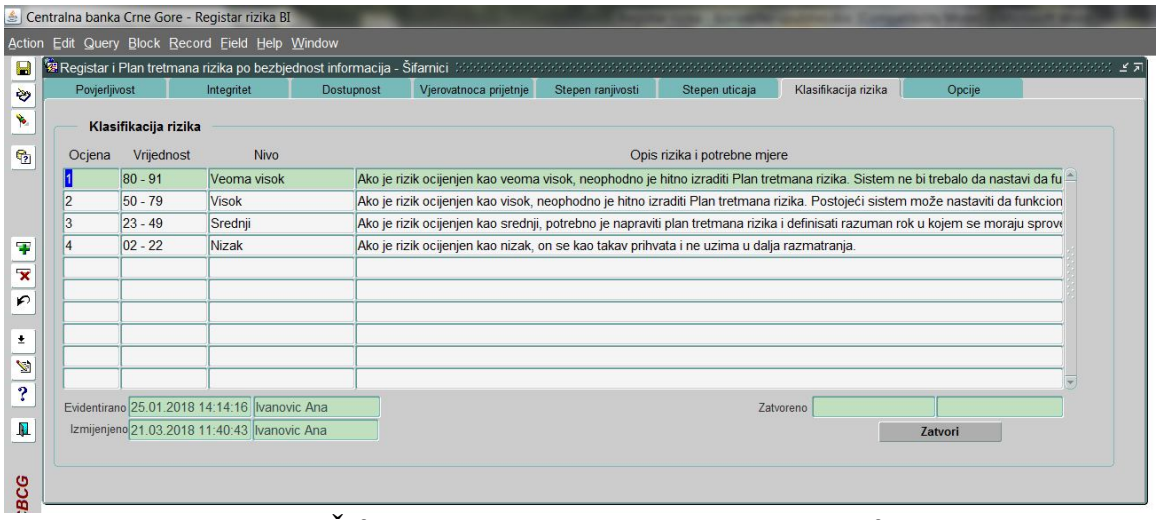
Slika 14: Modul Šifarnici – Metodologija - aplikacija Vjerovatnoća prijetnje



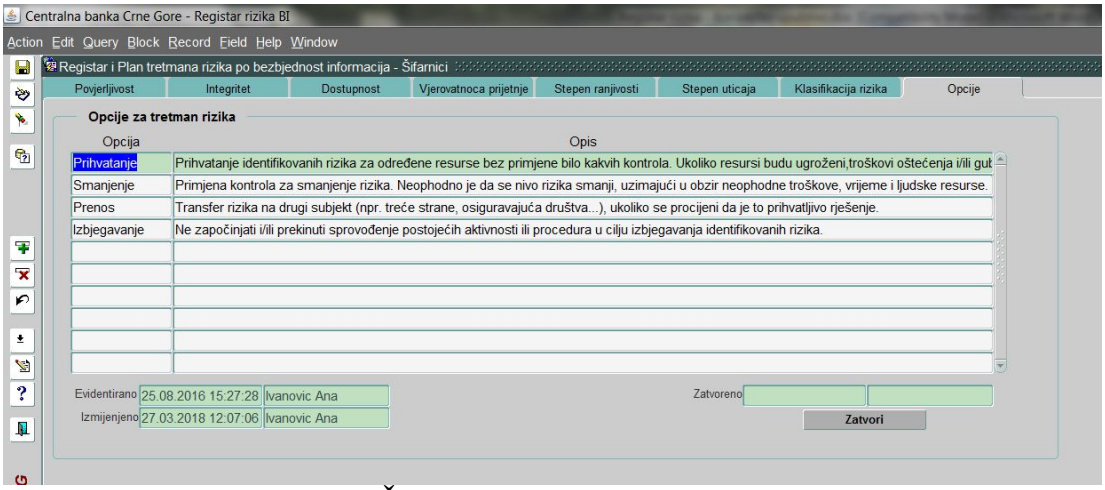
Slika 15: Modul Šifarnici – Metodologija - aplikacija Stepen ranjivosti



Slika 16: Modul Šifarnici – Metodologija - aplikacija Stepen uticaja



Slika 17: Modul Šifarnici – Metodologija - aplikacija Klasifikacija rizika



Slika 18: Modul Šifarnici – Metodologija - aplikacija Opcije

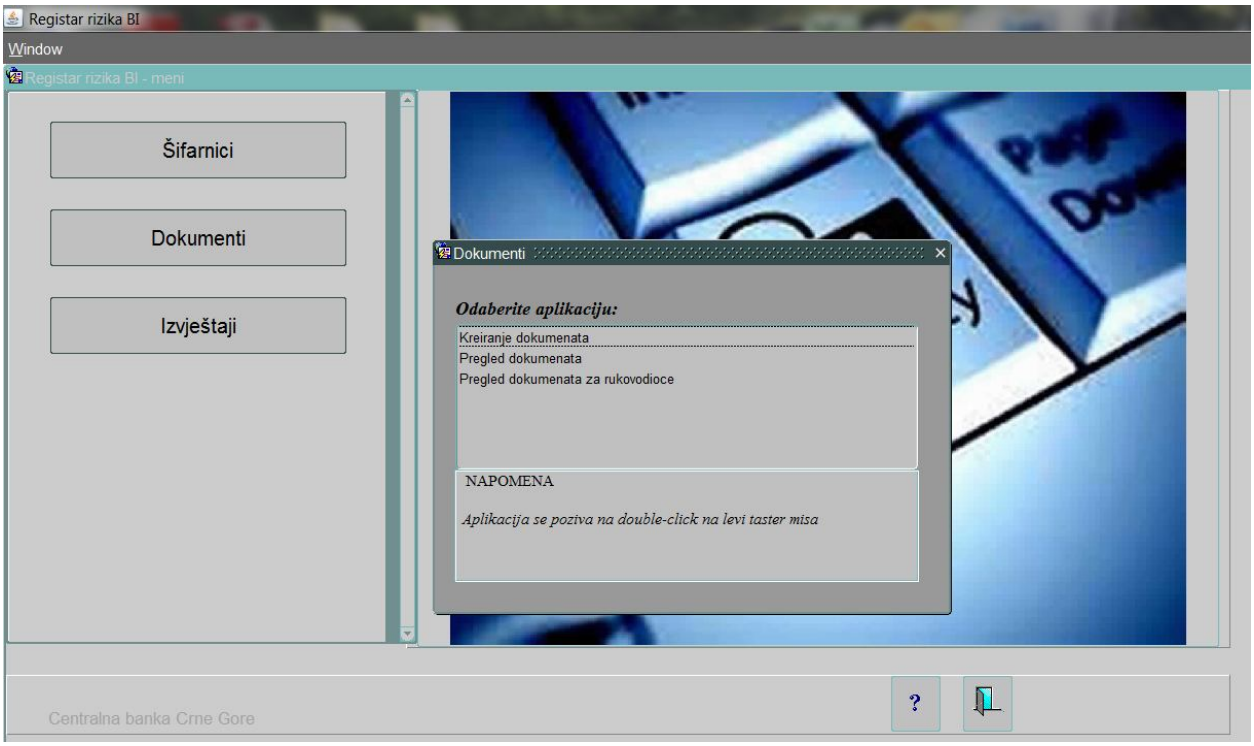
Na prethodnim slikama (Slika 11–18) uočavamo polja:

- **Povjerljivost –** obavezno, numeričko polje koje popunjava korisnik;
- **Integritet –** obavezno, numeričko polje koje popunjava korisnik;
- **Dostupnost –** obavezno, numeričko polje koje popunjava korisnik;
- **Klasifikacija –** obavezno tekstualno polje koje popunjava korisnik;
- **Opis –** obavezno tekstualno polje koje popunjava korisnik;
- **Vrijednost –** obavezno, numeričko polje koje popunjava korisnik;
- **Ocjena rizika –** obavezno, numeričko polje koje popunjava korisnik;
- **Vrijednost rizika –** obavezno alfanumeričko polje koje popunjava korisnik;
- **Nivo rizika –** obavezno tekstualno polje koje popunjava korisnik;
- **Opis rizika i potrebne mjere–** obavezno tekstualno polje koje popunjava korisnik;
- **Opcija –** obavezno tekstualno polje koje popunjava korisnik;
- **Opis opcije –** obavezno tekstualno polje koje popunjava korisnik;**,**
- **Evidentirano –** prilikom evidentiranja zapisa, ova polja se automatski popunjavau sistemskim datumom i imenom zaposlenog koji je evidentirao;
- **Izmijenjeno –** prilikom ažuriranja zapisa, ova polja se automatski popunjavaju sistemskim datumom ažuriranja i imenom zaposlenog koji je ažurirao zapis;
- **Zatvoreno –** prilikom zatvaranja zapisa, ova polja se automatski popunjavaju sistemskim datumom zatvaranja i imenom zaposlenog koji je zatvorio zapis;

Kao i dugme

- **Zatvori –** pritiskom na ovo dugme zapis postaje neaktivan, iako je i dalje vidljiv na formi. Zatvoreni zapisi se ne vide u listama vrijednosti.

5.2. Dokumenti

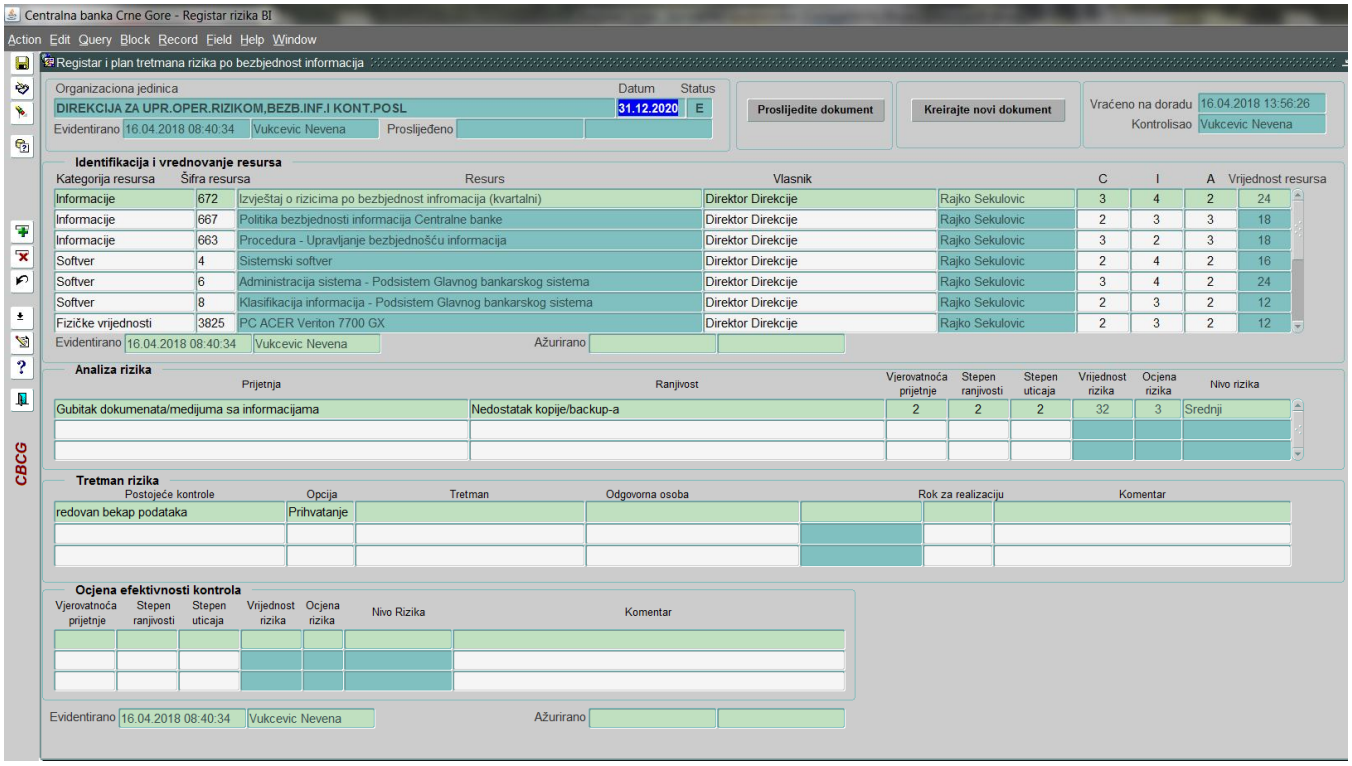


Slika 19: Dokumenti

Ova funkcija podsistema realizuje se kroz tri modula:

- **Kreiranje dokumenata**
- **Pregled dokumenata**
- **Pregled dokumenata – rukovodioci**

5.2.1. Kreiranje dokumenata



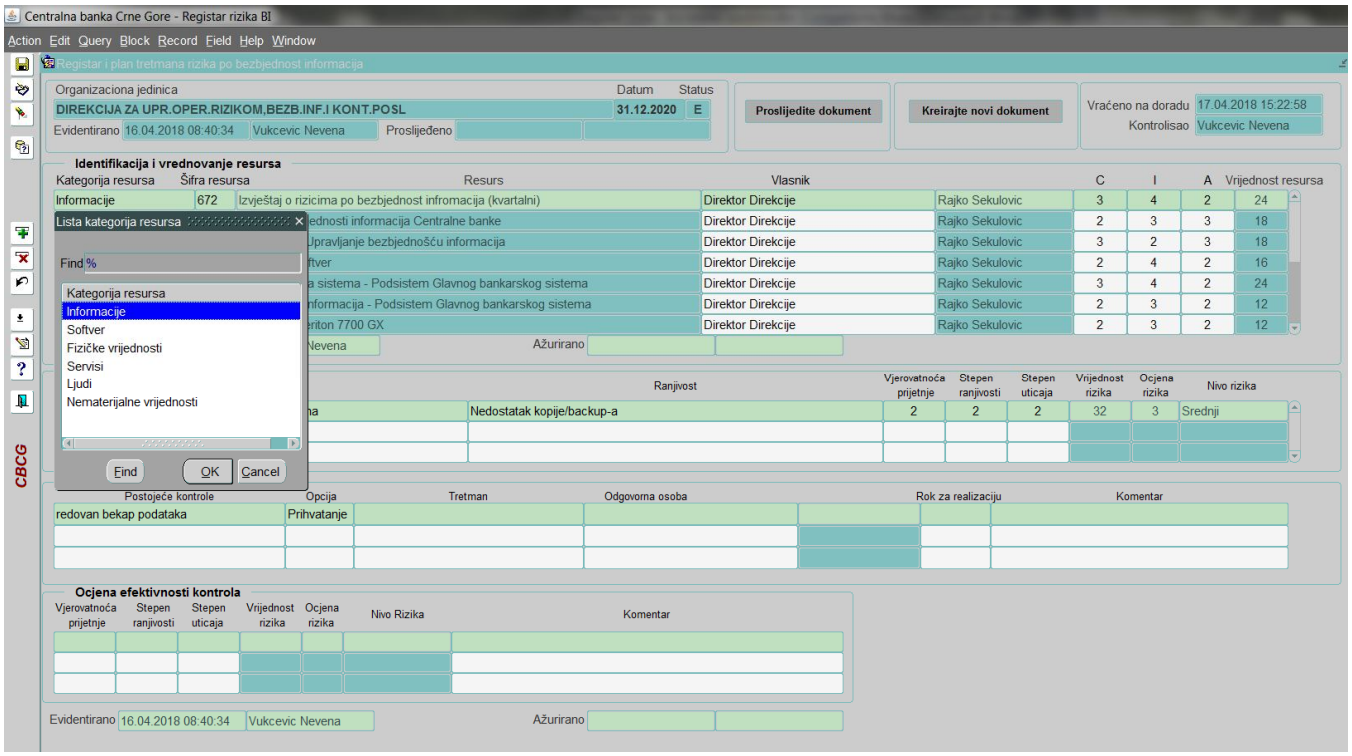
Slika 20: Izgled modula Kreiranje dokumenata

Opis funkcionalnosti modula

Ovaj modul namijenjen je korisnicima iz samostalnih OJ i omogućava kreiranje Registra i Plana tretmana rizika po bezbjednost informacija u vidu dokumenta za tu organizacionu jedinicu i zadati period. Za jednu organizacionu jedinicu i određeni datum kraja perioda može se kreirati samo jedan dokument. Nakon kreiranja dokument ima status **E** – evidentiran i u tom statusu se svi podaci osim datuma i organizacione jedinice mogu ažurirati. Kada korisnik iz samostalne OJ završi rad na dokumentu, on mu pritiskom na dugme **Proslijedi** mijenja status u P – proslijeđen i dokument postaje vidljiv Direkciji. Dokument koji ima status P se ne može ažurirati. Kroz ovaj modul zaposleni može da kreira i ima uvid samo u dokumente koji se odnose na samostalnu OJ kojoj on pripada. Dvostrukim klikom miša, otvara se modul (Slika 20). U modulu uočavamo sljedeća polja:

- **Organizaciona jedinica -** se popunjava automatski i predstavlja samostalnu OJ kojoj pripada zaposleni koji je prijavljen na aplikaciju;

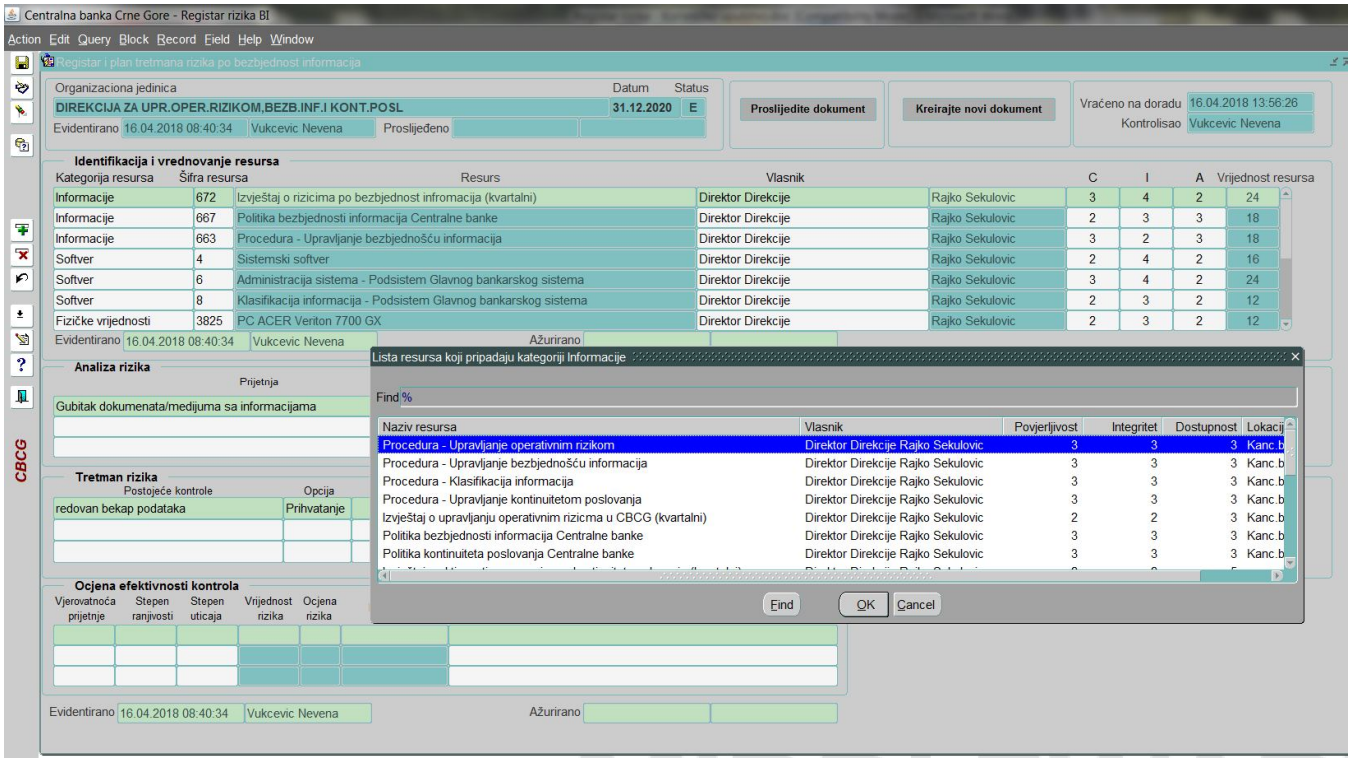
- **Datum –** obavezno datumsko polje koje popunjava korisnik prilikom kreiranja prvog dokumenta za svoju OJ. Dokument za tu OJ i naredni period kreira se automatski pritiskom na dugme ***Kreirajte novi dokument***. Tada se polje ***Datum*** automatski popunjava datumom koji je za godinu dana veći u odnosu na onaj na prvom dokumentu, u skladu sa dinamikom izvještavanja definisanom u Metodologiji. Unešeni datum se ne može ažurirati;



Slika 21: Lista vrijednosti za kategoriju resursa

- **Kategorija resursa** – obavezno polje koje popunjava korisnik iz liste vrijednosti (Slika 21) koja se poziva dvostrukim klikom miša na polje. Na listi se nalaze aktivni zapisi iz šifarnika kategorija resursa;
- **Šifra resursa** – obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje. Izabrana kategorija resursa definiše sadržaj liste vrijednosti za biranje resursa. Ako je izabrana kategorija resursa *Informacije*, na listi vrijednost se nalaze aktivni zapisi iz tabele Klasifikacija informacija za samostalnu OJ za koju se kreira dokument (Slika 22), ako je izabrana kategorija resursa *Softver*, na listi vrijednost se nalaze aktivni zapisi iz šifarnika Softver koji održava Direkcija (Slika 23), ako je izabrana kategorija resursa *Fizičke vrijednosti*, na listi vrijednost se nalaze zapisi iz tabele Osnovna sredstva, koji imaju status U,

kao i aktivni zapisi iz šifarnika Fizičke vrijednosti koji održava Direkcija (Slika 24), ako je izabrana kategorija resursa *Servisi*, na listi vrijednosti se nalaze aktivni zapisi iz šifarnika Servisi koji održava Direkcija, ako je izabrana kategorija resursa *Ljudi*, na listi vrijednosti se nalaze aktivni zapisi iz tabele Poslovi koji su vezani za samostalnu OJ za koju se kreira dokument (Slika 25), ako je izabrana kategorija resursa *Nematerijalne vrijednosti*, na listi vrijednosti se nalaze aktivni zapisi iz šifarnika Nematerijalne vrijednosti koji održava Direkcija. Polje **Resurs** se automatski povlači iz liste.



Slika 22: Lista vrijednosti za resurse iz kategorije Informacije

- **Vlasnik -** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 26). Na listi je organizaciona struktura Centralne banke Crne Gore, zajedno sa imenima zaposlenih koji su raspoređeni na radna mjesta;
- **C -** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 27). Vrijednost u ovom polju predstavlja stepen povjerljivosti identifikovanog resursa;

- **I -** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 28). Vrijednost u ovom polju predstavlja stepen integriteta identifikovanog resursa;
- **A -** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 29). Vrijednost u ovom polju predstavlja stepen dostupnosti identifikovanog resursa;
- **Vrijednost resursa –** polje koje se automatski izračunava i popunjava nakon popunjavanja vrijednosti za C, I i A, u skladu sa Metodologijom. Za resurse čija je procijenjena vrijednost manja od 12, u skladu sa Metodologijom, ne sprovodi se analiza rizika. Ova kontrola je ugrađena u softver tako da se nakon evidentiranja takvog resursa javlja odgovarajuća poruka upozorenja i softver ne dozvoljava dalje popunjavanje. Takav resurs se može izbrisati iz dokumenta, a može ostati u evidenciji, s tim se što se dio dokumenta koji se odnosi na analizu rizika ne popunjava.;
- **Prijetnja -** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 30). U listi vrijednosti su prijetnje koje su definisane za izabranu kategoriju resursa;
- **Ranjivost -** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 31). U listi vrijednosti su ranjivosti koje su definisane za izabranu kategoriju resursa;
- **Vjerovatnoća prijetnje -** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 32);
- **Stepen ranjivosti-** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 33);
- **Stepen uticaja -** obavezno polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 34);
- **Vrijednost rizika –** polje koje se automatski izračunava i popunjava nakon popunjavanja vrijednosti za Vjerovatnoću prijetnje, Stepen ranjivosti i Stepen uticaja, u skladu sa Metodologijom.
- **Ocjena rizika** i **Nivo rizika –** polja koje se automatski popunjavaju na osnovu Vrijednost rizika, u skladu sa šifarnikom za Klasifikaciju rizika**.** Rizik koji je ocijenjen kao nizak, u skladu sa Metodologijom, se prihvata i ne razmatra. Ova kontrola je ugrađena u softver tako da se nakon

evidentiranja takvog rizika javlja odgovarajuća poruka upozorenja i softver ne dozvoljava dalje popunjavanje;

- **Postojeće kontrole** – tekstualno polje koje popunjava korisnik. Popunjavanje polja je obavezno ukoliko rizik nije ocijenjen kao nizak;
- **Opcija –** polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 35). Popunjavanje polja je obavezno ako rizik nije ocijenjen kao nizak Ukoliko je opcija *Prihvatanje*, u skladu sa Metodologijom, ne sprovodi se tretman rizika. Ova kontrola je ugrađena u softver tako da se nakon evidentiranja takvog rizika javlja odgovarajuća poruka upozorenja i softver ne dozvoljava dalje popunjavanje;
- **Tretman** – tekstualno polje koje popunjava korisnik;
- **Odgovorna osoba –** polje koje popunjava korisnik iz liste vrijednosti koja se poziva dvostrukim klikom miša na polje (Slika 26). Na listi je organizaciona struktura Centralne banke Crne Gore, zajedno sa imenima zaposlenih koji su raspoređeni na radna mjesta;
- **Rok za realizaciju –** datumsko polje koje popunjava korisnik;
  Polja **Tretman**, **Odgovorna osoba** i **Rok za realizaciju** su polja koja se odnose na tretman rizika, pa su obavezna ukoliko izabrana opcija nije *Prihvatanje*.
- **Komentar** – neobavezno tekstualno polje koje popunjava korisnik;
- **Evidentirano –** prilikom evidentiranja zapisa, ova polja se automatski popunjavaju sistemskim datumom i imenom zaposlenog koji je evidentirao;
- **Izmijenjeno –** prilikom ažuriranja zapisa, ova polja se automatski popunjavaju sistemskim datumom ažuriranja i imenom zaposlenog koji je ažurirao zapis;
- **Proslijeđeno –** prilikom prosljeđivanja dokumenta Direkciji, ova polja se automatski popunjavaju sistemskim datumom prosljeđivanja i imenom zaposlenog koji je proslijedio dokument;

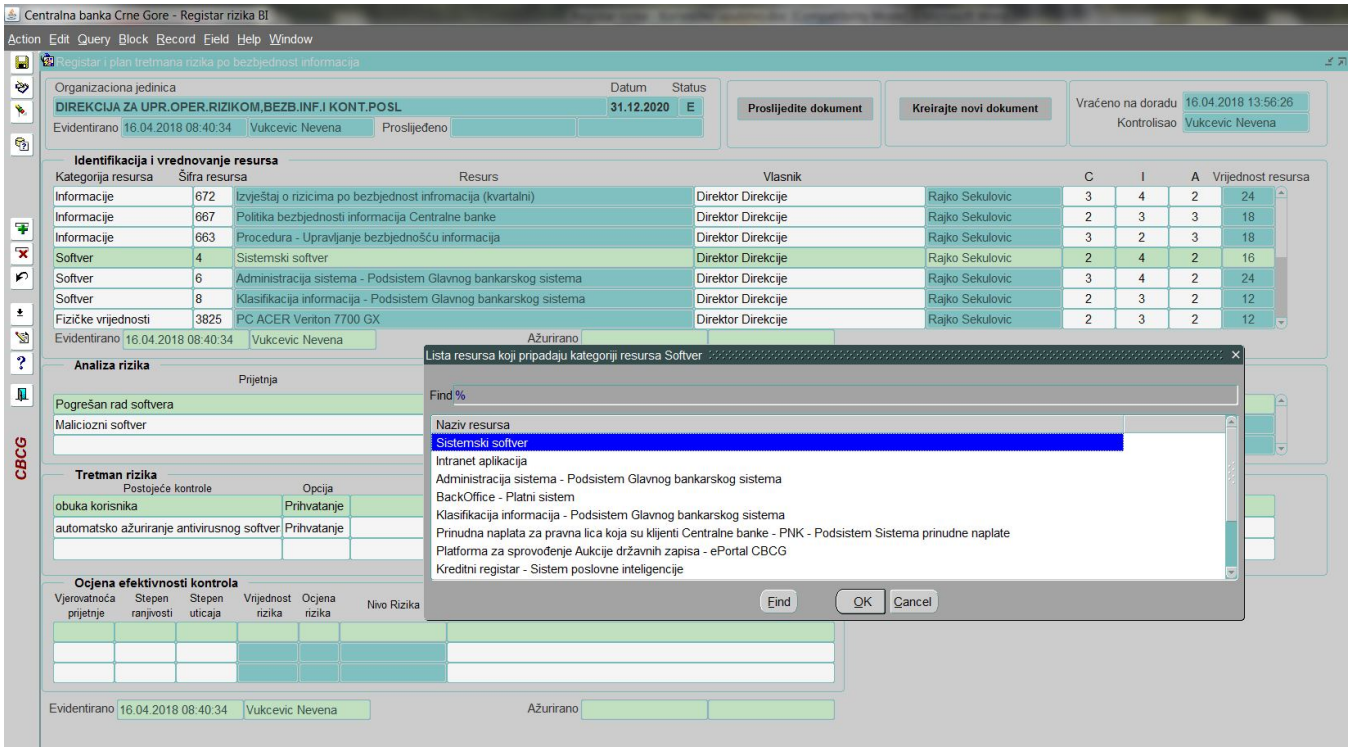
Uočavamo dugmad:

- **Proslijedite dokument –** pritiskom na ovo dugme, status dokumenta se mijenja u P – proslijeđen. Tada dokument postaje vidljiv Direkciji i podaci u njemu se ne mogu mijenjati. Nakon uspješnog prosljeđivanja dokumenta Direkciji, softver javlja poruku kao na Slici 37;
- **Kreirajte novi dokument –** pritiskom na ovo dugme, automatski se kreira novi dokument za samostalnu OJ, koji je identičan kao posljednji kreirani i proslijeđeni dokument, samo što mu je

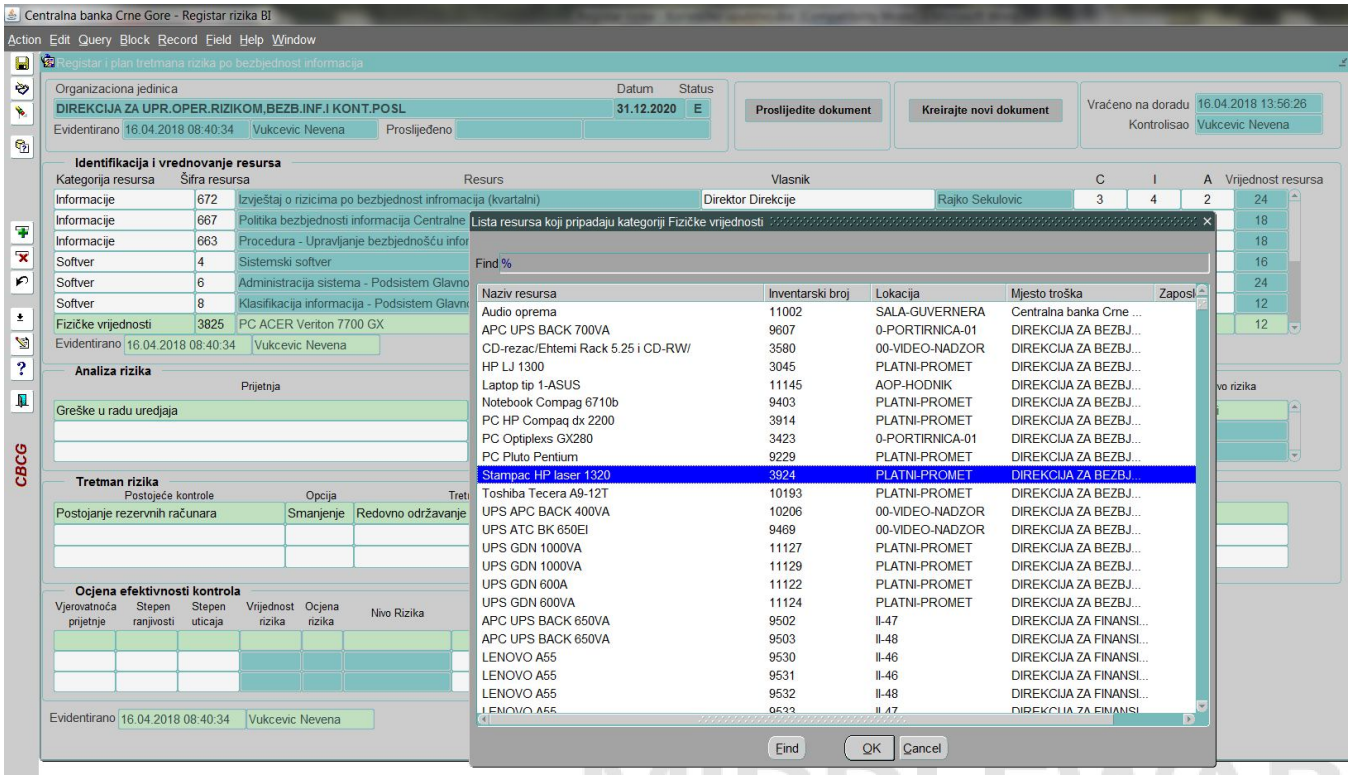
datum za godinu veći i dokument je u statusu E. Ova funkcionalnost omogućava da predstavnici samostalnih OJ **samo prvi put kreiraju** Registar i plan tretmana rizika **neposrednim unosom**. Za svaki sljedeći datum, **novi dokument se kreira automatski na osnovu prethodnog pritiskom na dugme.** U novokreiranom dokumentu, koji je u statusu E, mogu se brisati, mijenjati i dodavati podaci. Na taj način je omogućeno da se kreiranje Registra i plana tretmana za svaki naredni period, suštinski svede na doradu dokumenta za prethodni period. Da bi se automatski mogao kreirati novi dokument, svi prethodno kreirani dokumenti moraju biti proslijeđeni Direkciji, odnosno svi moraju biti u statusu P.

Za polja **Vjerovatnoća prijetnje, Stepen ranjivosti, Stepen uticaja, Vrijednost rizika, Ocjena rizika, Nivo rizika** i **Komentar**, koja se popunjavaju u okviru Ocjene efektivnosti kontrola važe već navedena pravila.

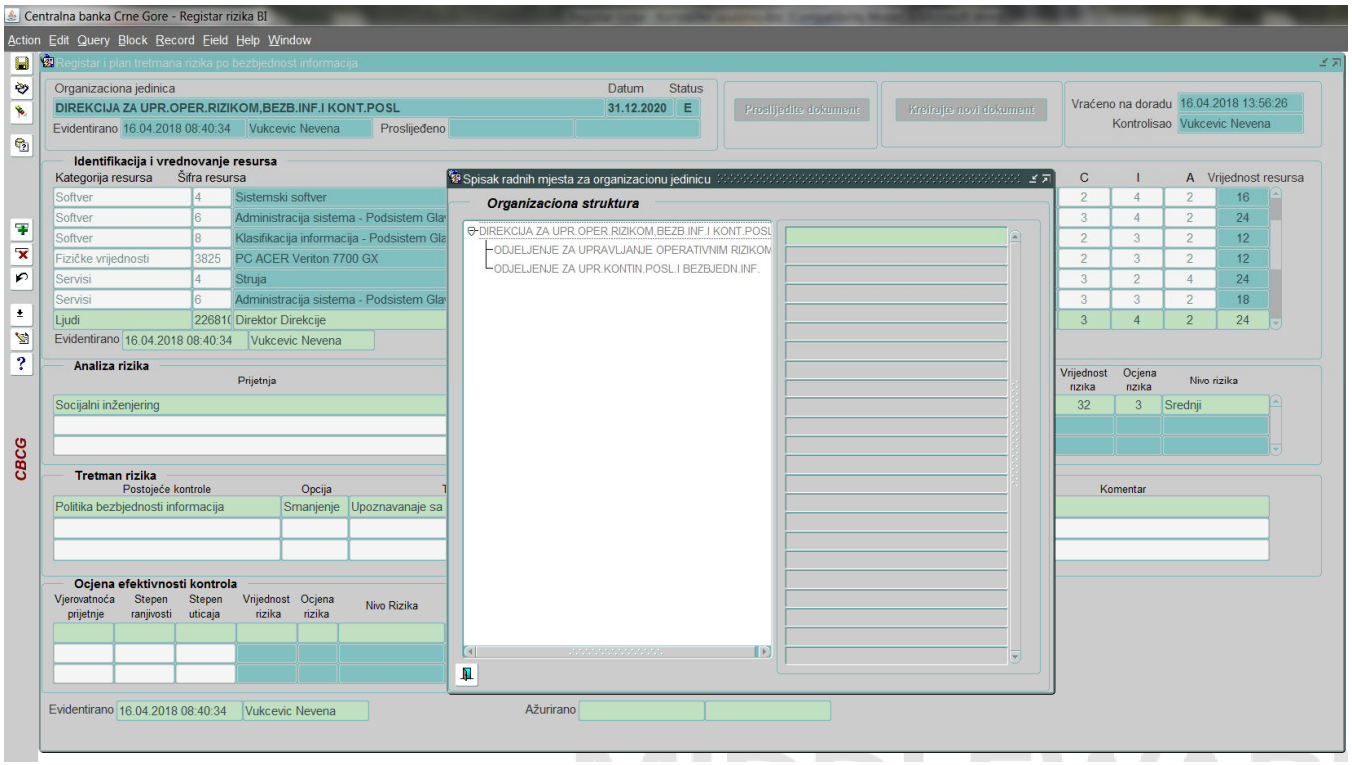
Sva polja za koja su predefinisane liste vrijednosti, imaju dodatnu kontrolu unosa u vidu validacije iz liste, tako da se ne može upisati nedozvoljena vrijednost.



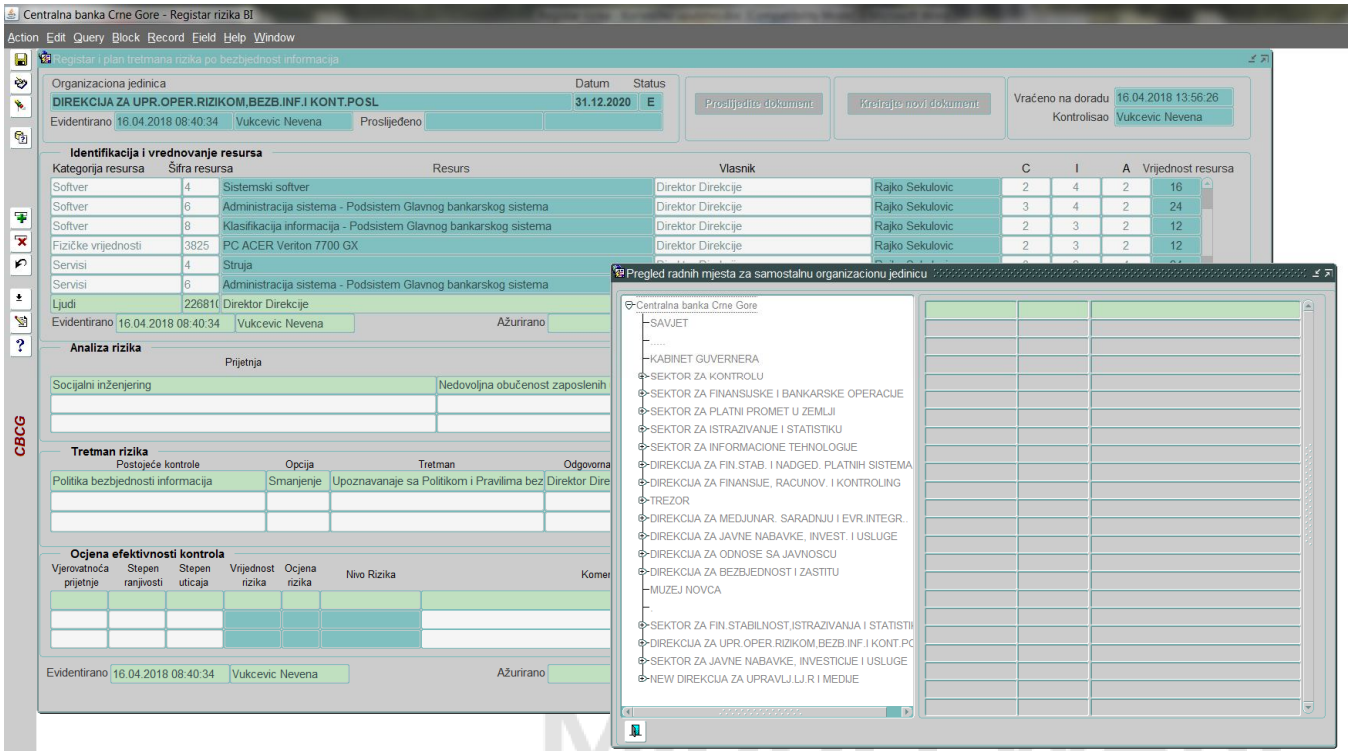
Slika 23: Lista vrijednosti za resurse iz kategorije Softver



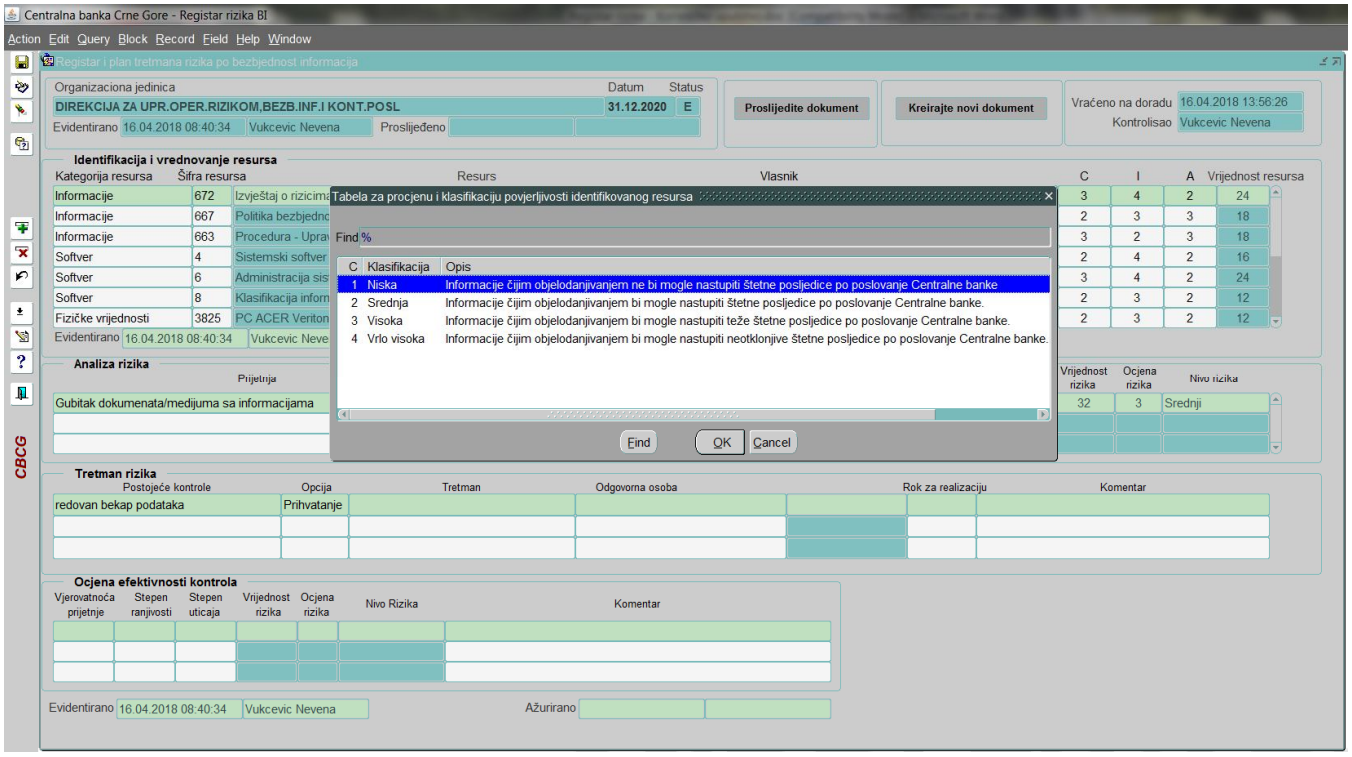
Slika 24: Lista vrijednosti za resurse iz kategorije Fizičke vrijednosti



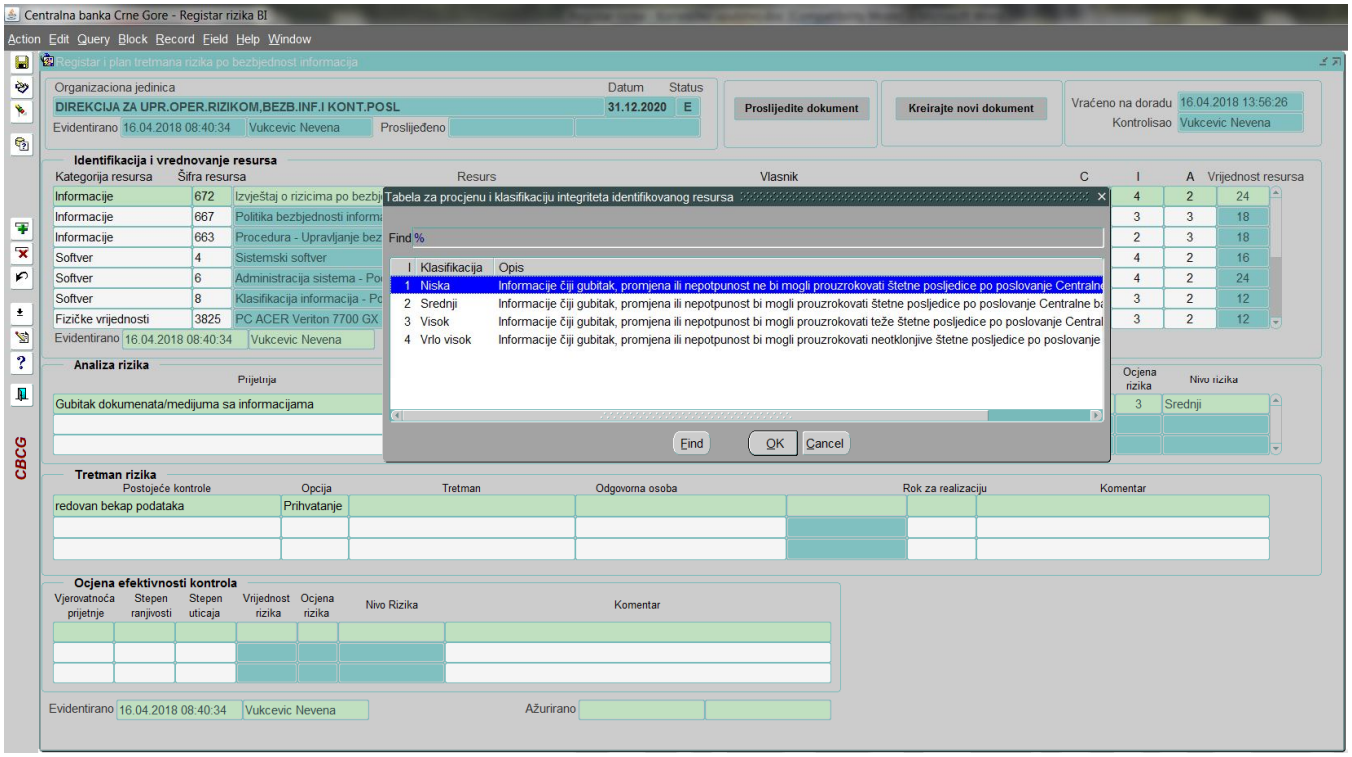
Slika 25: Lista vrijednosti za resurse iz kategorije Ljudi



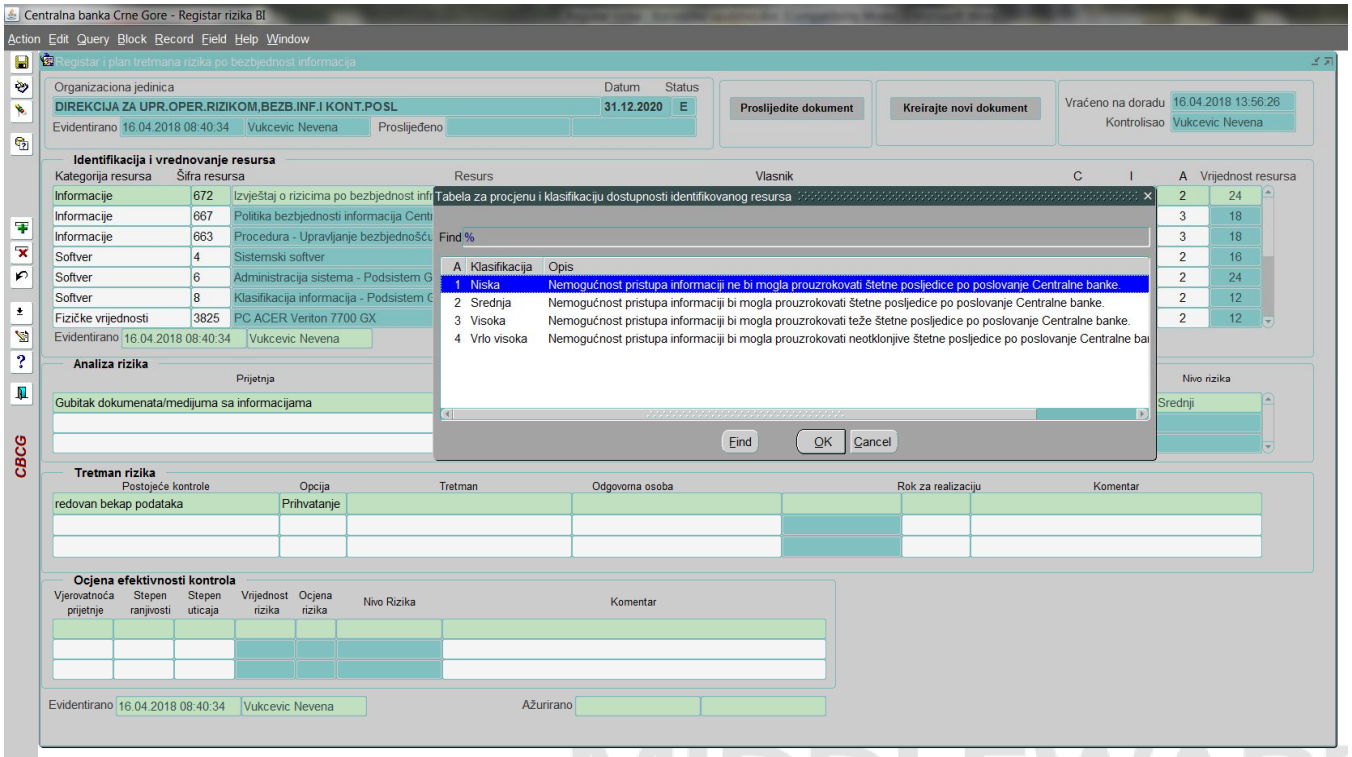
Slika 26: Lista vrijednosti za vlasnike identifikovanog resursa



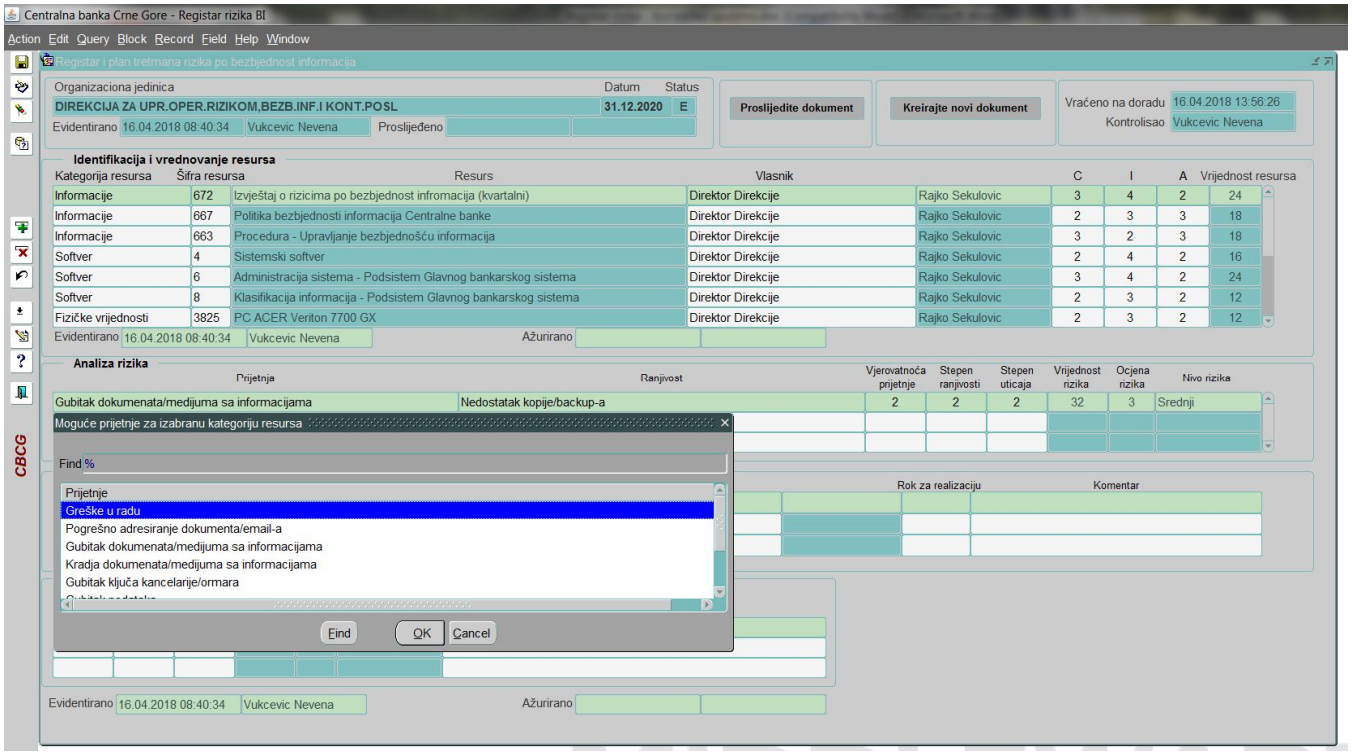
Slika 27: Lista vrijednosti za povjerljivost



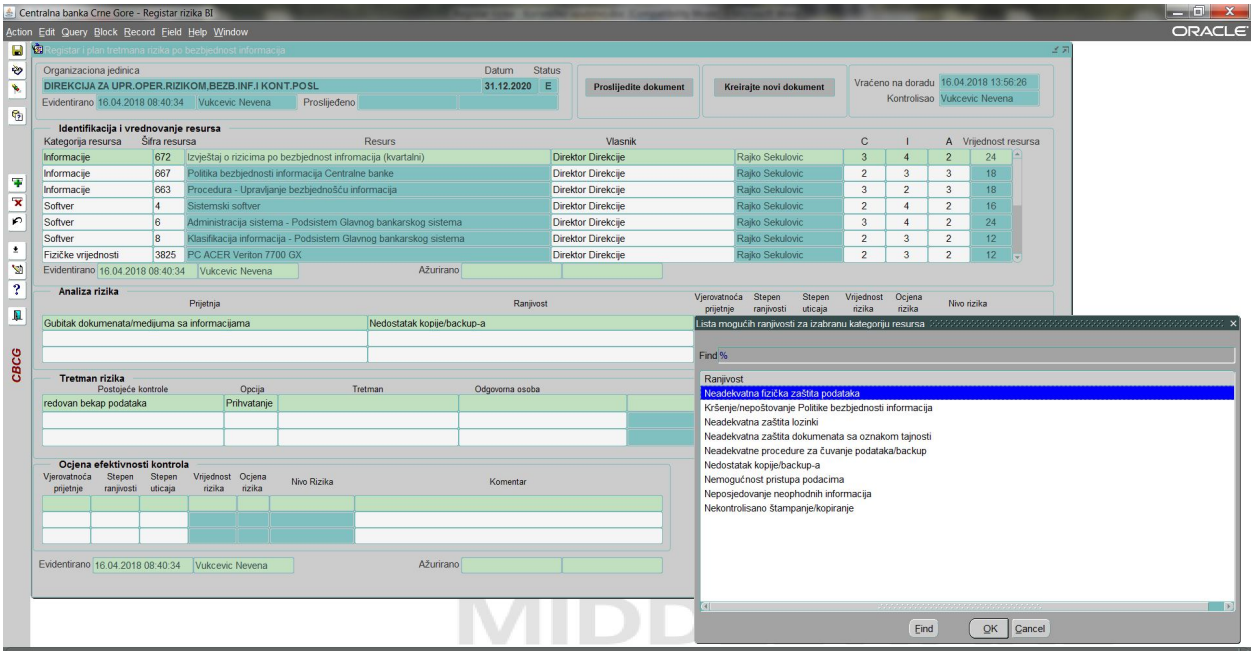
Slika 28: Lista vrijednosti za integritet



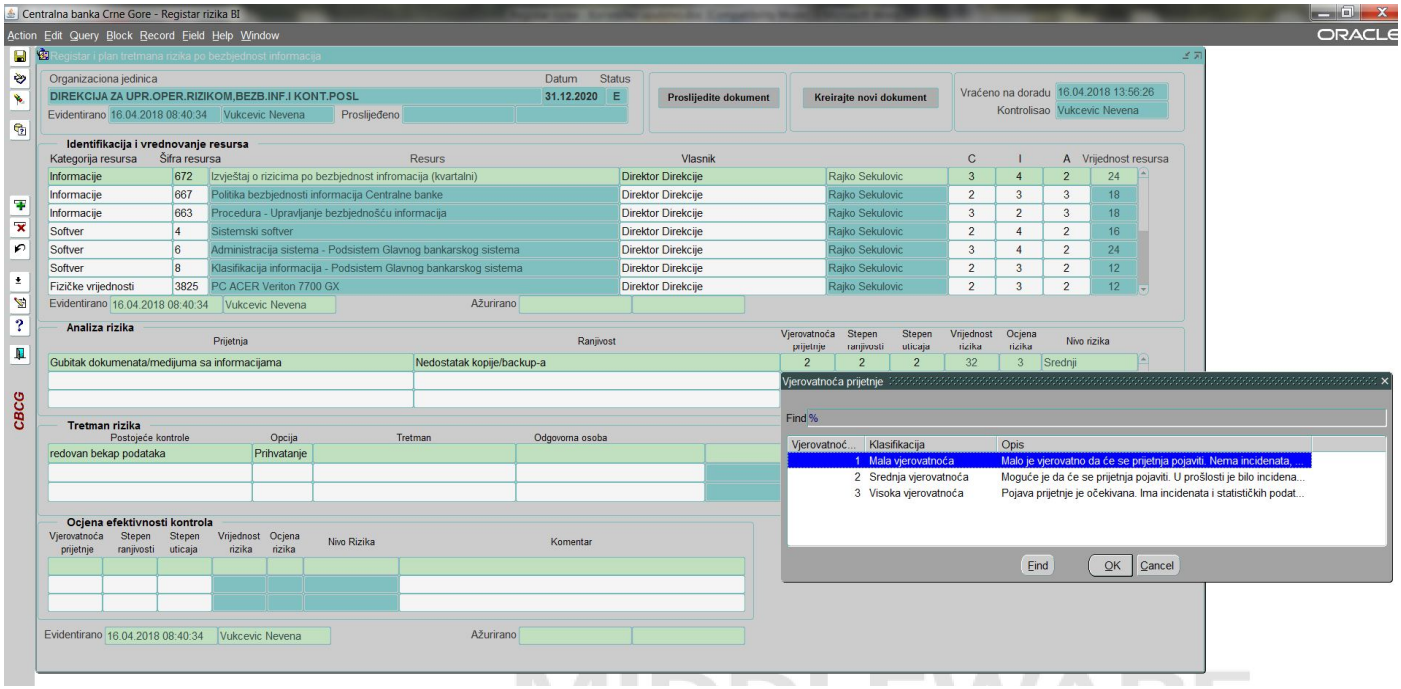
Slika 29: Lista vrijednosti za dostupnost



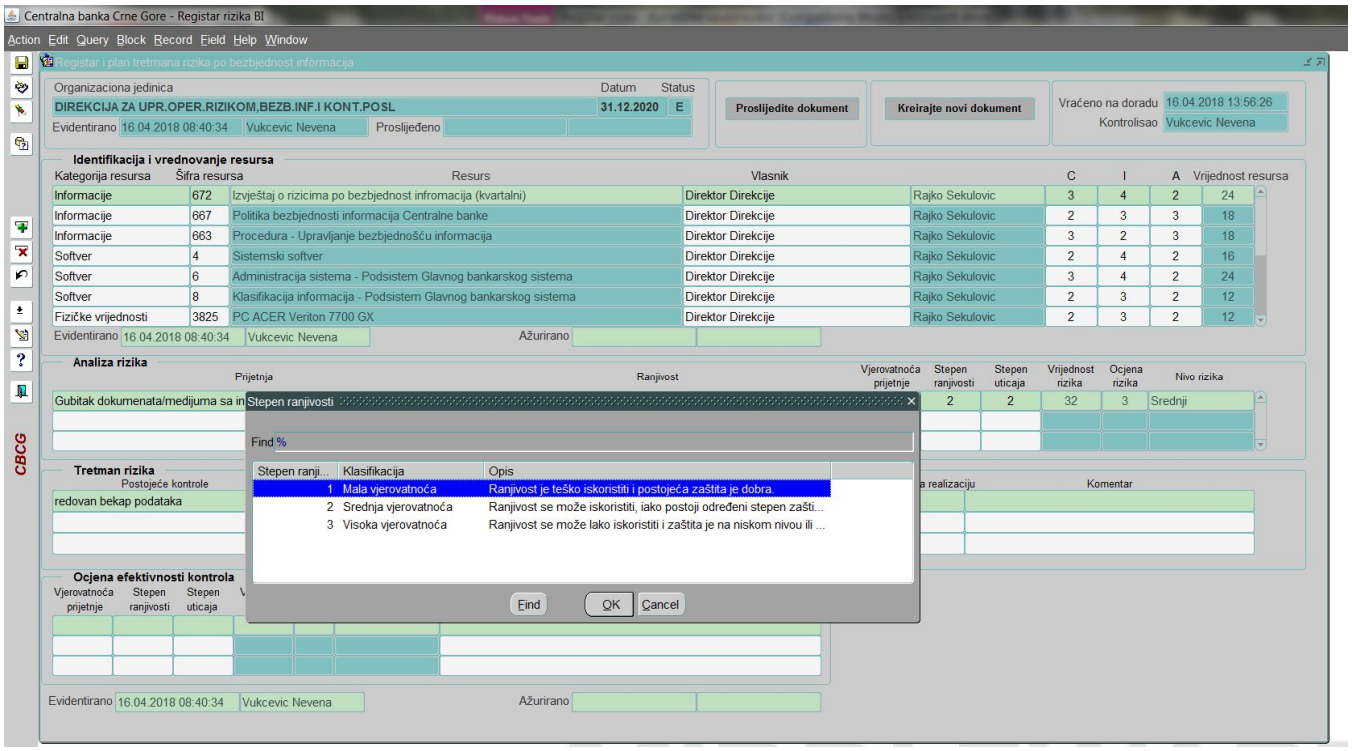
Slika 30: Lista vrijednosti za prijetnje definisane za izabranu kategoriju resursa



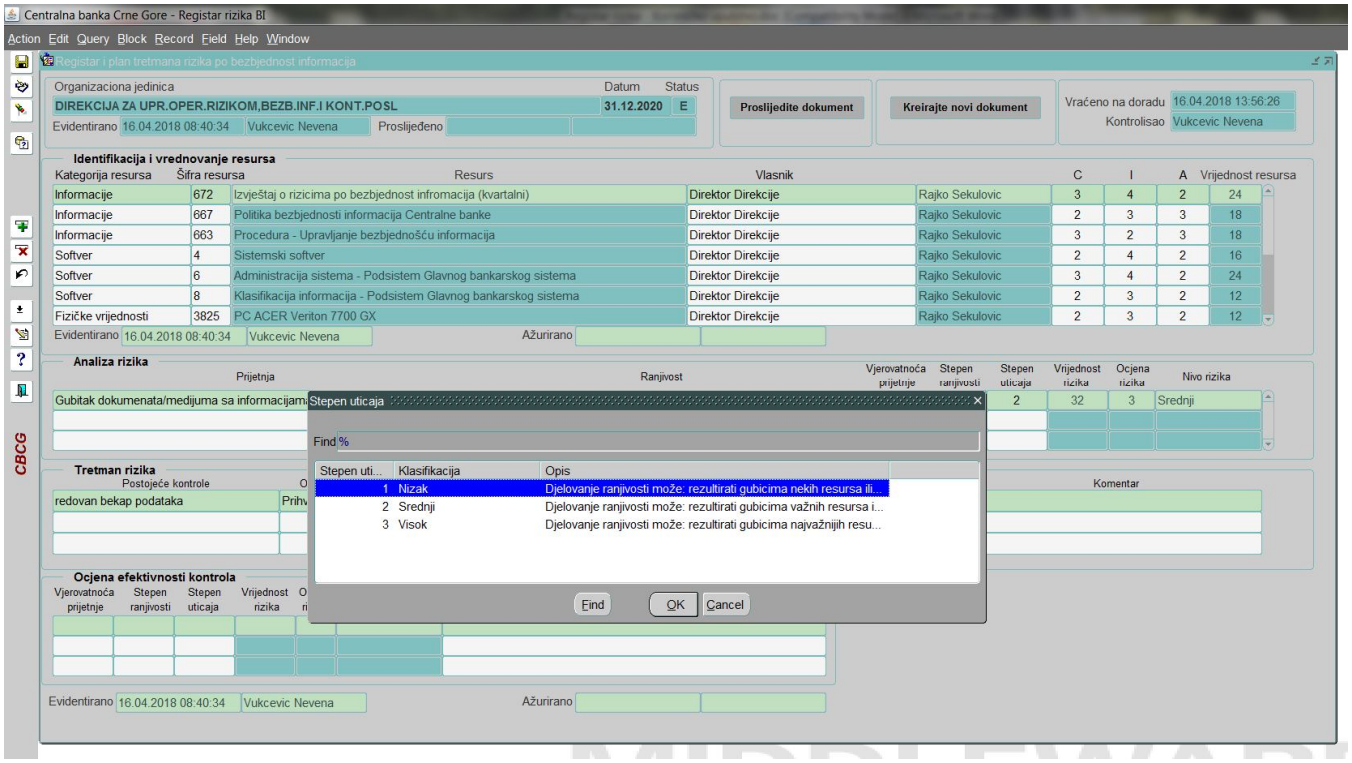
Slika 31: Lista vrijednosti za ranjivosti definisane za izabranu kategoriju resursa



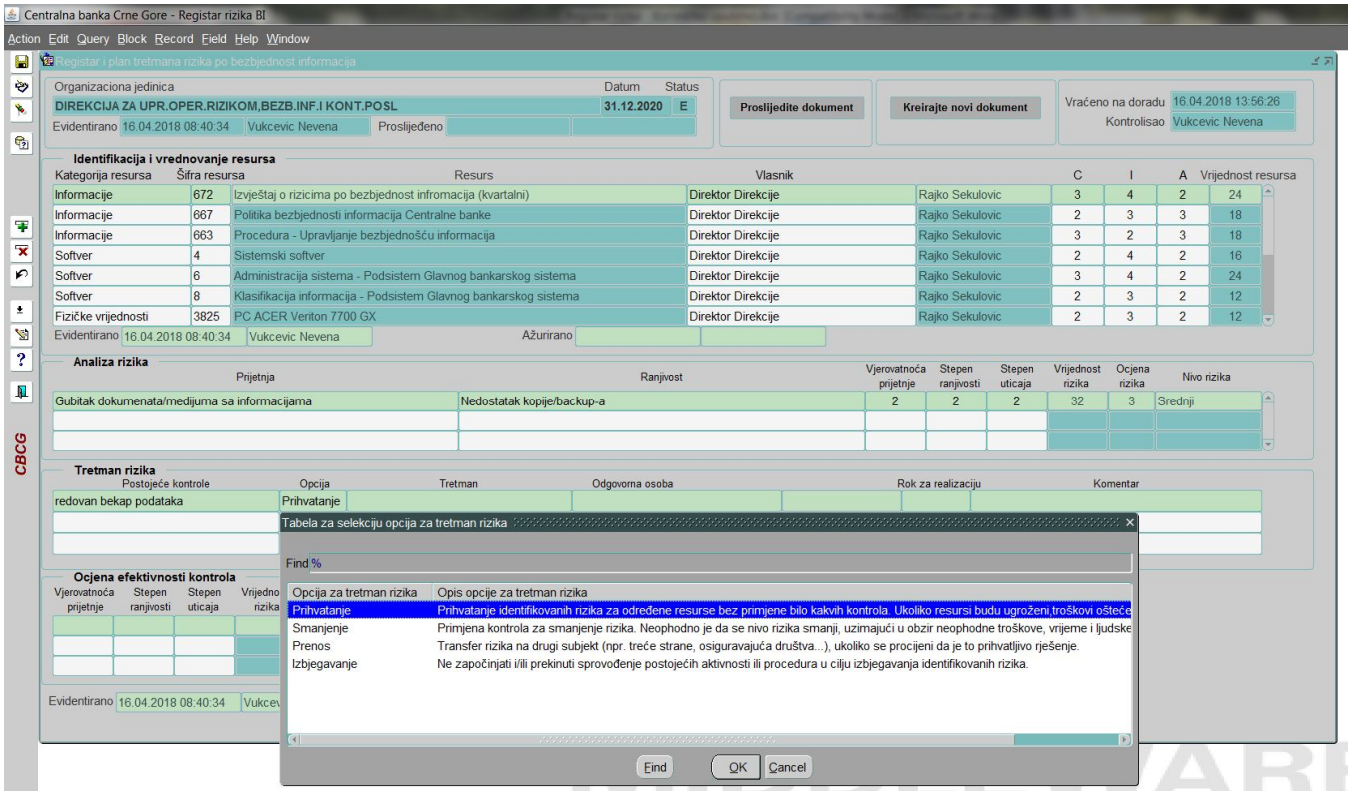
Slika 32: Lista vrijednosti za vjerovatnoću pojavljivanja prijetnje



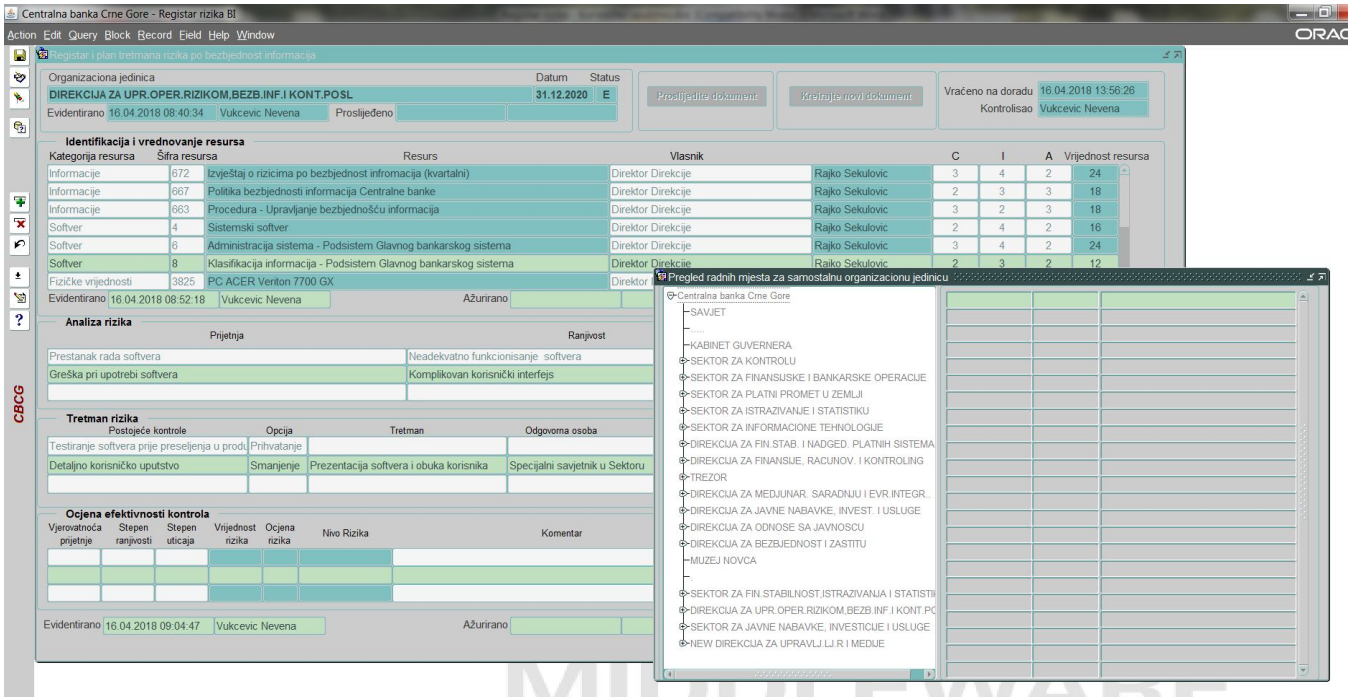
Slika 33: Lista vrijednosti za stepen ranjivosti



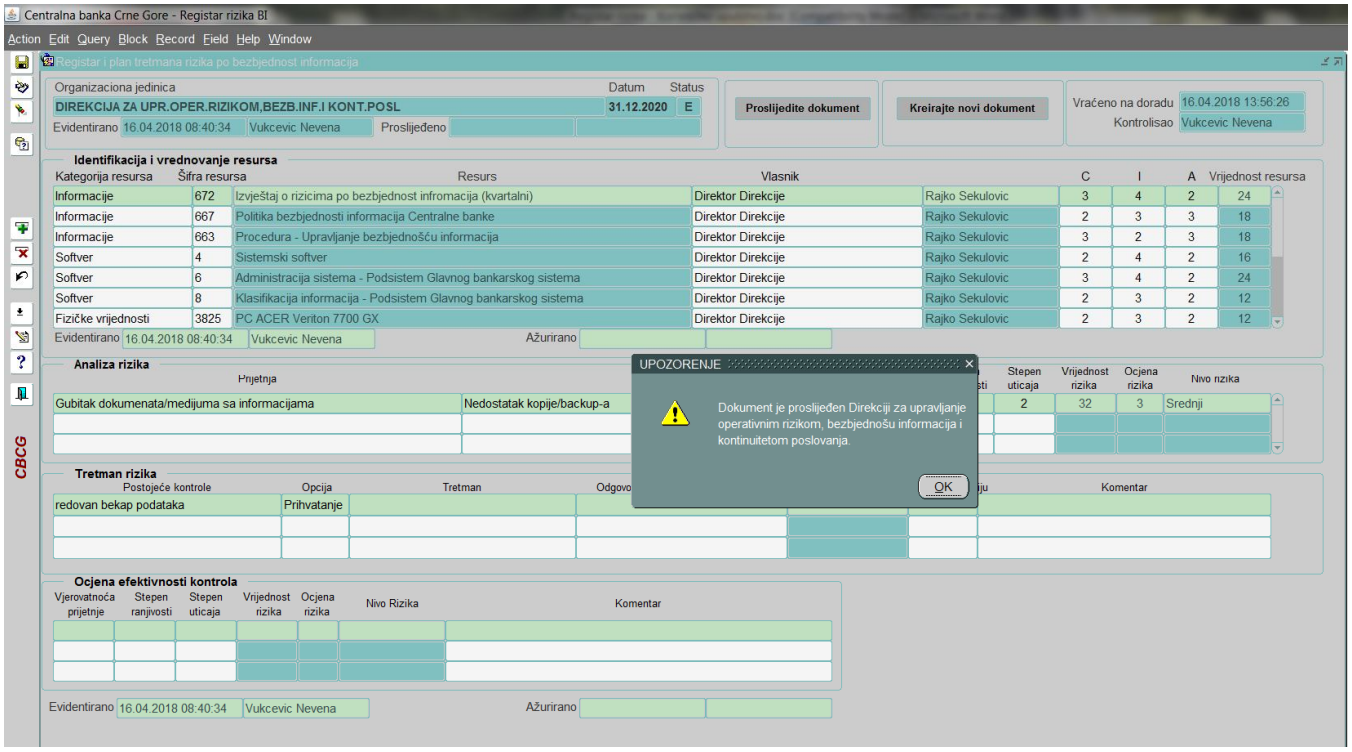
Slika 34: Lista vrijednosti za stepen uticaja



Slika 35: Lista vrijednosti za opcije za tretman rizika



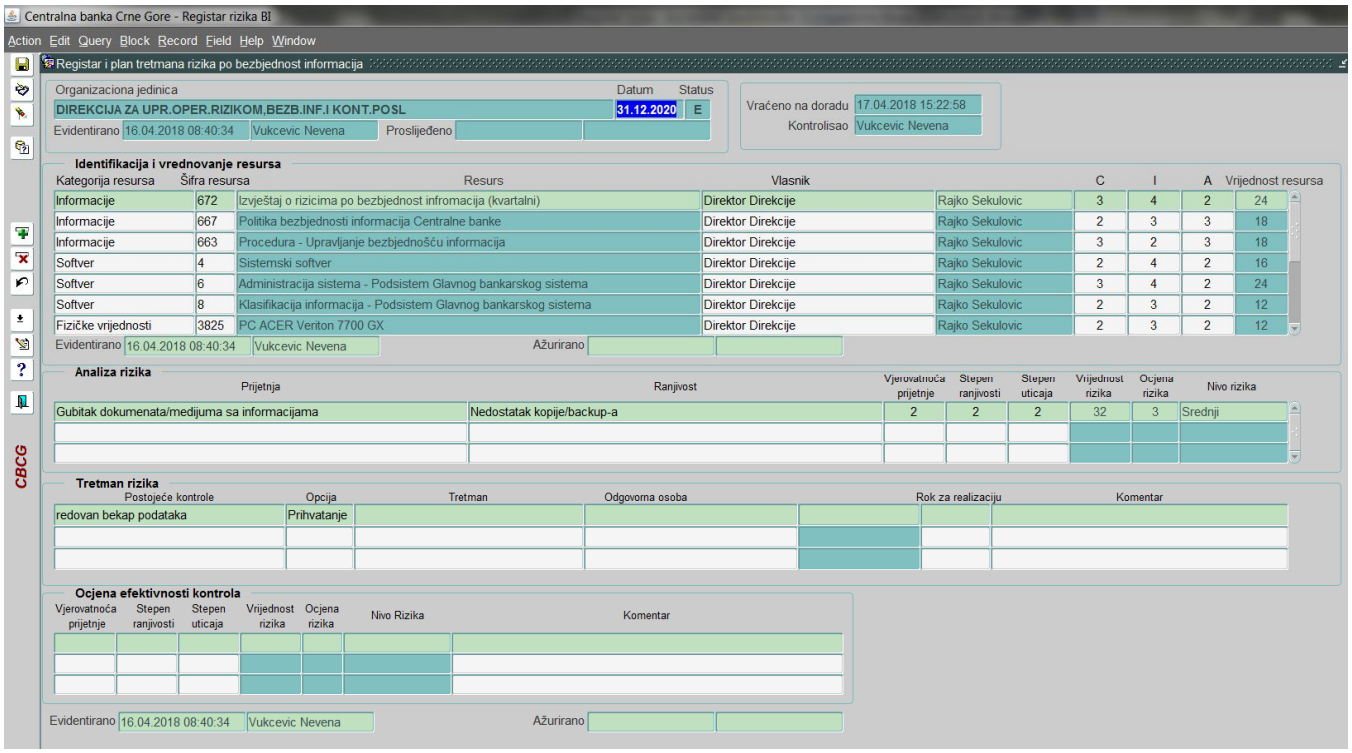
Slika 36: Lista vrijednosti za odgovornu osobu



Slika 37: Prosljeđivanje dokumenta Direkciji

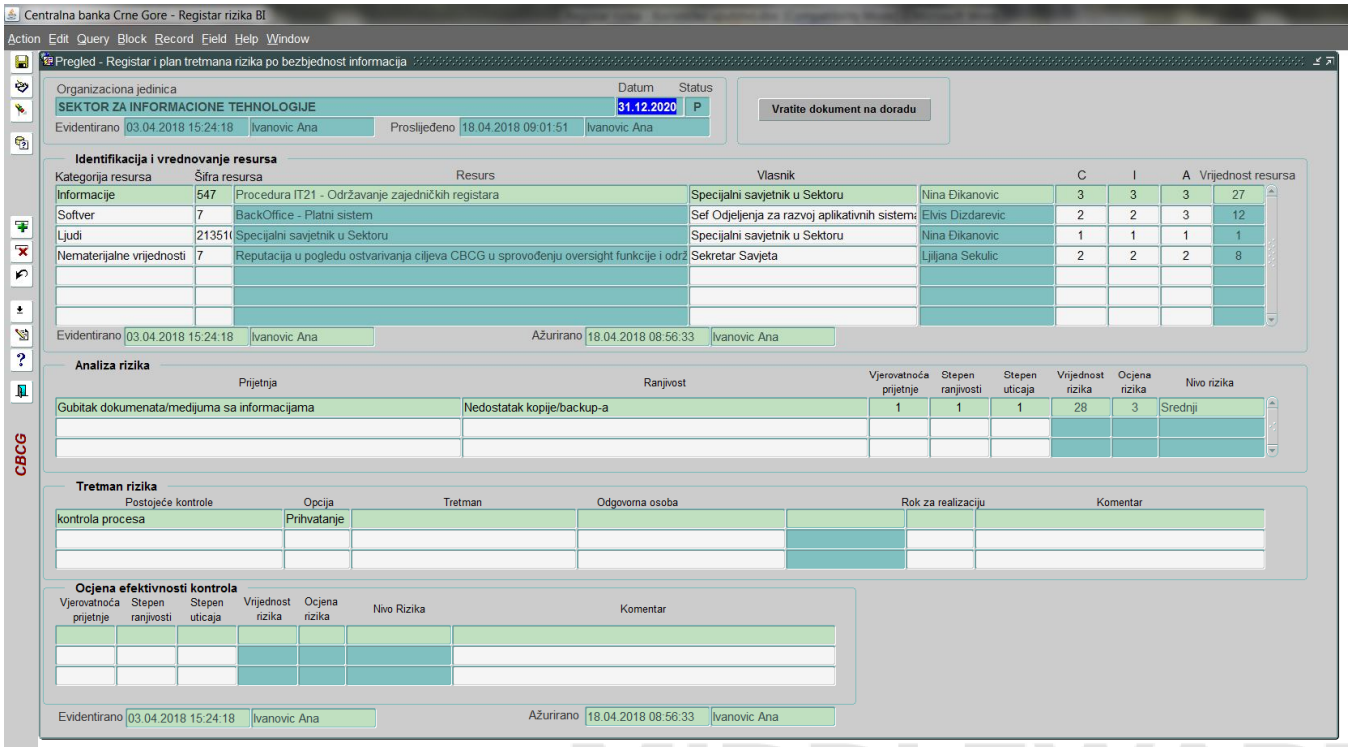
5.2.2. Pregled dokumenta – rukovodioci

Ovaj modul namijenjen je rukovodiocima samostalnih OJ da bi u svakom trenutku mogli da imaju uvid u dokumente koji se odnose na njihovu organizacionu jedinicu. Oni mogu vidjeti dokumente dok je rad na njima još u toku, dakle dok su još podložni promjeni (status E), kao i nakon prosljeđivanja Direkciji (status P). Ovaj modul je namijenjen pregledu dokumenta i kroz njega se ne mogu vršiti nikakve izmjene na dokumentu.



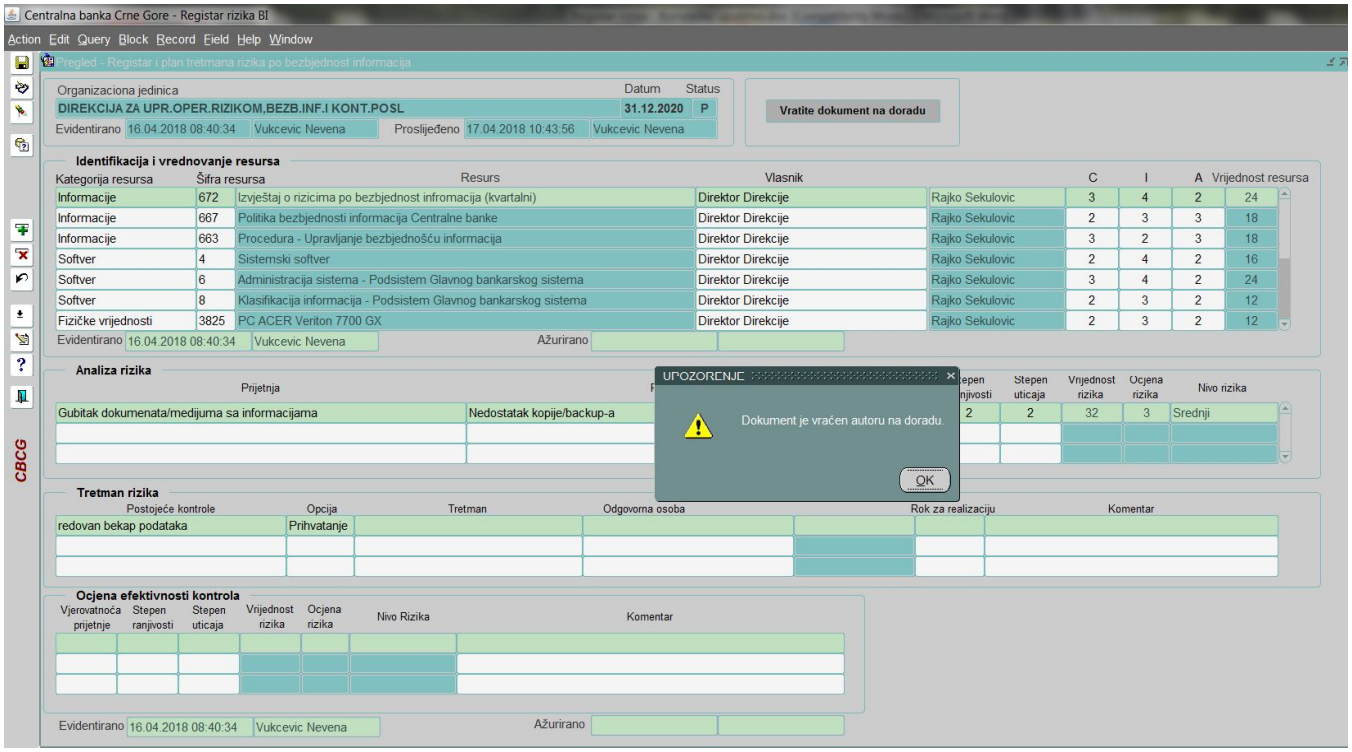
Slika 38: Izgled modula Pregled dokumenta – rukovodioci

5.2.3. Pregled dokumenta

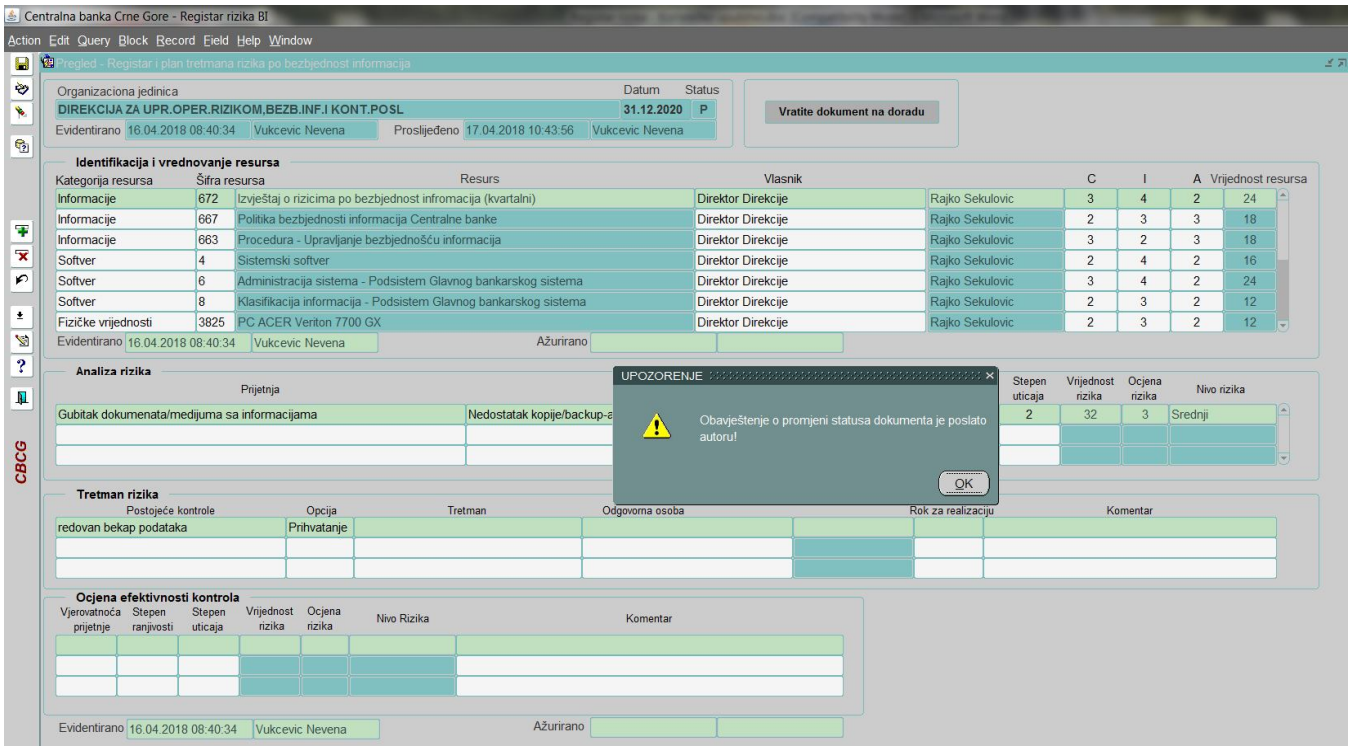


Slika 39: Izgled modula Pregled dokumenta

Ovaj modul namijenjen je Direkciji i služi za uvid u dokumente koje su joj samostalne OJ proslijedile. Dakle, dok samostalne OJ, kroz module koje su im namijenjeni, imaju uvid samo u svoje dokumente, Direkcija ima uvid u proslijeđene dokumente svih OJ, odnosno u dokumente svih OJ koji su u statusu P. Ovaj modul je namijenjen pregledu dokumenta i kroz njega se ne mogu vršiti nikakve modifikacije na dokumentu, osim promjene statusa dokumenta. Nakon prosljeđivanja dokumenta Direkciji, ovlašćeno lice iz Direkcije pregleda i analizira dokument. Ukoliko uoči da postoji neki nedostatak, to lice ima mogućnost da pritiskom na dugme **Vratite dokument na doradu** dokument vrati na doradu (Slika 40), poslije čega dokument ima ponovo status E. Pri tome, polje Vraćeno na doradu se automatski popunjava sistemskim datumom vraćanja na doradu, a polje Kontrolisao imenom zaposlenog koji je vratio dokument na doradu. Zaposleni iz samostalne OJ koji je Direkciji proslijedio dokument, nakon vraćanja dokumenta na doradu, dobija mail notifikaciju o tome da je dokument vraćen (Slika 41).

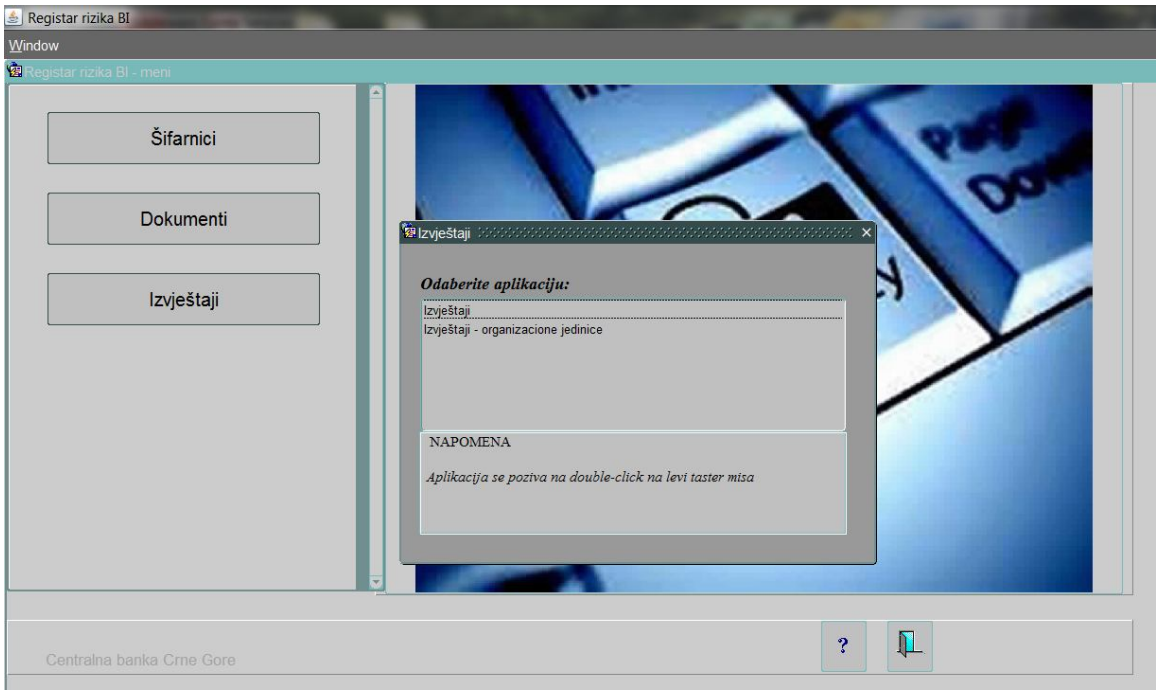


Slika 40: Modul Pregled dokumenta – potvrda o vraćanju dokumenta na doradu



Slika 41: Modul Pregled dokumenta – mail notifikacija prilikom vraćanja dokumenta na doradu

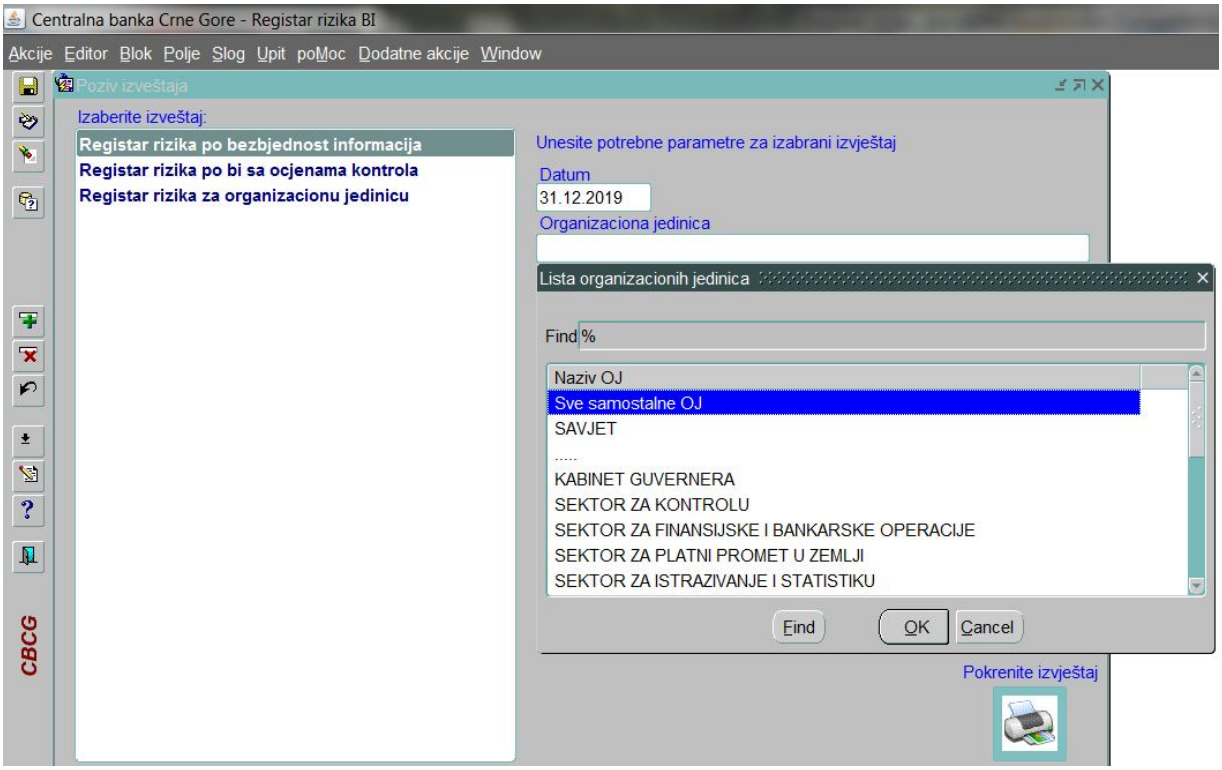
5.3. Izvještaji



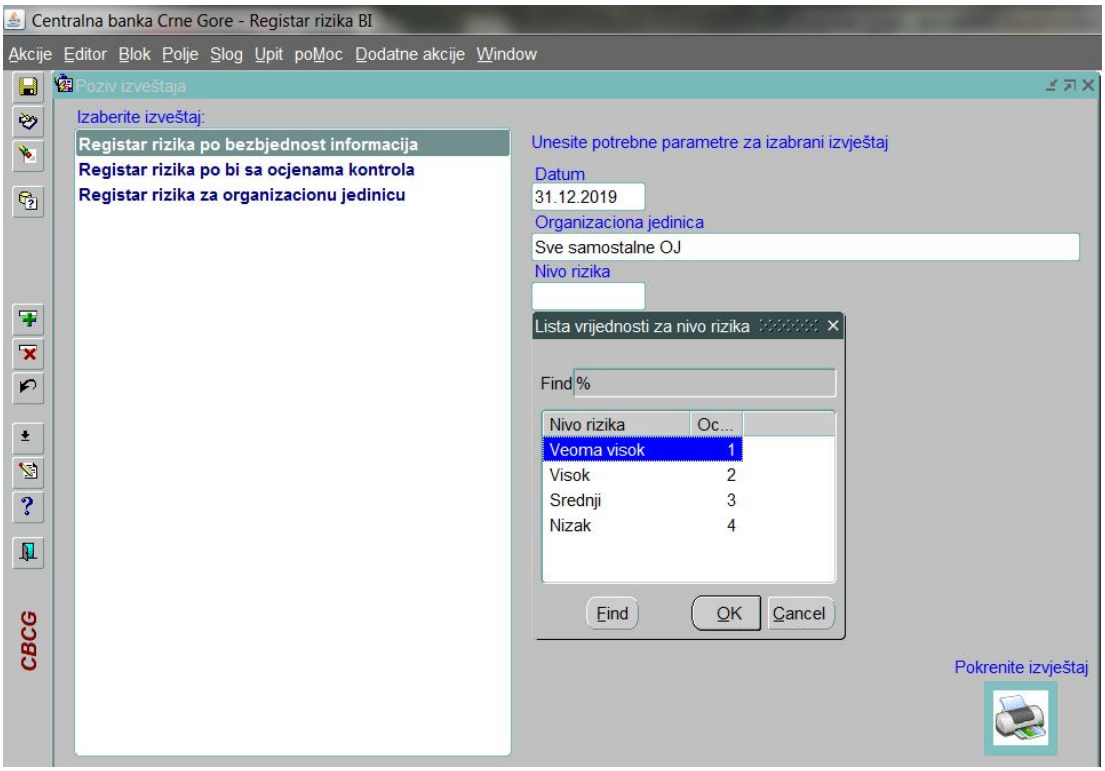
Slika 42: Izvještaji

Ova funkcija podsistema realizuje se kroz dvije aplikacije za izvještavanje:

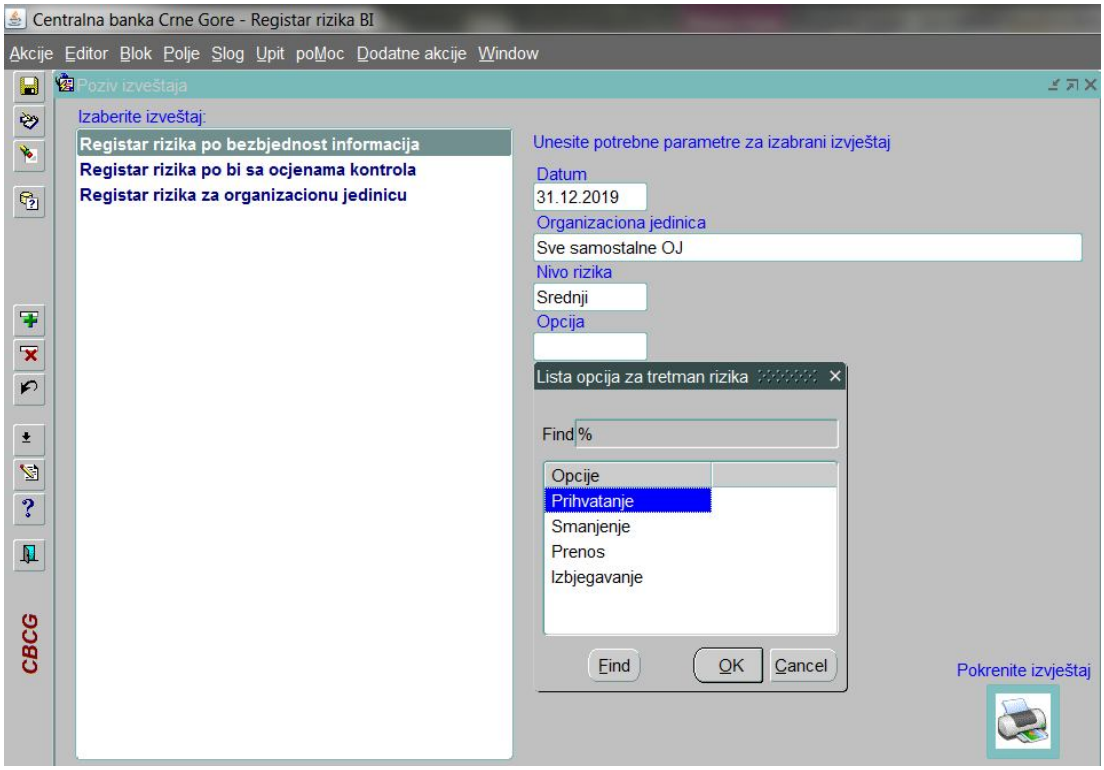
- **Izvještaji –** namijenjena je Direkciji i omogućava štampanje Registra i Plana tretmana rizika sa i bez ocjena efektivnosti kontrola, za zadati datum, uz mogućnost pokretanja izvještaja za određenu organizacionu jedinicu, ili za sve organizacione jedinice, i dodatnog filtriranja podataka po nivou rizika i po izabranoj opciji za tretman rizika. Na ovim izvještajima se izlistavaju samo dokumenti koji su proslijeđeni Direkciji, a u dokumentima samo resursi čija je procijenjena vrijednost veća ili jednaka 12.
- **Izvještaji – organizacione jedinice –** namijenjena je samostalnim OJ i prilikom pokretanja automatski preuzima parametar OJ kojoj pripada zaposleni koji je prijavljen na aplikaciju. Na taj način samostalne OJ imaju štampu sopstvenog Registra i plana tretmana rizika po bezbjednost informacija, na odabrani datum, uz mogućnost filtriranja po nivou rizika i po izabranoj opciji za tretman rizika. Na ovim izvještajima se izlistavaju samo dokumenti koji su proslijeđeni Direkciji, a na dokumentima svi resursi koje je ta samostalna OJ identifikovala i evidentirala, nezavisno od procijenjene vrijednosti resursa.



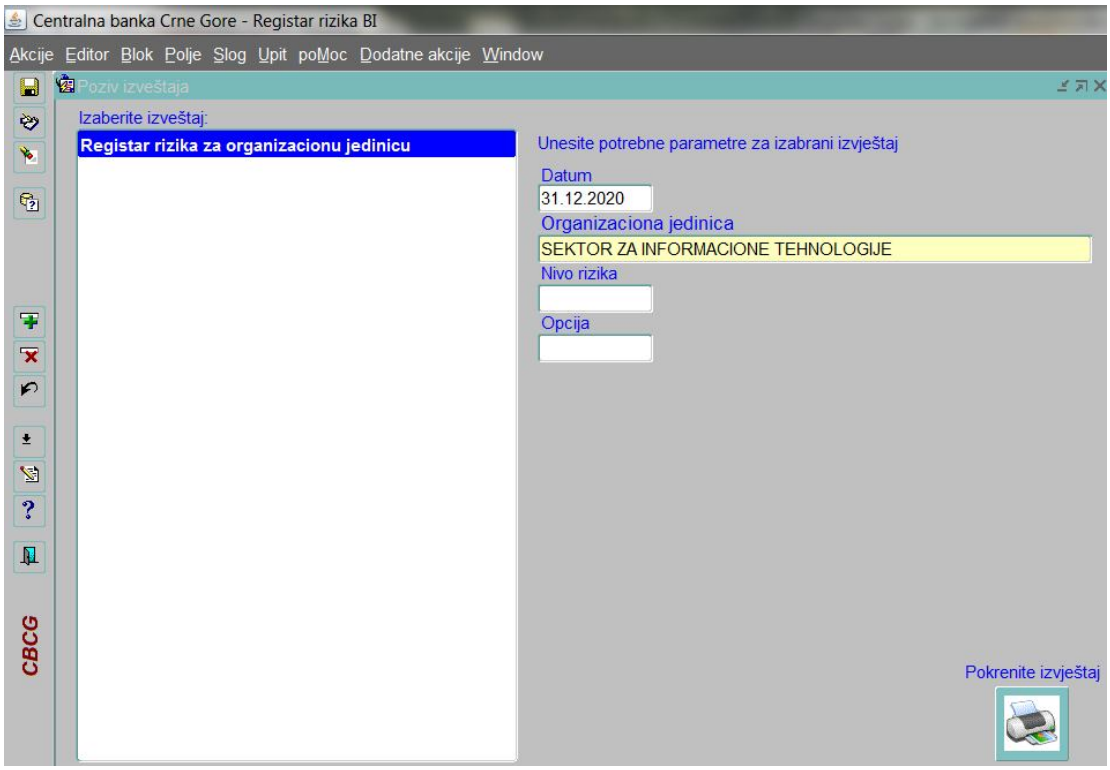
Slika 43: Izvještaji - – Mogućnost dodatnog filtriranja po datumu i OJ



Slika 44: Izvještaji – Mogućnost dodatnog filtriranja po Nivou rizika



Slika 45: Izvještaji – Mogućnost dodatnog filtriranja po opciji tretmana rizika



Slika 46: Izvještaji. – organizacione jedinice

Centralna banka Crne Gore
SEKTOR ZA INFORMACIONE TEHNOLOGIJE

Datum izvjestaja: 18.04.2018
Strana 1 od 2

Registar rizika po bezbjednost informacija i plan tretmana rizika na 31.12.2020. godine

Organizaciona jedinica **SEKTOR ZA INFORMACIONE TEHNOLOGIJE**

Kategorija resursa	*Resurs*	*Vlasnik*	*C*	*I*	*A*	*Vrijednost resursa*
Informacije	**Procedura IT21 - Održavanje zajedničkih registara**	**Specijalni savjetnik u Sektoru - Nina Đikanovic**	**3**	**3**	**3**	**27**

Prijetnja	*Ranjivost*	*Vjerovatnoća prijetnje*	*Stepen ranjivosti*	*Stepen uticaja*	*Vrijednost rizika*	*Ocjena rizika*	*Nivo rizika*
Gubitak dokumenata/medijuma sa informacijama	**Nedostatak kopije/backup-a**	**1**	**1**	**1**	**28**	**3**	**Srednji**

Postojeće kontrole	*Opcija*
kontrola procesa	Prihvatanje

Kategorija resursa	*Resurs*	*Vlasnik*	*C*	*I*	*A*	*Vrijednost resursa*
Softver	**BackOffice - Platni sistem**	**Sef Odjeljenja za razvoj aplikativnih sistema - Elvis Dizdarevic**	**2**	**2**	**3**	**12**

Prijetnja	*Ranjivost*	*Vjerovatnoća prijetnje*	*Stepen ranjivosti*	*Stepen uticaja*	*Vrijednost rizika*	*Ocjena rizika*	*Nivo rizika*
Maliciozni softver	**Neažuriranje antivirusnog softvera**	**3**	**3**	**3**	**54**	**2**	**Visok**

Postojeće kontrole	*Opcija*	*Tretman*	*Odgovoran*	*Rok*
firewall	Prenos	upgrade	Specijalni savjetnik u Direkciji-Vladimir Cadjenovic	09.08.2018

Prijetnja	*Ranjivost*	*Vjerovatnoća prijetnje*	*Stepen ranjivosti*	*Stepen uticaja*	*Vrijednost rizika*	*Ocjena rizika*	*Nivo rizika*
Neovlašćen pristup podacima	**Komplikovan korisnički interfejs**	**3**	**3**	**3**	**39**	**3**	**Srednji**

Postojeće kontrole	*Opcija*
kontrola pristupa	Prihvatanje

Prijetnja	*Ranjivost*	*Vjerovatnoća prijetnje*	*Stepen ranjivosti*	*Stepen uticaja*	*Vrijednost rizika*	*Ocjena rizika*	*Nivo rizika*
Pogrešan rad softvera	**Nedovoljna obučenost za rad sa softverom**	**2**	**2**	**2**	**35**	**3**	**Srednji**

Postojeće kontrole	*Opcija*	*Tretman*	*Odgovoran*	*Rok*
kontrola softvera	Smanjenje	poboljasanje kontrola	Specijalni savjetnik u Sektoru-Nina Đikanovic	09.08.2018

	Vjerovatnoća prijetnje	*Stepen ranjivosti*	*Stepen uticaja*	*Vrijednost rizika*	*Ocjena*	*Nivo rizika*	*Komentar*
Ocjena efektivnosti kontrola	2	1	1	29	3	Srednji	TEST

Slika 47: Registar i Plan tretmana rizika po bezbjednost informacija za samostalnu OJ na izabrani datum

6. Analiza informacionog sistema za upravljanje rizicima po bezbjednost informacija sa smjernicama za budući razvoj

6.1. Moguća unapređenja informacionog sistema za upravljanje rizicima po bezbjednost informacija

U prethodnoj glavi detaljno su opisane funkcionalnosti razvijenog informacionog sistema za upravljanje rizicima po bezbjednost informacija koji se već upotrebljava u Centralnoj banci Crne Gore. Benefiti postojanja ovog informacionog sistema su višestruki, [57]. Naime, za svaku kategoriju informacijskih resursa je moguće definisati set mogućih prijetnji i ranjivosti koji se mogu javiti za tu kategoriju resursa čime je sprovedena katalogizacija prijetnji i ranjivosti na nivou Centralne banke Crne Gore. S druge strane, za svaku od kategorija informacijskih resursa definisan je posebni skup vrijednosti iz koga se može izabrati mogući informacijski resurs. Upotrebom ovog informacionog sistema, svaka samostalna organizaciona jedinica Centralne banke za određeni datum kraja izvještajnog perioda kreira jedinstveni dokument koji predstavlja Registar i Plan tretmana rizika po bezbjednost informacija za tu organizacionu jedinicu i prosljeđuje ga nadležnoj Direkciji. Nadležna Direkcija ima mogućnost da, ukoliko za tim postoji potreba, vrati dokument na doradu organizacionoj jedinici koja ga je proslijedila, o čemu organizaciona jedinica biva obaviještena e – mail porukom koja se automatski šalje iz aplikativne forme. Uvođenjem informacionog sistema, poslovni proces upravljanja rizikom po bezbjednost informacija je u potpunosti uređen, unaprijeđen u odnosu na vrijeme prije uvođenja informacionog sistema i automatizovan, [57]. Pored toga, Centralna banka je kroz ovakav način kreiranja dokumenata dobila bazu potpuno sistematizovanih podataka o identifikovanim informacijskim resursima.

Ipak, postoji segment u kojem je moguće unaprijediti uvedeni informacioni sistem. Taj segment se odnosi na mail notifikaciju koja se automatski generiše prilikom vraćanja dokumenta na doradu i može se unaprijediti sa dva aspekta.

Prvo, e – mail poruka koja se šalje, mogla bi da sadrži i listu nepravilnosti zbog kojih je dokument vraćen, kao i listu odgovarajućih korekcija koje organizaciona jedinica treba da implementira na

dokumentu. Pomenuta izmjena bi podrazumijevala izradu aplikativne forme koja bi bila namijenjena nadležnoj Direkciji i pokretala se prilikom vraćanja dokumenta na doradu. Ova forma bi sadržala dva polja sa mogućnošću unosa više zapisa i dugme **Pošalji**. Prvo polje **Polje za korekciju** bi sadržalo informaciju o nazivu polja na vraćenom dokumentu čiji sadržaj treba promijeniti i popunjavalo bi se biranjem iz liste naziva svih polja na dokumentu. Drugo polje **Korekcija** bi bilo predviđeno za upisivanje korigovanog podatka. Pritiskom na dugme **Pošalji** bi se čuvali evidentirani podaci, a zatim se slala e – mail poruka u kojoj bi ti podaci bili ispisani.

Dalje, funkcionisanje informacionog sistema za upravljanje rizikom po bezbjednost informacija moglo bi biti unaprijeđeno kriptovanjem e – mail poruka koje se šalju. Kriptovanje onemogućava dešifrovanje i razumijevanje izvorne poruke ukoliko se desi zlonamjerni upad u komunikacioni kanal. Kriptografija javnog ključa dostupna je u više oblika, ali zahtijeva ogromnu potrošnju vremena, složenost i veliku računsku snagu. Pokazalo se da realizacija kriptovanja upotrebom vještačkih neuralnih mreža (Artifical Neural Networks - ANN) može biti najbolji način za prevladavanje navedenih problema, [69]. U tom smislu ovo unapređenje informacionog sistema bi podrazumijevalo odabiranje i treniranje odgovarajuće neuralne mreže za kriptovanje i dekriptovanje e – mail poruka. Iz tog razloga, dio teze koji slijedi će biti posvećen neuralnim mrežama.

6.2. Neuralne mreže

Neuralne mreže su interesantne i sa aspekta samog procesa bezbjednosti informacija. S obzirom da je najveći broj rizika nemoguće izbjeći, od vitalnog značaja je efikasno upravljanje rizicima. Jedan od načina da se unaprijedi upravljanje rizicima jeste predviđanje pojavljivanja prijetnji, a u skladu sa tim i procjena rizika koji te prijetnje izazivaju. Procjena rizika je složen i nelinearni proces koji podrazumijeva sprovođenje analize u realnom vremenu. Zbog toga se u procesu procjene rizika za predikciju i ispitivanje sve češće upotrebljavaju vještačke neuralne mreže, [69], [70]. Odlični rezultati koje neuralne mreže postižu pri tretiranju nelinearnih problema, kao i njihova sposobnost učenja čine ih veoma atraktivnim za primjenu u oblasti procjene rizika po bezbjednost informacija.

6.2.1. Istorija nastanka, pojam i definicije neuralnih mreža

U savremenom dobu, za obradu gotovo svih podataka, koju ne vršimo pomoću svog uma, upotrebljavamo računar. Preciznije rečeno cjelokupna automatska obrada podataka sprovodi se

upotrebom računara. Na prvi pogled djeluje da najveći dio podataka obrađuju računari. Međutim, ukoliko uzmemo u obzir količinu podataka koja se svakodnevno obradi u mozgu, ne samo čovjeka, već i drugih bića, shvatamo da je količina podataka koji se taj način obrađuju neuporedivo veća. Prethodno poređenje u potpunosti objašnjava nastanak ideje da se osmisli koncepcija za obradu podataka koja bi se zasnivala na logici funkcionisanja koja podražava mozak živih bića. Na taj način se došlo do pojave pojma vještačke inteligencije. Cilj razvoja vještačke inteligencije jeste kreiranje funkcionalne imitacije ljudskog mozga jer on predstavlja najviši stepen inteligencije koji je do sada poznat, [65]. Čovjek je sposoban da na osnovu znanja koje posjeduje, kao i na osnovu prethodnog iskustva, izvrši izbor, odnosno donosi odluke. Ne manje važna je i čovjekova sposobnost da kroz proces učenja usvaja nova znanja i na taj način da radi na sebi.

Ljudski mozak je sastavljen od ogromnog broja (oko 100 milijardi), [59], nervnih ćelija – neurona. Neuron je osnovna strukturna i funkcionalna jedinica nervnog sistema koja prenosi i obrađuje podatke. On se sastoji od sljedećih djelova: tijela, dendrita, neurita (akson, nervno vlakno) i nervnih završetaka, [59]. Nervni završeci formiraju anatomske i funkcionalne veze između nervnih ćelija. Te veze se nazivaju sinapse. U mozgu ima oko 60000 milijardi, sinaptičkih veza pri čemu jedna nervna ćelija može ostvariti oko 40000 sa susjednim nervnim ćelijama, [59]. Prema [65], [66], kroz sprovedena neurofiziološka istraživanja došlo se do zaključka da je funkcionisanju mozga najsličniji model u kojem veliki broj procesnih elemenata vrši paralelnu obradu podataka.

Pokušajmo da napravimo poređenje između ljudskog mozga i računara. Ulogu koju u funkcionisanju mozga imaju nervne ćelije, kod modernih računara imaju tranzistori koji su integrisani u jedno kolo, [59]. Prema [59], [67], [68], brzina odziva neurona je reda veličine milisekunde što je šest redova veličine manja brzina u odnosu na onu koja se postiže upotrebom digitalne logike. Iako su njegove strukturne jedinice sporije nego one kod računara, mozak ostvaruje neuporedivo veću brzinu funkcionisanja i to zahvaljujući ogromnom broju tih strukturnih jedinica. Mozak postiže fantastičnu energetsku efikasnost trošeći 10^{-16}J po operaciji u sekundi u odnosu na računar koji troši 10^{-6} J po operaciji u sekundi, [59]. U ljudskom mozgu vrši se distribuirana paralelna obrada podataka, pri čemu je jedna nervna ćelija povezana sa oko 10000 susjednih nervnih ćelija. Iz [59], u računaru se vrši sekvencijalna centralizovana obrada podataka.

U skladu sa [65], koncept obrade podataka zasnovan na imitiranju funkcionisanja ljudskog mozga zove

se vještačkom neuralnom mrežom (engl. Artifical Neural Network - ANN). Istraživači McCulloch i Pitts (Massachusetts Institute of Technology), su kao rezultat istraživanja neurofizioloških karakteristike živih bića, 1940.godine osmislili matematički model neuralne mreže u okviru teorije automata, [65]. To je, ustvari, početak kreiranja koncepta neuralnih mreža. Međutim, praktična realizacija neuralne mreže je izostala jer nijesu postojali računari koji su imali dovoljno veliku snagu procesiranja, [65]. Sredinom šesdesetih godina prošlog vijeka, razvijeni su računari III generacije zasnovani na LSI – Large Scale Integration arhitekturi, što je omogućilo prve praktične realizacije neuralnih mreža. Poslije toga dolazi do prestanka interesovanja za neuralne mreže koje traje skoro dvadeset godina. Istraživanja vezana za neuralne mreže ponovo počinju 1990.godine, objavljivanjem naučnog članka *An introduction to neural computing, I. Alexander, H. Morton.* U savremenom dobu neuralne mreže postaju dominantan koncept prilikom razvoja inteligentnih sistema.

Neuralne mreže su procesori kod kojih se vrši distribuirana paralelna obrada podataka, sa sposobnošću pamćenja empirijskog znanja i mogućnošću njegove upotrebe, [59]. Takođe, pod neuralnom mrežom se može podrazumijevati vještački ćelijski sistem koji ima kapacitivnost da preuzme, zapamti i upotrijebi znanje koje je stekao kroz iskustvo, [59]. U ovom slučaju pojam *znanje* označava sposobnost neuralne mreže da se pri zadatim vrijednostima ulaznih parametara ponaša na zadovoljavajući način. U cilju dobijanja očekivanih izlaznih vrijednosti za određene ulazne vrijednosti, neuralna mreža mora biti podvrgnuta procesu obučavanja odnosno treniranja, [59]. Neophodno je naglasiti da se proces obučavanja neuralne mreže ne završava njenim stavljanjem u funkciju, već se nastavlja i kroz njeno funkcionisanje, [59]. Prema [59], neuron je bazični strukturni element neuralnih mreža. On je, ustvari, bazična komponenta u kojoj se vrši distribuirana obrada podataka unutar neuralne mreže, [59]. U cilju postizanja potpune funkcionalnosti neuralne mreže, ona se realizuje upotrebom velikog broja neurona među kojima postoji veza. Neuroni su povezani tako da podatak koji je za jedan neuron izlazni, za drugi je ulazni, što znači da veza između neurona funkcioniše u jednom smjeru, [59]. U cilju obezbjeđivanja distribuirane obrade podataka bilo bi potrebno hardverski realizovati neuron. Međutim, praktična implementacija neuralnih mreža sprovodi se upotrebom računara baziranih na Von Neumannovoj jednoprocesorskoj arhitekturi. U pomenutim sistemima visoka djelotvornost se ostvaruje izvanredno velikom brzinom sekvencijalne obrade podataka, [67], [68].

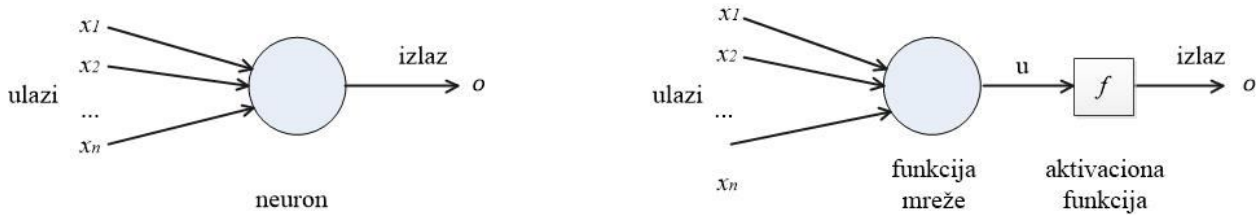
Prednosti neuralnih mreža u odnosu na konvencionalne načine obrade podataka ogledaju se u sljedećim njihovom osobinama, [58]:

- Veoma su uspješne u procjeni nelineranih odnosa uzoraka;
- Imaju mogućnost da rade sa nejasnim ili nepotpunim podacima, kao što su podaci dobijeni iz različitih senzora, kao na primjer kamera i mikrofona, i da u njima identifikuju uzorke;
- Otporni su na greške u podacima, za razliku od konvencionalnih metoda koje polaze od pretpostavke da ulazni podaci imaju normalnu raspodjelu;
- Ukoliko podaci nijesu definisani na eksplicitan simbolički način, neuralne mreže imaju sposobnost da kreiraju sopstvene odnose između podataka;
- Imaju sposobnost da rade sa velikim brojem promjenljivih ili parametara;
- Fleksibilne su u odnosu na okolinu;
- Mogu se realizovati u vidu jednostavne VLSI implementacija;
- Imaju mogućnost da stiču nova znanja na osnovu iskustva.

Neuralne mreže pronalaze svoju primjenu prilikom rješavanja problema klasifikacije i predviđanja što obuhvata sve situacije u kojima se može uočiti veza između ulaznih i izlaznih promjenjivih, bez obzira na kompleksnost odnosno nelinearnost te veze. U savremenom dobu neuralne mreže se upotrebljavaju u medicini, fizici, bankarstvu, mašinstvu, geologiji prilikom raspoznavanje uzoraka, rješavanja problema optimizacije, nelinearnog upravljanja, raznih simulacija, kao i obrade slike, govora i nepreciznih i nepotpunih podataka, [61], [62].

6.2.2. Modeliranje neurona i neuralne mreže

Prema [59], [60] prilikom kreiranja modela neurona najprije se vrši modeliranje njegovih ulaza i izlaza. Tijelo neurona posjeduje informaciju koja se ogleda u razlici električnih potencijala između unutrašnjeg i spoljašnjeg dijela ćelije. Ta razlika iznosi oko -70mV u nepobuđenom stanju. Dakle, i ulazni i izlazni podaci neurona su električni potencijali. S obzirom da je električne potencijale moguće modelirati realnim brojevima, u vještačkim neuralnim mrežama je upotrijebljeno isto pravilo. Istraživači McCulloch i Pitts su uveli model vještačkog neurona, tzv. Threshold Logic Unit (TLU), [59], [60]. Model je koncipiran na sljedeći način: signali su predstavljeni realnim brojevima, pa se na ulazu u neuron množe težinskim koeficijentima i nakon toga sumiraju. Ukoliko se sumiranjem dobije iznos koji je veći od definisanog praga, neuron daje izlazni signal . Na taj način, a u skladu sa [59], [60], neuron utiče na dobijanja jedne izlazne veličine od *N* ulaznih veličina. Taj proces se realizuje kroz dvije etape: u prvoj se kombinacijom *N* ulaznih veličina dobija jedna veličina *u,* a u drugoj etapi na osnovu vrijednosti te veličine se dobija izlazna veličina *i.* Obrazac po kome se dobija vrijednost *u* naziva se funkcija mreže, a obrazac po kome se određuje izlazna veličina naziva se aktivaciona funkcija.



Slika 49: Model neurona

Funkcija mreže je nosilac znanja koje neuron posjeduje. Grafički prikaz opisanog modela neurona dat je na slici 49.

6.2.2.1. Funkcija mreže

Kao što je već navedeno, funkcija mreže definiše način na koji se kombinuju ulazne veličine. Zbog svoje jednostavnosti, [63], najčešće se koristi linearna funkcija mreže koja predstavlja linearnu kombinacija *N* ulaznih veličina sa težinskim koeficijentima *w*. U opštem slučaju vrijednost funkcije mreže ne zavisi samo od ulaznih veličina, već i od stanja u kome se nalazi neuron. To stanje se opisuje pomoću realne veličine θ koja se naziva "bias" ili prag. Uticaj stanja neurona na izlaznu linearnu funkciju može se uzeti u obzir uvođenjem dodatne ulazne *N*+1 veličine x_0, za koju važi da je uvijek jednaka 1. Na taj način bias se modelira težinskim koeficijentom w_0, pri čemu tada važi da neuron ima bias jednak nuli. Napomenimo da se znanje nalazi u težinskim koeficijentim w_i funkcije mreže. Funkcija mreže može biti data u nekom od sljedećih oblika: linerna $u = \sum_{i=1}^{n} w_i x_i + \theta$, linearna forma II reda $u = \sum_{i=1}^{n} \sum_{k=1}^{n} w_{ik} x_i x_k + \theta$, proizvod $u = \prod_{i=1}^{N} x_i^{w_i}$.

6.2.2.2. Aktivaciona funkcija

Aktivaciona funkcija ima ulogu da vrijednost funkcije mreže uobliči tako da se na izlazu dobije odgovarajuća vrijednost, [63]. U najvećem broju slučajeva zahtijeva se da raspon u kojem se mogu kretati vrijednosti izlaznih veličina bude ograničen. U tom cilju, vrijednosti aktivacionih funkcija su realni brojevi koji se najčešće kreću između 0 i 1 ili -1 i 1. To se najčešće sprovodi upotrebom aktivacionih funkcija čije su vrijednosti realni brojevi koji kreću između 0 i 1 ili -1 i 1. U skladu sa tim, unipolarna funkcija praga, $f(u) = \begin{cases} 1, & u > 0 \\ 0, & u < 0 \end{cases}$, i unipolarni sigmoid, $f(u) = 1/(1+e^{-u})$, su aktivacione funkcije najveće važnosti.

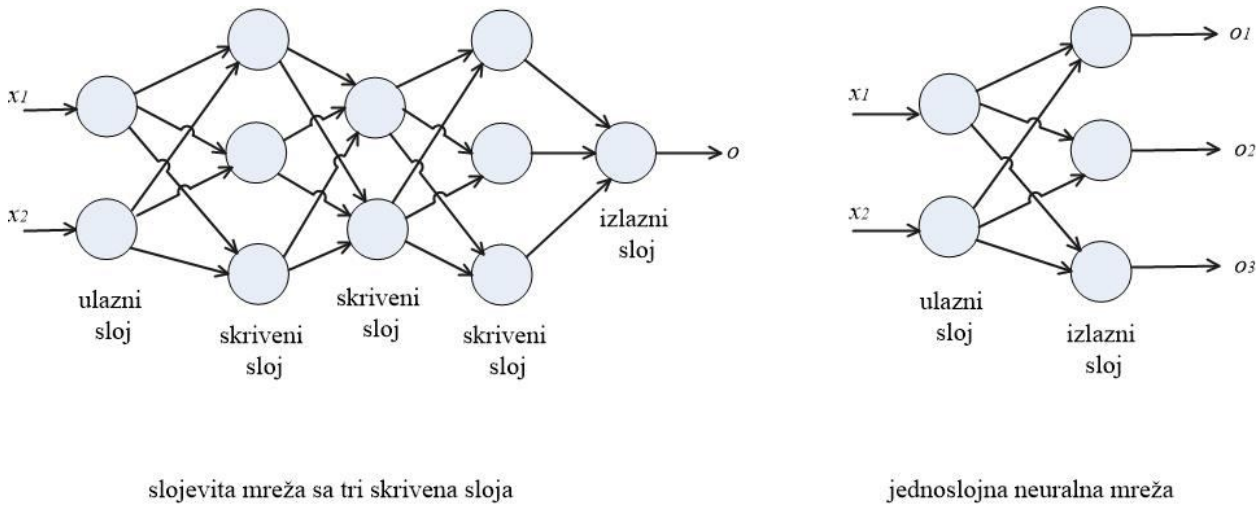
6.2.2.3. Struktura neuralne mreže

Neuralna mreža sastoji se od velikog broja neurona koji su povezani među sobom kao i sa ulaznim signalima, [64]. Tok signala kroz neuralne mreže može se prikazati orjentisanim grafom pri čemu su čvorovima grafa prikazani neuroni, a granama grafa tokovi signala. Specifičnu vrstu grana grafa predstavljaju ulazne i izlazne grane grafa, koje ne počinju odnosno ne završavaju se neuronom. Ulazne grane su grane grafa koje počinju čvorom van neuralne mreže namijenjenim za prikupljanje električnih signala koji reprezentuju neku fizičku pojavu - ulaznim čvorom. Izlazne grane su grane grafa koje se završavaju čvorom grafa koji reprezentuje izlaznu informaciju iz neuralne mreže.

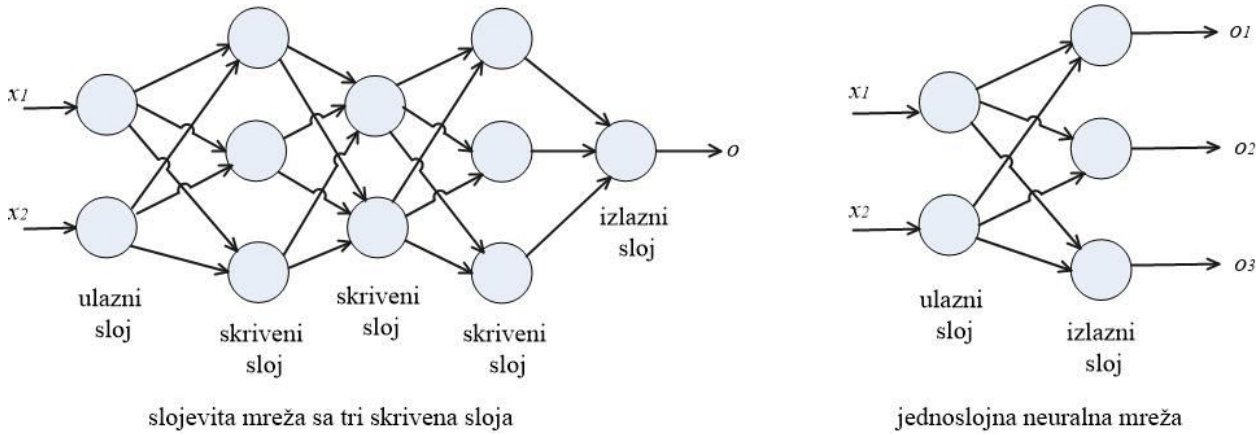
U odnosu na to da li graf kojim je neuralna mreža predstavljena sadrži zatvorene konture ili ne, neuralne mreže svrstavamo u ciklične - mreže s povratnom vezom (engl. recurrent net) ili aciklične (engl. feedforward net), [64]. Mreže sa povratnom vezom nemaju ulazni i izlazni sloj neurona, već kod njih postoje vidljivi čvorovi koji komuniciraju sa okolinom i skriveni čvorovi. Takve neuralne mreže upotrebljavaju se za modeliranje nelinearnih dinamičkih sistema – sistema sa memorijom. Zbog nelinarne prirode aktivacionih funkcija ovakvih sistema, projektovanje i obučavanje cikličnih neuralnih mreža je veoma komplikovano.

Posmatrajući aciklične mreže napomenimo da posebnu vrstu ovih mreža predstavljaju slojevite neuralne mreže kod kojih su neuroni podijeljeni u slojeve tako da izlazne informacije jednog sloja istovremeno predstavljaju ulazne informacije za sloj koji slijedi. Informacije sa ulaza mreže prosljeđuju se na ulaz prvog sloja neurona, a izlazi posljednjeg sloja neurona su, ustvari, izlazne informacije iz neuralne mreže. Neuralne mreže koje sadrže jedan ili dva sloja neurona su najjednostavnije slojevite neuralne mreže. Matematički model za analizu višeslojnih neuralnih mreža zasniva se na pretpostavci da izlazi iz svih neurona koji pripadaju $N-1$ sloju predstavljaju ulaze neurona koji pripadaju N - tom sloju.

Ukoliko želimo da modeliramo slučaj u kojem sve ulazne vrijednosti nemaju uticaj na stanje nekog neurona, to sprovodimo tako što težinskim koeficijentima u funkciji mreže neurona dodijelimo nulte vrijednosti. Prilikom upotrebe slojevitih neuralnih mreža, često se uvodi i nulti, ulazni, sloj koji je sastavljen od neurona u kojima se ne sprovodi procesuiranje podataka. Kod neurona koji pripadaju nultom sloju vrši se prosljeđivanje informacija sa ulaza na izlaz. Posljednji sloj neuralne mreže je izlazni sloj.



Slika 50: Topologija neuralne mreže



Slika 51: Slojevite neuralne mreže

6.2.2.4. Obučavanje neuralne mreže sa nadgledanjem

Da bi se neuralna mreža prilagodila za izvršavanje određenih zadataka sprovodi se obuka ili treniranje mreže, [65], [66]. Postupku treniranja prethodi prikupljanje podataka za treniranje mreže i inicijalizacija mreže. Pomenuti podaci obuhvataju parove ulaz - izlaz, takve da se do izlaznih podataka dolazi eksperimentalnim putem, metodom pretpostavke ili estimacijom na bazi iskustva. Skup podataka mora biti konačan. Smatrajmo da je broj parova ulaz - izlaz jednak K. Prilikom inicijalizacije mreže parametri neurona se uzimaju slučajno, osim u slučajevima kada se unaprijed zna kako ih treba zadati. Poslije ovih koraka počinje postupak treniranja koji se realizuje prema algoritmu koji se sastoji od nekoliko iteracija. U prvoj iteraciji, iz skupa ulaznih podataka bira se par ulaz-izlaz, pa se izračunava izlaz iz neuralne

mreže. Izračunati izlaz se upoređuje sa željenim izlazom. Ako je izračunati izlaz neuralne mreže jednak željenom izlazu ili se veoma malo razlikuje od njega, korekcija mreže se ne sprovodi. Ako se poređenjem utvrdi da se željeni i dobijeni izlaz razlikuju toliko da se ta razlika ne može tolerisati, neophodno je sprovesti korekciju parametara neuralne mreže u cilju postizanja boljeg rezultata. U drugoj iteraciji, uzima se sljedeći par ulaz-izlaz i za taj par se sprovodi postupak iz prve iteracije. Ovaj ciklus treniranja naziva se epoha. Epoha se završava kada upotrijebimo sve parove iz skupa podataka koji služe treniranju mreže. U trećoj iteraciji se analizira cjelokupni rezultat koji je neuralna mreža postigla u realizovanoj epohi. U slučaju da je dobijen zadovoljavajući izlaz neuralne mreže za svih K analiziranih slučajeva, završeno je treniranje mreže. Ukoliko nije tako, neophodno je vratiti se na prvu iteraciju odnosno sprovesti narednu epohu treniranja.

Napomenimo da algoritam treniranja neuralne mreže ne mora konvergirati. On se mijenja tako što se unaprijed odredi maksimalni broj epoha treniranja. Ako neuralna mreža i poslije provođenja postupka treniranja ne ostvaruje prihvatljive rezultate, postupak se ponavlja tako što polazni parametri mreže inicijalizuju drugim vrijednostima. Najveći problem koji se javlja u postupku treniranja neuralne mreže jeste da se utvrdi kako modifikovati parametre mreže ako ne dobijamo željeni rezultat, [69], [70]. U nekim situacijama se pokazalo da je korisno dodati i slučajnu korekciju koja ne zavisi od realne greške, pri čemu treba napomenuti da se radi o maloj vrijednosti korekcije. Uvođenjem pomenute korekcije moguće je izbjeći dobijanje nezadovoljavajućih rezultata zbog obustavljanja procesa treniranja na lokalnom minimumu greške.

6.2.2.5. Jednoslojna neuralna mreža sa binarnim vrijednostima na izlazu - Perceptron

Perceptron je jednoslojna neuralna mreža čiji je zadatak da utvrdi da li ulazni podaci posjeduju ispitivanu osobinu odnosno da li pripadaju određenoj klasi, [64]. Imajući u vidu da je podatak koji se dobija na izlazu mreže logička vrijednost, dolazi se do zaključka da za aktivacionu funkciju neurona treba izabrati funkciju koja ima binarne izlazne vrijednosti. Ta funkcija može biti unipolarna ili bipolarna funkcija praga. Zbog jednostavnosti, za aktivacionu funkciju izabraćemo unipolarnu funkciju:

$$f(u)=\begin{cases}1, & u>0\\ 0, & u<0\end{cases}$$

Tada se, uz pretpostavku da perceptron ima N ulaznih veličina, mrežna funkcija perceptrona može predstaviti u obliku linearne forme: $u(x_1,x_2,...,x_N)=\sum_{k=1}^{N} w_k x_k$. ”Znanje” koje mreža stiče kroz

postupak obučavanja ugrađeno je u težinske koeficijente w_k. Ukoliko ulazne veličine i težinske koeficijente predstavimo u obliku vektora

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{bmatrix}$$

$$W = \begin{bmatrix} w_1 & w_2 & \cdots & w_N \end{bmatrix}_{1\times N}$$

tada funkciju mreže zapisujemo kao $u = W \cdot X$, a izlaz neurona kao $o = f(u) = f(W \cdot X)$. Esencijalno perceptron sadrži jedan neuron te je on primjer aciklične, jednoslojne neuralne mreže.

Međutim, prema [64], možemo analizirati perceptron koji sadrži više neurona tako što ga tretiramo kao jednoslojnu mrežu koja ima M izlaza tako da može da ispita da li ulazni podaci imaju neku od M osobina. Tada se izlaz mreže može zapisati kao vektor kolona od M elemenata, $o = \begin{bmatrix} o_1 & o_2 & \cdots & o_M \end{bmatrix}_T$, a težinski koeficijenti pojedinih neurona W_l, $l = 1,...,M$, mogu se zapisati u obliku matrice:

$$W = \begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_M \end{bmatrix} = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1N} \\ w_{21} & w_{22} & \ddots & w_{2N} \\ \vdots & \vdots & \cdots & \vdots \\ w_{M1} & w_{M2} & \cdots & w_{MN} \end{bmatrix}_{M\times N}$$

Na kraju dolazimo do jednostavne veze izlaza i ulaza:

$$o = f(W \cdot X)$$

Posmatrajmo ponovo perceptron koji sadrži jedan neuron. Neka tokom procesa treniranja za ulaz X_k dobijamo izlaz o_k, pri čemu je željeni izlaz d_k. Uporedimo o_k sa d_k. Uočavamo situaciju kada je $o_k = d_k$, pa ne treba korigovati koeficijente mreže W i situaciju $o_k \neq d_k$ kada koeficijente mreže treba korigovati. Tada je $W_{novo} = W_{staro} + \Delta W$, a korekciju ΔW treba odrediti tako da vrijednost stvarnog izlaza bude što bliža vrijednosti željenog izlaza. U posmatranom slučaju na izlazu se mogu dobiti samo dvije vrijednosti, 0 ili 1, jer je izlazna vrijednost definisana unipolarnom aktivacionom funkcijom. Neka je na izlazu dobijena vrijednost 0, a želimo da dobijemo vrijednost 1. Ako je na izlazu dobijena vrijednost 0, znači da važi $WX < 0$, a želimo da bude $WX > 0$. Nameće se zaključak da treba korigovati koeficijente mreže tako da se vrijednost WX poveća. Analogno tome, ako na izlazu imamo vrijednost 1,

a želimo da dobijemo vrijednost 0, koeficijente mreže treba korigovati tako da se vrijednost WX smanji. Dakle, korekcija koeficijenata mreže se može sprovesti prema jednačini:

$$W_{novo} = W_{staro} + \mu(d_k - o_k)X^T$$

Za prvi slučaj koji smo posmatrali, prethodna jednačina dobija oblik

$$W_{novo} = W_{staro} + \mu X^T$$

Dalje slijedi $W_{novo}X = W_{staro}X + \mu X^T X = W_{staro}X + \mu||X||$, gdje $||X||$ označava sumu kvadrata koordinata vektora X odnosno normu vektora X. To znači da je vrijednost WX povećana za $\mu||X||$. Za drugi slučaj, vrijednost WX će biti smanjena za $\mu||X||$. Koeficijent μ se naziva koeficijent učenja neuralne mreže i njegova vrijednost je pozitivan broj. Brzina konvergencije algoritma treniranja mreže veoma zavisi od toga koju vrijednost izaberemo za ovaj koeficijent.

6.2.2.6. Jednoslojna neuralna mreža sa kontinualnim izlaznim vrijednostima

Kod ove vrste neuralnih mreža na izlazu dobijamo vrijednosti koje pripadaju kontinualnom podskupu skupa realnih brojeva, [59]. Za razliku od perceptrona, kod ovih mreža ne možemo očekivati da postignemo da stvarni izlaz bude jednak željenom, već je cilj postizanje minimalne greške.
Jedan primjer ovakvog tipa mreže jeste mreža kod koje je aktivaciona funkcija oblika unipolarnog sigmoida

$$f(u) = \frac{1}{(1+e^{-u})}.$$

Da bismo izmjerili razliku između stvarnog i željenog izlaza, upotrijebićemo kvadrat greške:

$$E = \frac{1}{2}(d_k - o_k)^2,$$

pri čemu konstanta $\frac{1}{2}$ ima ulogu da pojednostavi izračunavanja. Za smanjivanje greške mogu se upotrijebiti različite metode. Neke od njih su Njutnova metoda, metoda konjugovanog gradijenta i metoda najbržeg spuštanja.

Posmatrajmo neuralnu mrežu koja se sastoji od jednog neurona sa N ulaza. Pretpostavimo da su ulazni podaci dati u obliku vektora X_k, a da je željeni izlaz d_k . Stvarni izlaz neurona se dobija po formuli:

$$o_k = f(u) = f(W \cdot X) = f\left(\sum_{i=1}^{n} w_i x_i\right)$$

a greška koja se čini data je izrazom

$$E = \frac{1}{2}(d_k - o_k)^2 = \frac{1}{2}(d_k - f\left(\sum_{i=1}^{n} w_i x_i\right))^2 .$$

Upotrebljavajući metodu najbržeg spuštanja za minimizaciju greške dobijamo

$$w_{i,(novo)} = w_{i,(staro)} - \mu \frac{\partial E}{\partial w_i}$$

$$W_{novo} = W_{staro} - \mu \frac{\partial E}{\partial w_i},$$

gdje je $\frac{\partial E}{\partial w_i}$ gradijent funkcije greške. Polazeći od formule za grešku, dolazimo do izvoda

$$\frac{\partial E}{\partial w_i} = -(d_k - o_k)\frac{\partial o_k}{\partial w_i} = -(d_k - o_k) f'(\sum_{i=1}^{n} w_i x_i) x_i .$$

Ukoliko je aktivacionu funkciju oblika unipolarnog sigmoida, dobijamo

$$f'(u) = \frac{d}{du}\frac{1}{1+e^{-u}} = -\frac{-e^{-u}}{(1+e^{-u})^2} = \frac{1}{1+e^{-u}}\frac{e^{-u}}{1+e^{-u}} = f(u)(1-\frac{1}{1+e^{-u}}) = f(u)(1-f(u)).$$

Uzimajuću u obzir prethodnu formulu i koristeći $o_k = f\left(\sum_{i=1}^{n} w_i x_i\right)$, dolazimo do

$$\frac{\partial E}{\partial w_i} = -(d_k - o_k) o_k (1-o_k) x_i .$$

Kao rezultat sprovedenih matematičkih izvođenja dobili smo formulu koja predstavlja pravilo učenja mreže:

$$w_{i,(novo)} = w_{i,(staro)} + \mu(d_k - o_k) o_k (1-o_k) x_i .$$

Možemo je zapisati i u vekorskom obliku:

$$W_{novo} = W_{staro} + \mu(d_k - o_k) o_k (1-o_k) X^T .$$

Označavajući $(d_k - o_k) o_k (1-o_k)$ sa δ_k , zapis pravila učenja dobija oblik koji se naziva delta pravilo:

$$W_{novo} = W_{staro} + \mu\delta_k X^T$$

Ako je aktivaciona funkcija oblika bipolarnog sigmoida $f(u) = \frac{2}{1+e^{-2u}} - 1 = \frac{1-e^{-2u}}{1+e^{-2u}}$.

Prvi izvod aktivacione funkcije je:

$$f'(u) = \frac{4e^{-2u}}{(1+e^{-2u})^2} = \frac{(1+e^{-2u})^2 + 4e^{-2u} - (1+e^{-2u})^2}{(1+e^{-2u})^2} = 1 - \frac{(1+2e^{-2u}+e^{-4u}) - 4e^{-u}}{(1+e^{-2u})^2}$$

$$f'(u) = 1 - \frac{(1-e^{-2u})^2}{(1+e^{-u})^2} = 1 - f^2(u)$$

i dobija se $\delta_k = (d_k - o_k)(1 - o_k{}^2)$.

6.2.2.7. Višeslojne mreže

Kod višeslojnih neuralnih mreža je moguće grupisati neurone u slojeve, pri čemu postoji bar jedan skriveni sloj neurona, [61]. Pod skrivenim slojem neurona podrazumijeva se sloj čiji se izlazi ne pojavljuju na izlazu neuralne mreže. Prilikom obučavanja ovih mreža znaju se parovi ulaznih i izlaznih podataka mreže, ali su nepoznati izlazi skrivenih neurona. Za obučavanje višeslojnih mreža često se koristi metoda koja se naziva algoritam sa širenjem greške unazad – backpropagation algoritam, [61]. Pomenuti algoritam inverznim putem transformiše grešku na izlaznom sloju neurona u grešku na izlazima prethodnog sloja. Računajući grešku svakog neurona, algoritam širi grešku od izlaznog sloja ka ulaznom, odnosno unazad kroz mrežu.

U cilju objašnjenja načina rada ovog algoritma posmatrajmo dvoslojnu neuralnu mrežu takvu da skriveni sloj mreže sadrži M, a izlazni sloj jedan neuron. Pretpostavimo da mreža ima N ulaza, da je mrežna funkcija definisana kao linearna kombinacija tih ulaza i da je aktivaciona funkcija unipolarni sigmoid. Uočimo jedan par ulaz-izlaz (X_k, d_k) za obučavanje mreže, tada se izlazi iz skrivenog sloja mogu računati prema formuli

$$O_k = f(WX_k)$$

u kojoj O_k označava vektor od M izlaznih veličina, a $W_{M\times N}$ matricu težinskih koeficijenata neurona u skrivenom sloju. Slijedi da se izlaz neuralne mreže može dobiti kao

$$o_k = f(VO_k) = f(Vf(WX_k))$$

Gdje $V_{1\times M}$ označava vektor težinskih koeficijenata izlaznog neurona. Napravljenu grešku definišemo formulom

$$E=\frac{1}{2}(d_k-o_k)^2,$$

u kojoj je d_k željena vrijednost izlaza. Korigujući koeficijente V metodom najbržeg spuštanja, dobijamo:

$$v_{m,(novo)}=v_{m,(staro)}-\mu\frac{\partial E_k}{\partial v_m}$$

pri čemu je

$$\frac{\partial E_k}{\partial v_m}=-(d_k-o_k)f'(VO_k)O_{k,m}=-(d_k-o_k)o_k(1-o_k)O_{k,m},$$

a $O_{k,m}$ je m-ti element vektora o_k. Na kraju dolazimo do:

$$V_{novo}=V_{staro}+\mu(d_k-o_k)o_k(1-o_k){O_k}^T$$

Uzimajući $\delta_k=(d_k-o_k)o_k(1-o_k)$, dobijamo:

$$V_{novo}=V_{staro}+\mu\delta_k{O_k}^T.$$

Uočimo u skrivenom sloju neuron čiji je indeks n. Njegovi težinski koeficijenti nalaze se u n-toj vrsti matrice W, pa ćemo ih obilježiti sa W_n Sprovešćemo korekciju tih koeficijenta pravilom najbržeg spuštanja

$$w_{np,(novo)}=w_{np,(staro)}-\mu\frac{\partial E_k}{\partial w_{np}},$$

gdje je

$$\frac{\partial E_k}{\partial w_{np}}=-(d_k-o_k)f'(Vf(WX_k))Vf'(WX_k)X_{kp}$$

a sa X_{kp} je obilježen p-ti elemenat ulaznog vektora X_k Imajući u vidu da je da je $O_k=f(WX_k)$ dolazimo do

$$\frac{\partial E_k}{\partial w_{np}}=-(d_k-o_k)o_k(1-o_k)V\left[O_{k.}*(1-O_k)\right]X_{kp},$$

gdje množenje u uglastoj zagradi $O_{k.}*(1-O_k)$ označava množenje vektora element po element.

Konačno utvrđujemo pravilo za korekciju koeficijenata uočenog neurona:

$$W_{n,(novo)} = W_{n,(staro)} + \mu(d_k - o_k)o_k(1-o_k)V\left[O_{k.} * (1-O_k)\right]{X_k}^T$$

$$W_{n,(novo)} = W_{n,(staro)} + \mu\delta_k V\left[O_{k.} * (1-O_k)\right]{X_k}^T$$

Prethodno opisani redosljed koraka se može primijeniti i na neuralne mreže koje sadrže više od dva sloja nerona. Suština je da se izračunata greška u poslednjem sloju neurona upotrebljava za korekciju koeficijenata tog sloja, a nakon toga i za korekciju koeficijenata svih slojeva ispod njega. Na taj način, inverznim putem, uticaj izlazne greške svodimo na korekciju koeficijenata pojedinih slojeva neurona.

6.2.3. Primjena neuralnih mreža u enkripciji i dekripciji podataka

Prema [69], [70], [71], [72], [73], sistemi za kriptovanje i dekriptovanje poruka realizovani upotrebom vještačkih neuralnih mreža pokazali su se veoma efikasnim. Sekvencijalna mašina sa konačnim brojem stanja implementirana pomoću neuralnih mreža je naročito pogodna za realizaciju enkripcije i dekripcije, [69], [70].

Iz [69], sekvencijalna mašina ima n stanja i m - bitni ulaz. Izlaz će se generisati na osnovu ulaza i početnog stanja, a zatim će se stanje mijenjati prema tabeli stanja. Nezavisno od odnosa ulaza i izlaza, izlaz zavisi od početnog stanja. Početno stanje se koristi kao ključ za enkripciju i dekripciju. Za enkripciju i dekripciju se crta dijagram stanja i na osnovu njega se dobija tabela stanja koja se dalje koristi za dobijanje skupa podataka za treniranje mreže, [69]. Skup ulaznih podataka obuhvata sve moguće ulaze i sva moguća stanja. Skup izlaznih podatak obuhvata enkriptovane ili dekriptovane izlaze i sljedeće stanje.

Za implementaciju sekvencijalne mašine može se upotrijebiti rekurzivna neuralna mreža koja sadrži tri sloja neurona: ulazni sloj, skriveni sloj i izlazni sloj, [69]. Veličina ulaznog sloja mreže zavisi od broja ulaznih bitova i broja izlaznih bitova neophodnih da se opišu sva stanja. Kao aktivaciona funkcija može se upotrijebiti sigmoid. Treniranje mreže se sprovodi prema backpropagation algoritmu, [69]. Za treniranje neuralne mreže može se upotrijebiti bilo koja vrsta sekvencijalne mašine u zavisnosti od složenosti i dobijenog stepena sigurnosti. Za realizaciju sekvencijalne mašine koristi se serijski kumulativni sabirač i sekvencijalni dekoder, [74], [75], [76], [77]. Učenje mreže po delta pravilu realizuje se kroz dvije faze:

U prvoj fazi se na ulaz mreže dovodi veličina x i provlači kroz mrežu da bi se dobile izlazne vrijednosti y_p iz svake od izlaznih jedinica, [69]. Izlaz se upoređuje sa željenim izlazom što rezultira dobijanjem signala greške δ_p za svaku od izlaznih jedinica.

Druga faza uključuje širenje greške unazad kroz sve slojeve mreže dok se ne dobije odgovarajuća korekcija težinskih koeficijenata.

7. Zaključak

U tezi je predstavljena primjena informacionog sistema, kao jedne od informacionih tehnologija, na proces upravljanja rizicima po bezbjednost informacija u realnom poslovnom sistemu. Teza je izložena u dva dijela – teorijski dio teze i dio teze koji se odnosi na razvoj aplikativnog rješenja.

Teorijski dio teze je organizovan u dvije glave (Glava 2, 3). Glava 2 je posvećena informaciji, informacionim tehnologijama, sistemima i informacionom društvu. U njenom prvom poglavlju je dato objašnjenje pojma informacije, pregled različitih definicija informacije i poređenje pojmova podatak i informacija. U naredna tri poglavlja glave 2 su razmatrani istorija nastanka, definicija i principi informacionog društva i informacionih tehnologija, veza informacionog društva i informacionih tehnologija, sa posebnim osvrtom na informacione sisteme. Glava 3 se bavi pojmom bezbjednosti informacija, dajući njegovu definiciju i detaljnu analizu implementacionih ciljeva, pregled oblasti zastupljenosti bezbjednosti informacija, kao i pregled standarda za upravljanje bezbjednošću informacija, uz poseban osvrt na Opštu uredbu o zaštiti podataka.

Dio teze koji se odnosi na razvoj aplikativnog rješenja je organizovan u tri glave (Glava 4, 5, 6). Glava 4 detaljno prikazuje projektovanje informacionog sistema za upravljanje rizicima po bezbjednost informacija u Centralnoj banci Crne Gore, stavljajući akcenat na modeliranje procesa i kreiranje baze podataka za aplikativno rješenje. Uz to, u istoj glavi je objašnjena uloga Centralne banke, njen način čuvanja bezbjednosti informacija kroz utvrđenu regulativu za upravljanje rizikom po bezbjednost informacija, pregled stanja prije razvoja aplikativnog rješenja sa analizom problema koji su tada postojali. Glava 5 je posvećena detaljnom prikazu funkcionalnosti razvijenog aplikativnog rješenja. Glava 6 obuhvata analizu razvijenog aplikativnog rješenja u smislu perspektive budućeg razvoja, kao i osvrt na neuralne mreže u smislu njihove značajne upotrebljivosti u procesu upravljanja rizikom po bezbjednost informacija.

Istraživanje i rad na tezi rezultirali su ostvarivanjem konkretnih doprinosa:

- Kreiran je model informacionog sistema za realizaciju procesa upravljanja rizicima po bezbjednost informacija koji omogućava standardizaciju i automatizaciju vrednovanja informacijskih resursa, procjene i klasifikacije rizika i izrade plana tretmana rizika po bezbjednost informacija, kroz sistematizaciju i katalogizaciju samih informacijskih resursa, kategorija resursa i potencijalnih prijetnji i ranjivosti koje se mogu javiti za određenu kategoriju resursa u realnom poslovnom sistemu.

- Predloženi model ima opšti značaj – primjenjiv je na bilo koju regulativu upravljanja rizicima. Model je koncipiran tako da se njegov centralni dio koji sadrži podatke o rizicima za popisane informacijske resurse oslanja na šifarnike u kojima se nalaze podaci vezani za regulativu upravljanja rizicima i šifarnike sa popisom identifikovanih resursa, kategorija resursa i za njih definisanih prijetnji i ranjivosti. Ovakav način modeliranja registra rizika, kao jednog dokumenta koji se oslanja na niz šifarnika, daje opštost modelu.

- Dokazano je da se može sprovesti praktična implementacija predloženog modela tako što je na osnovu njega napravljen realni informacioni sistem za upravljanje rizikom po bezbjednost informacija. Naime, na osnovu modela podataka napravljene su tabele u bazi podataka, a na osnovu modela procesa izrađene su aplikacije koje su sačinile aplikativni podsistem Registar rizika po bezbjednost informacija. Predloženi model je primijenjen na realni poslovni sistem – Centralnu banku Crne Gore. Rezultat je kreiranje informacionog sistema za upravljanje rizikom po bezbjednost informacija koji je omogućio svim samostalnim organizacionim jedinicama Centralne banke Crne Gore da kreiraju, u skladu sa jedinstvenom metodologijom i koristeći podatke iz jedinstvenih šifarnika, svoje registre i planove tretmana rizika po bezbjednost informacija, kao i da ih čuvaju i da iz njih dobijaju sve potrebne izvještaje. Na taj način je postignuto efikasno upravljanje rizicima po bezbjednost informacija za Centralnu banku kao cjelinu.

- Predloženi model ima visok nivo integrabilnosti. S obzirom da u Centralnoj banci Crne Gore postoji Glavni bankarski sistem, koji pokriva veliki broj poslovnih procesa, nakon izgradnje informacionog sistema za upravljanje rizicima, sprovedena je njegova integracija sa postojećim aplikativnim sistemom. Najznačajniji aspekt integracije jeste upotreba postojećih šifarnika Glavnog bankarskog sistema kao “izvora” identifikovanih informacijskih resursa.

Literatura

[1] L. Applegate, R. Austin, W. McFarlan, "Corporate Information Strategy and Managament", MCGraw- Hill, Boston, 2007.

[2] I. Luković, A. Popović, J. Mostić, S. Ristić, "A Tool for Modeling Form Type Check Constraints and Complex Functionalities of Business Applications", Computer Science and Information Sistems, Volume 7, No 2, pp. 359-385, 2010.

[3] J. Poliščuk, „Baze podataka", Informatička literatura JEP, Podgorica, 2003.

[4] G. Panayotova, G. P. Dimitrov, P. Petrov, B. Os, "Modeling and data processing of information systems", Third International Conference on Artificial Intelligence and Pattern Recognition (AIPR), 2016.

[5] M. Pavlić, „Oblikovanje baza podataka", Odjel za informatiku Sveučilišta u Rijeci, Rijeka, 2011.

[6] R. Freeman, "Oracle Database 11g New Features", Mc Graw Hill, 2007.

[7] M. West, "Developing High Quality Data Models", Morgan Kaufmann Publ.Inc, 2011.

[8] R. Barker: CASE*Method: Entity Relationship Modelling. Addison-Wesley, 1990.

[9] T. J. Teorey, "Database Modeling and Design: The Entity-Relationship Approach", Morgan Kauffman Publ.Inc, 1990.

[10] J. Price, "Oracle Database 11g SQL", Mc Graw Hill, 2007.

[11] F. D. Rolland, "Relational Database Management with ORACLE", Addison Wesley Publ.Inc.,1989.

[12] W. W. Armstrong, "Dependency structures of data base relationships", Information Processing, 74, North-Holland Publ. Co., Amsterdam, 1974.

[13] O. Juwita, F. N. Arifin, "Design of information system development strategy based on the conditions of the organization", 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Conference Proceedings, Kuta Bali, 2017.

[14] J. Poliščuk, „Software četvrte generacije ORACLE", NIP „Tehnička knjiga", Beograd, 1991.

[15] J. Poliščuk, „Projektovanje informacionih sistema", Informatička literatura JEP, Podgorica, 2007.

[16] D. Pintar, „Model uslužno orijentirane arhitekture za stvarnovremensko skladištenje podataka zasnovan na metapodacima", Doktorska disertacija, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, 2009.

[17] D. Lečić, „Izrada modela informacionog sistema za upravljanje ljudskim resursima u poslovnim sistemima", Doktorska disertacija, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, 2016.

[18] H. Lajšić, „Razvoj modela upravljanja ljudskim resursima uz podršku informacionih tehnologija", Doktorska disertacija, Univerzitet u Novom Sadu, 2016.

[19] R. J. Paul, "What an Information System is, and why is it important to know this", 31st International Conference on Information Technology Interfaces, Conference Proceedings, Dubrovnik, 2009.

[20] M. Tepšić, R. Tanjga, „Zaštita informacionih sistema", Banja Luka College, Besjeda, 2011.

[21] N. Hađina, „Zaštita i sigurnost informacijskih sustava", Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, 2009.

[22] R. Raković, „Sistem bezbjednosti informacija – iskustva i preporuke", Infotech, Aranđelovac, 2013.

[23] W. Abbass, A. Baina, M. Bellafkih, "Survey of information security risk assessment", 2016 International Conference on Information Technology for Organizations Development (IT4OD), Fez, 2016.

[24] J. Cheng, Y. Goto, S. Morimoto, D. Horie, "A Security Engineering Environment Based on ISO/IEC Standards: Providing Standard, Formal, and Consistent Supports for Design, Development, Operation, and Maintenance of Secure Information Systems", 2008 International Conference on Information Security and Assurance (isa 2008), Busan, South Korea, 24 - 26 April, 2008.

[25] S. Faris, S. El Hasnoui, H. Medromi, H. Igguer, A. Sayouti, "Toward an Effective Information Security Risk Management of Universities' Information Systems Using Multi Agent Systems, Itil, Iso 27002, Iso 27005", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 6, pp 114-118, 2014.

[26] "Information security management systems - Overview and vocabulary", ISO Week 2018: The 41st ISO Annual General Assembly, pp. 19, Geneva, 2018.

[27] Skupština Republike Crne Gore, „Zakon o Centralnoj banci Crne Gore", "Službeni list CG", br. 40/10, 46/10 i 6/13, 2010.

[28] Centralna banka Crne Gore, „Metodologija za upravljanje rizicima po bezbjednost informacija Centralne banke Crne Gore", 2018.

[29] Centralna banka Crne Gore, „Politika bezbjednosti informacija Centralne banke Crne Gore", 2018.

[30] A. Ivanović, M. Daković, „Primjer integracije aplikativnih modula iz različitih aplikativnih podsistema u Centralnoj banci Crne Gore", IT, Žabljak, 19. - 24. februar, 2018.

[31] N. Wiener, "The Human Use Of Human Beings: Cybernetics And Society, Doubleday Anchor 1954.

[32] G. Klaus, "Cybernetisc as Viewed by Philosophy" (Kybernetik in Philosophischer Sicht), Dietz Verlga, Berlin, 1965.

[33] C. E. Shannon, W. Weaver, "The Mathematical Theory of Communication", University of Illinois Press, 1949.

[34] B. Rodić, G. Đorđević, „Da li ste sigurni da ste bezbedni", Produktivnost, Beograd, 2004.

[35] J. Feather, "The Information Society, Sixth Edition: A Study of Continuity and Change", Facet Publishing, UK, 2013.

[36] C. Sarrocco, "Elements and Principles of the Information Society", background document, World Summit on the Information Society (WSIS), Geneva 2003 – Tunis 2005.

[37] WSIS document, "Declaration of Principles - Building the Information Society: a global challenge in the new Millennium" World Summit on the Information Society (WSIS), Geneva 2003 – Tunis 2005.

[38] M. Castells, "Communication power", Oxford University Press Inc., New York, 2009.

[39] F. Webster, "Theories of the Information Society", Routledge, London, 2014.

[40] G. Gay, R. Blades, "Oxford Information Technology for CSEC: Third edition", OUP Oxford, Oxford, 2019.

[41] D. Landoll, "The Security Risk Assessment Handbook", CRC Press, Boca Raton, 2012

[42] J. D. Wareham, "Information assets in interorganizational governance: exploring the property rights perspective", IEEE Transactions on Engineering Management, Volume 50, Issue 3, pp 337 - 351. Aug. 2003.

[43] A. O. Kalashnikov, I. K. Michkalevich, "About the unified system of classification of protection of automated control systems and infocommunication systems by the criteria of importance and of information security", Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 2018.

[44] E. Humphreys, "Implementing the ISO/IEC 27001 ISMS Standard", Artech House, USA, 2016.

[45] X. Shu, J. Zhang, D. Yao, W. Feng, „Fast Detection of Transformed Data Leaks", IEEE Transactions on Information Forensics and Security, pp 528–542, 2015.

[46] K. Padayachee, E. Worku, "Shared situational awareness in information security incident management", 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, 2017.

[47] O. A. Randle, M. Y. Solange, "Critical factors influencing employees compliance with information security policies of an organization: Systematic review and Meta-analysis", International Conference on Information Society (i-Society), Dublin, 2017.

[48] N. S. Safa, C. Maple, T. Watson, "Information security collaboration formation in organisations", IET Information Security, pp 238–245, 2018.

[49] A. Caro, V. Lovino, A. O'Neal, "Receiver- and sender-deniable functional encryption", IET Information Security, pp 207–216, 2018.

[50] M. Abdala, A. Caro, D. H. Phan, "Generalized Key Delegation for Wildcarded Identity-Based and Inner-Product Encryption", IEEE Transactions on Information Forensics and Security, pp 1695–1706, 2012.

[51] M. Lundgren, "Making information security research great again: Assumptions and practical aspects of case-study research in information security", 2nd International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS), Cavan, 2018.
[52] A. Calder, S. Watkins, "IT Governance - A Manager's guide to Data Security and ISO 27001/ISO 27002", 4th Edition, Kogan Page, London and Philadelphia, 2008.
[53] R. Wang, "Research on information security strategy and risk management for smart grid", CICED, 2014.
[54] H. Liu, L. Yu, "Toward integrating feature selection algorithms for classification and clustering", IEEE Trans. on Knowledge and Data Engineering, pp 491-502, 2005.
[55] T. Tzolov, "One Model For Implementation GDPR Based On ISO Standards", International Conference on Information Technologies (InfoTech), Bulgaria, September 2018.
[56] V. Ayala – Rivera, L. Pasquale, "The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements", IEEE 26th International Requirements Engineering Conference (RE), Canada, August 2018.
[57] A. Ivanović, „Značaj aplikativnog rješenja u sistematizaciji podataka o potencijalnim rizicima po bezbjednost informacija", na recenziji, IT, Žabljak, 18. - 22. februar, 2020.
[58] M. Daković, T. Ružić, T. Rogač, M. Brajović, and B. Lutovac, "Neural Networks Application to Neretva Basin Hydro-meteorological Data," 13th Symposium on Neural Networks and Applications NEUREL 2016, Belgrade, Serbia, November 2016.
[59] K. L. Priddy, P. E. Keller, "A Artificial Neural Networks: An Introduction", Bellingham, Wash.: SPIE Press, 2005.
[60] A. A. Ali, R. Tervo, "Traffic identification using artificial neural network", Canadian Conference on Electrical and Computer Engineering, Conference Proceedings (Cat. No.01TH8555), Toronto, Ontario, 2001.
[61] J. Shun, H. A. Malki, "Network Intrusion Detection System Using Neural Networks", 2008 Fourth International Conference on Natural Computation, Jinan, China, 18-20 Oct. 2008, Vol. 5, pp 242-246
[62] B. Subba, S. Biswas, S. Karmakar, "A Neural Network based system for Intrusion Detection and attack classification", Twenty Second National Conference on Communication (NCC), Guwahati, 2016.
[63] Lj. Stanković, "Digital signal processing", CreateSpace Independent Publishing Platform, USA, 2015.
[64] LJ. Stanković, M. Daković, "Adaptive Systems," Chapter in the Book: Digital Signal Processing, Lj. Stankovic, CreateSpace, Amazon, pp. 423-520, 2015.
[65] X. Gao, L – Z. Liao, "A New One-Layer Neural Network for Linear and Quadratic Programming", IEEE Transactions on Neural Networks, Vol. 21, No. 6, June 2010.
[66] B. Yang, W. Li, "An Evaluation System for Cognitive Impairment based on Brain Functional Network Links", IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), China, March 2019.
[67] V. N. Ivanović, N. R. Brnović: "Superior execution time design of a space/spatial-frequency optimal filter for highly nonstationary 2D FM signal estimation," IEEE Trans. on Circuits and Systems I: Regular Papers, vol. 65, issue 10, Oct. 2018, pp. 3376–3389.
[68] V. N. Ivanović, S. Jovanovski, N. Radović: "Superior execution time design of optimal (Wiener) time-frequency filter," Electronics Letters, vol.52, no.17, Aug.2016, pp.1440–1442.
[69] N. Agarwal, P. Agarwal, "Use of Artificial Neural Network in the Field of Security", MIT International Journal of Computer Science & Information Technology, Vol. 3, No. 1, Jan. 2013, pp. 42–44
[70] L. Bao, "Parallel algorithms based on neural network ensemble for risk assessment", Journal of Anhui University of Technology and Science (Natural Science), pp 38-41, 2009, Issue 04
[71] Y. He, L. Wang, "Chaotic neural networks and their applications", Proceedings of the 3rd World Congress on Intelligent Control and Automation (Cat. No.00EX393), 26 June-2 July 2000, Hefei, China
[72] A. Ruhan Bevi, S. Tumu, N. Varsha Prasad, "Design and investigation of a chaotic neural network architecture for cryptographic applications", Computers & Electrical Engineering, Volume 72, November 2018, Pages 179-190.
[73] I. Dalkiran, K. Danisman, "Artificial neural network based chaotic generator for cryptology", Turkish Journal of Electrical Engineering and Computer Sciences, Vol.18, No.2, March 2010, Tubitak

[74] S. Jovanovski, V. N. Ivanović: "Signal adaptive pipelined hardware design of time-varying optimal filter for highly nonstationary FM signal estimation," Journal of Signal Processing Systems, Volume 62, Issue 3 (2011), pp.287–300.

[75] V. N. Ivanović, R. Stojanović, LJ. Stanković: "Multiple clock cycle architecture for the VLSI design of a system for time-frequency analysis", EURASIP Journal on Applied Signal Processing, Special Issue on Design Methods for DSP Systems, vol.2006, pp.1-18.

[76] N. R. Brnović, I. Djurović, V. N. Ivanović, M. Simeunović: "Hardware Implementation of the Quasi Maximum Likelihood Estimator Core for Polynomial Phase Signals," IET Circuits, Devices & Systems, vol. 13, no. 2, March 2019, pp. 131-138

[77] V. N. Ivanović, N. Radović: "Signal Adaptive Hardware Implementation of a System for Highly Nonstationary Two-Dimensional FM Signal Estimation," AEUE – International Journal of Electronics and Communications, vol. 69 (2015), Issue 12, Dec. 2015, pp.1854–1867.

Bibliografija

Radovi na međunarodnim naučnim konferencijama:

[1] A. Ivanović, M. Daković, „Primjer integracije aplikativnih modula iz različitih aplikativnih podsistema u Centralnoj banci Crne Gore“, IT, Žabljak, 19. - 24. februar, 2018.

[2] A. Ivanović, „Značaj aplikativnog rješenja u sistematizaciji podataka o potencijalnim rizicima po bezbjednost informacija“, na recenziji, IT, Žabljak, 18. - 22. februar, 2020.

Ime i prezime autora: Ana Ivanović, dipl.ing.el.

E T I Č K A I Z J A V A

U skladu sa članom 22 Zakona o akademskom integritetu i članom 24 Pravila studiranja na postdiplomskim studijama, pod krivičnom i materijalnom odgovornošću, izjavljujem da je master rad pod naslovom

"Informacione tehnologije u službi identifikacije, procjene i kontrole rizika po bezbjednost informacija sa primjerom implementacije"

moje originalno djelo.

Podnosilac izjave,

Ana Ivanović, dipl.ing.el.

Ana Ivanović

U Podgorici, dana 22. 01. 2020. godine