MODEL PROCJENE VJEROJATNOSTI NEŽELJENIH DOGAĐAJA U INFORMACIJSKOM SUSTAVU UPOTREBOM BAYESOVOG TEOREMA

Očevčić, Hrvoje

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
ELEKTROTEHNIČKI FAKULTET

MODEL PROCJENE VJEROJATNOSTI NEŽELJENIH DOGAĐAJA U INFORMACIJSKOM SUSTAVU UPOTREBOM BAYESOVOG TEOREMA

DOKTORSKA DISERTACIJA

Hrvoje Očevčić

Osijek, 2015.

Doktorska disertacija izrađena je na:	**Elektrotehnički fakultet Osijek** **Sveučilište J. J. Strossmayera u Osijeku**
Mentor:	**Doc. dr. sc. Krešimir Nenadić**
Doktorska disertacija ima:	**125 stranica**

Rad broj: **50**

Povjerenstvo za ocjenu doktorske disertacije:

1. Dr.sc. Drago Žagar, redoviti profesor, predsjednik, Elektrotehnički fakultet Osijek
2. Dr.sc. Krešimir Nenadić, docent, mentor, Elektrotehnički fakultet Osijek
3. Dr.sc. Marin Golub, izvanredni profesor, član, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu

Povjerenstvo za obranu doktorske disertacije:

1. Dr.sc. Drago Žagar, redoviti profesor, predsjednik, Elektrotehnički fakultet Osijek
2. Dr.sc. Krešimir Nenadić, docent, mentor, Elektrotehnički fakultet Osijek
3. Dr.sc. Marin Golub, izvanredni profesor, član, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu
4. Dr.sc. Snježana Rimac-Drlje, redovita profesorica, član, Elektrotehnički fakultet Osijek
5. Dr.sc. Krešimir Grgić, docent, član, Elektrotehnički fakultet Osijek

Datum obrane doktorske disertacije: 30. lipnja 2015.

SADRŽAJ

ZAHVALA

Želim se zahvaliti svojim roditeljima Ljubici i Martinu na poticaju.

Posebno želim zahvaliti supruzi Tihani na velikoj podršci, a djeci Ivi i Bruni na tome što su uglavnom imali razumijevanja na moju povremenu odsutnost.

Hvala mentoru i ostatku „tehničke podrške“…

POPIS SLIKA

POPIS TABLICA

POPIS KRATICA

ISMS	Information Security Management System
ICT	Information and Communication Technology
IS	Information System
Cobit	Control Objective for IT
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SPAM	Neželjena elektronička pošta
Anti-SPAM	Izraz, kratica koji se koristi za sustave i alate za sprječavanje posljedica neželjene pošte
HAM	Izraz korišten za valjanu poruku elektroničke pošte
ROC	Receiver Operating Characteristic
AUC	Area under an ROC Curve
TPR	True Positive rate
FPR	False Positive rate
EM	Estimation Maximization
NIDS	Network Intrusion Detection System
DIDS	Distributed Intrusion Detection System
HIDS	Host Intrusion Detection System
ISS	Indeks Security Systems
VPN	Virtual Private Network
IDPS	Intrusion Detection and Prevention Systems
IP	Internet Protocol
ADSL	Asymmetric Digital Subscriber Line
HAZOP	Hazard Operability Analysis
FMEA	Failure Mode and Effect Analysis

POPIS POJMOVA

Dependability	Oslonjivost - označava metode i tehnike koje omogućavaju razvoj oslonjivih sustava kao što su prevencija pogrešaka, tolerancija pogrešaka, uklanjanje i predviđanje pogrešaka [76].
Reliability	Pouzdanost - Osobine oslonjivosti su one koje se očekuju od sustava. Tri su primarne osobine oslonjivosti: pouzdanost, dostupnost i sigurnost [76].
Availability	pripravnost informacijskog sustava za korištenje usluga
Safety	nepojavljivanje katastrofalnih posljedica zatajenja informacijskog sustava za svoju okolinu
Confidentiality	nepojavljivanje neautoriziranih otkrivanja podataka/informacija u informacijskom sustavu
Integrity	nepojavljivanje nevaljanog ažuriranja podataka/ informacija u informacijskom sustavu
Maintainability	Lakoća podvrgavanja popravcima i održavanju informacijskog sustava
Impact	Utjecaj, razina efekata koji nastaju kao uzrok nekog događaja
Mitigacija	Smanjenje, umanjenje rizika
System failure	Zatajenje informacijskog sustava
System restore	Obnavljanje sustava
Fault	Kvar, posljedice greške
Decision support system	Sustav za potporu odlučivanju
Expert Systems	Ekspertni sustavi
Knowledge acquisition	Sakupljanje znanja
Knowledge representation	Predstavljanje znanja
Artificial Inteligence	Umjetna inteligencija
Machine learning	Strojno učenje
Pattern recognition	Prepoznavanje oblika
Overfitting	preugođenost

Underfitting	neugođenost
Hipoteza	Predloženo objašnjenje fenomena ili razumna pretpostavka koje predlaže moguću korelaciju između više fenomena. Termin se izvodi iz grčkog jezika, hypotithenai znači staviti ispod ili pretpostaviti
Firewall	Vatroštit
Risk Assessment	Procjena rizika, niz postupaka s ciljem smanjenja i kontrole vjerojatnosti rizičnih događaja
What-if-Analysis	„što-ako“ analiza
Fault Tree and Event Tree Analysis	Analiza stabla kvara i stabla događaja
Risk Evaluation	Ocjena rizika
Risk Estimation	Određivanje rizika
Threat	Prijetnja
Vulnerability	Ranjivost
Anti-Fraud	Djelovanje s ciljem sprječavanja prijevara

1. UVOD

§

Na početku knjige „Vjerojatnost i slučaj“ (njem. „*Wahrscheinlichkeit und Zufall*“) autor Max Woitschach (Munchen, 1973) piše:

> *„Dragi čitaoče, da li bi smatrali korisnim kada bi odmah na početku neke knjige mogli ustanoviti da li se isplati čitati tu knjigu? Zato ću započeti pričom:*
> *Zamislite kako neki čovjek 60 puta zaredom baci kocku i pri tome izbroji koliko je puta dobio svaki od šest brojeva. Nakon bacanja, on upita:*
>
> > *1. Šest brojeva se nisu pojavili svaki jednako puta usprkos tome što su svi brojevi imali jednaku vjerojatnost pojavljivanja.*
> > *2. Šest brojeva se nisu pojavili svaki jednako puta zato što su svi brojevi imali jednaku vjerojatnost pojavljivanja.“*

Na sljedećoj stranici Woitschach pita:

> *1. Ako mislite da se svi brojevi nisu jednako puta pojavili usprkos tome što su svi imali jednaku vjerojatnost – vi obavezno trebate čitati ovu knjigu dalje, jer ćete naučiti da je praktički nemoguće dobiti svaki broj pojavi jednako puta kod većeg broja bacanja. Potpuno jednaka vjerojatnost je ono što uzrokuje nejednaku raspodjelu brojeva.*
> *2. Ako smatrate da se svi brojevi nisu jednako puta pojavili zato što su svi imali jednaku vjerojatnost, tada vi očito pripadate malom broju onih kojima su osnove teorije vjerojatnosti poznaju i pitanje je hoće li iduće stranice išta novo pridonijeti vašem znanju.*

Upravo to Woitschach pita na početku svoje knjige, a slično pitanje mogao bih postaviti i ja vama:

Kako ste odgovorili na Woitschachovo pitanje?

Ovime želim naglasiti da se model procjene vjerojatnosti neželjenih događaja u informacijskom sustavu temelji na jednostavnim izračunima vjerojatnosti i da su upravo jednostavna primjena i korištenje ciljevi ovoga rada.

§

1.1. Uvodno razmatranje

Upravljanje informacijskim sustavima podrazumijeva provođenje različitih aktivnosti s ciljem optimizacije rada svih dijelova sustava. Informacijski sustavi služe za upravljanje informacijskom imovinom. Informacijska imovina je skup imovine (resursa) koji sadrži određeno znanje koncipirano u strukturiranim podacima odnosno informacijama. Moderni informacijski sustavi pod pojmom informacijska imovina često podrazumijevaju različite kategorije imovine pa čak često i sklopovlje, okruženje i osoblje. Odabirom opsega koji je sadržan u pojmu, izražava se politika informacijske sigurnosti i strategija poslovanja.

Informacija je podatak s određenim značenjem, odnosno saznanje koje se može prenijeti u bilo kojem obliku, pisanom, audio, vizualnom, elektroničkom ili nekom drugom. Kako bi se informacije što lakše i jednostavnije obrađivale potrebno ih je na odgovarajući način klasificirati, odrediti im svrhu, vrijednost, dostupnost i ostale atribute. U takvom okruženju, razvojem računala, sustavi za upravljanjem informacijama postaju stvarnost i obveza organizacija kojima je informacija srž djelovanja. Takve organizacije su među prvima uvele i pojam informacijske sigurnosti. Taj pojam se ne odnosi isključivo na tehničke mjere zaštite (korisnička imena, zaporke, enkripciju, prava pristupa i slično), već podrazumijeva i administrativne mjere (sigurnosna politika, pravilnici, procedure) i fizičke mjere (video nadzor, zaštita prostorija, fizička kontrola pristupa). Kako bi informacijski sustav bio zaštićen na pravi način, potrebno je uspješno uskladiti, implementirati i nadzirati sve postojeće mjere zaštite.

Rizici se procjenjuju s aspekta učinka koji bi mogao biti uzrokovan narušavanjem funkcionalnosti i sigurnosti informacijskog sustava, odnosno narušavanjem temeljnih načela informacijskog sustava. Upravljanje rizikom informacijskog sustava obuhvaća postupke procjene rizika te poduzimanja radnji za smanjenje rizika na prihvatljivu razinu i održavanje prihvatljive razine rizika. Tvrtke danas moraju obavljati mjerenje, procjenu i upravljanje svim rizicima kojima su u svom poslovanju izložene. Rizici kojima su tvrtke izložene u svom poslovanju i za koje minimalno moraju biti propisani postupci mjerenja, procjene i upravljanja uključuju i rizik koji proizlazi iz neadekvatnog upravljanja informacijskim i pridruženim tehnologijama. Procjena rizika je identifikacija i određivanje vrijednosti resursa zasnovanih na poslovnim potrebama organizacije. Prikladna zaštita nužno zahtjeva procjenu vrijednost imovine ovisno o njihovoj važnosti za poslovni proces. Potrebno je razmotriti zakonske i poslovne zahtjeve, posljedice (engl. *impact*), gubitka povjerljivosti, raspoloživosti i integriteta. U radu su opisane osnove upravljanja rizicima informacijskog sustava, kao i metodologija i načini provođenja svih podrazumijevanih aktivnosti.

Upravljati rizicima općenito, znači baviti se pojmom vjerojatnosti. Svaki događaj koji se osjeti i koji za posljedicu ima određeni učinak nosi određenu vjerojatnost. Te su vjerojatnosti podaci koji se najčešće izračunavaju naknadno i koji služe za retroaktivnu analizu u procesima upravljanja rizicima.

Ovaj rad će predstaviti jednu metodu u kojoj je moguće koristiti podatke koji se već nalaze u različitim dijelovima informacijskih sustava i čuvaju u spremnicima, komunikaciju koja već postoji između perifernih dijelova sustava i uređaja za zaštitu koji generiraju informacije i koriste komunikacijske tehnike.

U radu je korišten Bayesov teorem i model se temelji na uporabi teorije izračuna uvjetne vjerojatnosti. Razrađeno je korištenje Bayesovog teorema u različitim scenarijima i okruženjima. Pomoću modela predloženog u radu se izračunavaju i procjenjuju vjerojatnosti neželjenih događaja u informacijskom sustavu na temelju informacija o prethodnim događajima. Parametri događaja se prate i s vremenom povećavaju bazu znanja koja svojim rastom matematički povećava točnost predložene odluke.

Opseg rada modela je ispitan u različitim informacijskim sustavima i cilj je prikazati načine uporabe u različitim okruženjima, ali naslovom je model ograničen na informacijske sustave koji su prema definiciji svi sustavi unutar kojih se obrađuju podaci i prenose informacije.

Eksperimenti u radu su provedeni korištenjem stvarnih sustava za filtriranje neželjene pošte i upada, ali i simulacijama izrađenim na testnim okruženjima. Simulacije su detaljno opisane i cilj im je nadomjestiti stvarni sustav i prikazati rad u što realnijem okruženju.

Evaluacija je provedena usporedbom dobivenih rezultata s rezultatima stvarnih sustava koji su predloženi kao referenca sukladnosti. Evaluacija rezultata eksperimenta s korištenjem rizika u informacijskom sustavu je provedena usporedbom s mišljenjem eksperata iz područja upravljanja sustavima informacijske i komunikacijske tehnologije.

Primjena predloženog modela je široka. Predviđa se mogućnost uporabe modela u poslovnim i informacijskim sustavima, odnosno u svim sustavima u kojima je informacija temeljni parametar za potporu odlučivanju. Objektivnost i matematička podloga jamči točnost rezultata, a prilagodljivost različitim okruženjima ukazuje na neke od koristi koje donosi predloženi model.

1.2. Ciljevi rada

Dugogodišnji rad na upravljanju informacijskom sigurnošću i reviziji informacijskih sustava generirao je neke ideje od kojih se najvažnije nalaze u nastavku i predstavljaju ciljeve ovoga rada.

- Izraditi model za predviđanje neželjenog događaja u informacijskom sustavu zasnovanog na Bayesovom teoremu i korištenju agenata u raspodijeljenom okruženju.

Prijedlog modela kojim je moguće izračunavati vjerojatnosti neželjenih događaja u stvarnom vremenu temeljenog na Bayesovom teoremu i agentskoj komunikaciji.

- Predložiti algoritam agenta u raspodijeljenom okruženju.

Izrada algoritma koji opisuje rad agenata u raspodijeljenom okruženju. Opis načina komunikacije i pravila za implementaciju modela u okruženje.

- Ispitati predloženi model i usporediti ga s postojećim rješenjima

Odabir primjera iz prakse na temelju kojih rezultati rada najbolje prikazuju mogućnosti modela. Ispitivanje modela na primjerima iz prakse i evaluacija rezultata s ciljem dokazivanja valjanosti.
Rad na brojnim projektima unutar područja upravljanja informacijskom sigurnošću potaknuo je mnoga razmišljanja, a posebno se mogu istaknuti kontinuitet poslovanja, klasifikacija informacija i implementacija sustava upravljanja informacijskom sigurnošću (ISMS).

1.3. Korištene metode i mjerenja

U radu su prikazani teorijski dijelovi koji predstavljaju temelj predložene metode. Eksperimenti provedeni u drugom dijelu rada su provedeni s ciljem dokazivanja ispravnosti teza donesenih uporabom modela. Model preporuča odluku i izračunava vjerojatnost ostvarenja neželjenih događaja, odnosno vjerojatnost ostvarenja događaja općenito, a neželjeni događaj predstavlja scenarij čiji efekti mogu prouzročiti neželjene posljedice na poslovanje. Izračun ispravnosti i statističke analize su provedene korištenjem konfuzijskih matrica.
Evaluacija je provedena usporedbom rezultata s referentnim vrijednostima. Referentne vrijednosti korištene za usporedbu su dobivene ispitivanjem jednakih scenarija, ali korištenjem alata za specifičnu namjenu. Eksperiment otkivanja neželjene pošte je uspoređen s rezultatima *Google mail* sustava za istu namjenu. Otkrivanje napada je uspoređeno s rezultatima alata *Snort*, a otkrivanje

neželjenih događaja na temelju rizika u informacijskom sustavu je uspoređeno s rezultatima procjene rizika i mišljenjem eksperata iz područja informacijske i komunikacijske tehnologije.

1.4. Uvodni eksperiment

Kao uvodni eksperiment, u nastavku je opisana metodologija upravljanja rizicima informacijskog i komunikacijskog sustava (ICT) u kojemu se rizicima upravlja korištenjem preporuka porodica standarda ISO27000, ISO31000 [1] i smjernica Cobit (*Control Objective for IT*) [2].
Višegodišnjim korištenjem metodologije upravljanja rizika identificirane su mnoge ranjivosti i prijetnje koje konsolidirane tvore rizike čija je vjerojatnost predmetom daljnje analize. Usporedbom vjerojatnosti ostvarenja rizika i stvarnih događaja u istom informacijskom sustavu utvrđena je veza između vrijednosti rizika i stvarnih događaja na koje su te vjerojatnosti potencijalno ukazivale. Neke od većih vjerojatnosti ostvarenja rizika nisu smanjivane (mitigacija rizika) [3] već je sukladno metodologiji, moguće donijeti odluku o prihvaćanju nepravilnosti. Ideja je bila načiniti model koji bi mogao izračunati vjerojatnost ostvarenja neželjenog scenarija opisanog rizikom na nekoj informacijskoj imovini. Sudjelovanje u projektima kontinuiteta poslovanja [3] ideja je razrađena u skladu s intenzivnijim korištenjem upravljanja rizicima i zaštitom informacijskih sustava. Razradom ideje koja je dovela do korištenja Bayesovog teorema, zaključena je mogućnost uporabe modela u širem spektru upravljanja informacijskim i komunikacijskim sustavima. Načelo koje je potrebno uvrstiti u model je objektivnost i na temelju kojeg je izgrađen model preporučen i ispitan u ovome radu.
U nastavku rada su prikazane teorijski temelji na kojima se zasniva model i eksperimenti i evaluacija rezultata rada modela za procjenu vjerojatnosti neželjenih događaja u informacijskom sustavu.
U poglavlju 2 opisani su osnovni pojmovi iz teorije o informacijskim i komunikacijskim sustavima. Ovo poglavlje predstavlja uvod u sustave za potporu odlučivanju i navodi tehnike komunikacije između dijelova sustava. Navedeni su statistički podaci o prekidima u radu koji su zabilježeni u svijetu i prouzročili su poslovne gubitke. Posljedice prekida u radu informacijskih sustava trebaju biti umanjene implementacijom predloženog modela.

Poglavlje 3 sadrži teorijske osnove uvjetne vjerojatnosti i Bayesove logike. Na nekoliko primjera je prikazana primjena Bayesovog teorema za izračun vjerojatnosti neželjenih događaja. Navedeni

su i temelji raspodijeljenih sustava i načina rada agenata u njima, odnosno okruženja u kojenu je predviđen rad modela za procjenu vjerojatnosti neželjenih događaja.

Poglavlje 4 opisuje rad modela za procjenu vjerojatnosti neželjenih događaja. Način rada je predstavljen pomoću algoritma temeljenog na Bayesovom teoremu. Opisan je i način rada agenata i njihove međusobne komunikacije tijekom procjene vjerojatnosti neželjenih događaja u informacijskim sustavima.

U poglavlju 5 su prikazani rezultati testiranja modela unutar tri različita okruženja informacijskih sustava: filtriranje neželjenih poruka, otkrivanje upada i analizu rizika. Opisani su načini provođenja simulacija i eksperimenata. Simulacijama je prikazan utjecaj različitih okruženja u kojima model provodi procjenu i različitih veličina baza podataka na točnost procjene. Rezultati su evaluirani usporedbom s rezultatima referentnih modela. Kao kriteriji evaluacije u ovom istraživanju koristit će se točnost klasifikacije i brzina provođenja selekcije atributa. Svi rezultati su prikazani na jednak način i uspoređeni upotrebom statističkih pokazatelja točnosti.

Zaključak rada prikazuje rekapitulacija dobivenih rezultata i osvrt na predložene znanstvene doprinose.

2. INFORMACIJSKI SUSTAV

2.1. Informacijski i komunikacijski sustavi

Pojam sustava javlja se u području tehnoloških, organizacijskih i znanstvenih aktivnosti, kao i u neformalnoj komunikaciji, odnosno jeziku. Informacijski sustav je sastavni dio svakog ciljno orijentiranog sustava. Informacijski sustav nekog tehnološkog i/ili organizacijskog sustava je onaj dio tog sustava koji stalno opskrbljuje potrebnim informacijama sve razine upravljanja i odlučivanja u sustavu. Osnovna funkcija informacijskog sustava je stalna opskrba potrebnim informacijama i podrška odlučivanju u tehnološkom odnosno organizacijskom obliku. Ulazne i izlazne veličine informacijskog sustava su podaci odnosno informacije.

Cilj informacijskog sustava (IS) je pribaviti informacije potrebne pri izvođenju poslovnog procesa i upravljanju poslovnim sustavom. Uobičajeni su dijelovi informacijskog sustava sustav za obradu transakcija, upravljački izvještajni sustav, sustav za potporu odlučivanju i sustav uredskog poslovanja. Djelovanje informacijskog sustava upotpunjuje se primjenom informacijskih i komunikacijskih tehnologija (ICT) i s njima povezanim programima, procedurama, uputama, algoritmima i znanjem kojima se informacijske tehnologije pokreću zbog izvršenja poslovnih zadataka i ciljeva. Informacijski sustav je prema tome sprega i sustav materijalnih i nematerijalnih elemenata kojima se opisuje poslovna stvarnost, rješavaju poslovni zadaci i ispunjavaju poslovni ciljevi.

Brzim rastom informacijske i telekomunikacijske tehnologije i međudjelovanjem s procesima, izazvane su razne strukturne promjene, ali i promjene samih procesa i društva u cjelini. Dolazi do jake sinergije tehnologije i različitih ljudskih djelatnosti što uzrokuje velike opasnosti od njihovih zatajenja. Djelatnosti kao što su transport, komunikacije, energetika, bankarstvo i zdravstvo posebno su osjetljive, ali ne smiju se zanemariti niti druga područja privrede od kojih većina danas ovisi o informacijskoj i komunikacijskoj tehnologiji. Razlozi povećanja opasnosti kriju se u sve većoj ovisnosti različitih poslovnih djelatnosti na informacijske sustave koje podržavaju informacijska i telekomunikacijska tehnologija. Stoga informacijski sustavi moraju imati takva obilježja kojima će se objektivno moći ocijeniti do koje razine se u njih može imati povjerenja. Svojstvo sustava koje opisuje razinu do koje mu se može vjerovati je njegova oslonjivost (engl.

dependability) [4]. Oslonjivost informacijskog sustava može se definirati kao svojstvo koje opravdava oslanjanje na usluge koje sustav pruža. Usluge informacijskog sustava koriste korisnici i oni se prema definiciji oslanjaju na informacijski sustav [5]. Oslanjanje predstavlja vezu između informacijskog sustava i korisnika i ona direktno ovisi o korisničkim aktivnostima. Zbog toga je moguće da neki korisnici kroz svoje aktivnosti doživljavaju informacijski sustav kao potpuno oslonjiv, dok ga drugi korisnici s drugim aktivnostima doživljavaju kao manje oslonjiv ili potpuno neoslonjiv [6]. Oslonjivost informacijskog sustava moguće je analizirati iz tri perspektive: obilježja oslonjivosti, prijetnje i dostizanje oslonjivosti. Oslonjivost informacijskog sustava je svojstvo složeno iz niza obilježja čije vrijednosti grade ukupnu razinu oslonjivosti sustava. Razinama obilježja oslonjivosti prijete kvarovi, pogreške i zatajenja. Kako bi se ove prijetnje izbjegle, postoji niz različitih metoda dostizanja veće razine oslonjivosti.
Oslonjivost informacijskog sustava višedimenzionalno je svojstvo koje se sastoji od šest obilježja [5]:

1. Dostupnost (engl. *availability*) – predstavlja pripravnost informacijskog sustava za korištenje usluga,
2. Pouzdanost (engl. *reliability*) – predstavlja neprekidnost usluge informacijskog sustava;
3. Sigurnost (engl. *Safety*) – predstavlja nepojavljivanje katastrofalnih posljedica zatajenja informacijskog sustava za svoju okolinu,
4. Povjerljivost (engl. *confidentiality*) – predstavlja nepojavljivanje neautoriziranih otkrivanja podataka/informacija u informacijskom sustavu,
5. Cjelovitost (engl. *integrity*) – predstavlja nepojavljivanje nevaljanog ažuriranja podataka/ informacija u informacijskom sustavu,
6. Lakoća održavanja (engl. *maintainability*) – predstavlja lakoću podvrgavanja popravcima i održavanju informacijskog sustava.

Zaštita informacijskih sustava kao zajedničko obilježje dostupnosti, cjelovitosti i povjerljivosti predstavlja njegovu sposobnost zaštite od slučajnih ili namjernih vanjskih napada [7]. Obilježje cjelovitosti informacijskog sustava označava nemogućnost nevaljanog ažuriranja (dodavanja, brisanja ili izmjene) podataka/informacija u informacijskom sustavu [8]. Povjerljivost informacijskog sustava je njegova sposobnost da informaciju otkriva samo onim sustavima (ljudima ili drugim programskim podrškama i/ili sklopovljem) s pravom i potrebom pristupa podacima ili informacijama [6].

Informacijski sustav pruža kvalitetnu uslugu ako ta usluga sadrži stvarnu funkciju informacijskog sustava. Funkcija informacijskog sustava je sve ono za što je sustav namijenjen i ona je opisana karakteristikama sustava. Zatajenje informacijskog sustava (engl. *system failure*) događaj je koji se javlja samo onda kada se usluga informacijskog sustava razlikuje od kvalitetne usluge. Informacijski sustav može zatajiti iz više razloga: jer nije u skladu sa svojim karakteristikama ili karakteristike adekvatno ne opisuju njegovu funkciju. Zatajenje je prijelaz iz kvalitetne u nekvalitetnu uslugu. Obrnuti prijelaz, iz nekvalitetne u kvalitetnu uslugu je obnavljanje sustava (engl. *system restore*). Pogreška (engl. *error*) je stanje informacijskog sustava koje može uzrokovati kasnije zatajenje [9]. Kvar (engl. *fault*) je stvarni ili pretpostavljeni uzrok pogreške.

Kvar nužno ne rezultira pogreškom u informacijskom sustavu, jer kvar sustava može biti kratkotrajan ili prolazan i uklonjen prije pojave pogreške. Nadalje, pogreška sustava ne mora nužno dovesti do zatajenja sustava, jer pogreška može biti ispravljena prije zatajenja [7]. Kvar, pogreška i zatajenje informacijskog sustava predstavljaju prijetnje njegovoj oslonjivosti jer stvaraju ili uzrokuju nepouzdanost informacijskog sustava, odnosno gubitak jednog ili više svojstava [5].

Temeljni uzroci smanjenja kvalitete usluge informacijskog sustava su kvarovi. Stoga metode smanjenja pojave kvara u informacijskom sustavu ujedno predstavljaju i metode povećanja razine oslonjivosti informacijskog sustava i očuvanja njegovih svojstava. Postoje četiri metode smanjenja pojave kvara:

- prevencija kvara,
- neosjetljivost na kvar,
- predviđanje kvara i
- uklanjanje kvara.

Smanjenje pojave kvara njegovom prevencijom postiže se tehnikama kontrole kvalitete koje su primijenjene tijekom oblikovanja i izrade programske podrške i sklopovlja. Kod programske podrške ona uključuje strukturirano programiranje, skrivanje informacija, modularnost itd., a kod sklopovlja stroga pravila njegova oblikovanja. Fizički kvarovi u radu se sprječavaju, primjerice, oklopljenim sklopovljem, dok se kvarovi u interakciji između korisnika i informacijskog sustava sprječavaju obukom, strogim procedurama održavanja itd.

Informacijski sustavi kod kojih je implementirana neosjetljivost na kvar pokušavaju pružiti ispravnu uslugu i uz postojanje kvara. Ovo se postiže ugradnjom sustava za otkrivanje pogreški u

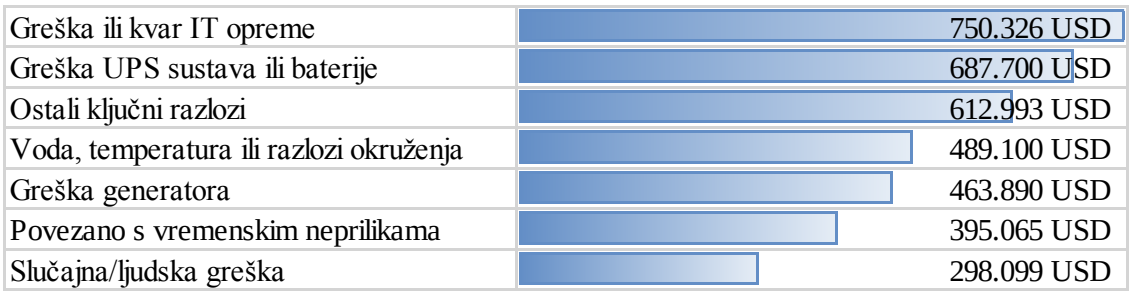
informacijskom sustavu i njegovu oporavku [8]. Jedan od korištenih pristupa u izgradnji sustava neosjetljivih na kvar je N-verzijsko programiranje kod kojega se razvija više inačica programske podrške. Zatim, informacijski sustav se podržava barem dvjema inačicama programske podrške koji istovremeno prihvaćaju korisnički zahtjev, obrađuju ga te svoje rezultate dostavljaju izlaznom komparatoru koji ih uspoređuje i određuje konačni izlaz koji će biti upućen korisniku [7]. Preteče neosjetljivosti na kvar su i metode identifikacije neželjene pošte (SPAM, u nastavku teksta će se koristiti izraz SPAM zbog razumljivosti tehničkim stručnjacima, ekspertima) i sustavi za detekciju i prevenciju upada (engl. *Intrusion Detection and/or Prevention System*). Smanjenje pojave kvara u informacijskom sustavu metodom njegova predviđanja sastoji se u procjeni ponašanja informacijskog sustava u odnosu na vjerojatnost pojave kvara ili njegova aktiviranja. Utvrđuje se postojeći broj kvarova, procjenjuje se buduća pojava kvarova i njihove moguće posljedice na informacijski sustav. Provodi se kvalitativna i kvantitativna procjena kvarova – kvarovi se identificiraju, klasificiraju itd., te se određuje vjerojatnost njihove pojave. U tu svrhu koriste se Markovljevi lanci, Petrijeve mreže, stablo kvarova. [8]. Markovljevim lancem je je moguće predstaviti niz stanja sustava i na taj način analizirati međuovisnosti i promjene vjerojatnosti u vremenu. Petrijevim mrežama i stablima kvarova se vizualno predstavljaju dinamički sustavi i međuovisnosti unutar njih.

Krajem 2010. godine provedeno je istraživanje zatajenja informacijskih sustava u SAD-u [10]. Tablica 2-1 prikazuje rang listu rezultata toga istraživanja [10].

Tablica 2-1. Rang lista zatajenja informacijskog sustava

Okolnosti uz zatajenje	**Razina**
Saniranje ili nadogradnja podatkovnih centara bez prekida	1
Neodgovarajuće napajanje	2
Neodgovarajuće hlađenje	3
Točno praćenje resursa podatkovnog centra	4
Neodgovarajući prostor	5
Ograničavanje pristupa podatkovnom centru	6

Analiza zatajenja informacijskih sustava iz 2012. godine [11] provedena na uzorcima u kojima su sudjelovale 358 poslovne organizacije pokazalo je da je 13% organizacija imalo trošak preko 500.000USD. Utvrditi učestalosti zatajenja informacijskih sustava izrazito je teško, budući da su podaci o zatajenju i kvarovima osjetljivi i često povjerljivi [12]. Slika 2-1 prikazuje uzroke zatajenja u informacijskim sustavima i troškove.



Slika 2-1. Uzroci i troškovi uslijed zatajenja informacijskog sustava (u tisućama dolara)

Sustavi osjetljivi na kvar zataje prosječno 4 do 8 puta na godinu uz trajanje zatajenja od 1 do 4 sata. Ukupno vrijeme trajanja zatajenja na godinu iznosi od 4 do 32 sata. Prosječna raspoloživost „klijent – poslužitelj“ sustava iznosi 98%. Ako se navedenim podacima izračuna cjelogodišnji period zatajenja, može se reći da u jednoj godini sustav nije raspoloživ oko tjedan dana [5].

U literaturi [12] je moguće pronaći analize niza istraživanja zatajenja informacijskih sustava koje su često citirane. Pokazuje se da postotak zatajenja povezanih programskom podrškom iznosi od 20% do 50%, a 10% do 30% odnosi se na zatajenja čiji je uzrok sklopovlje. Za oko 5% zatajenja kao uzrok je prijavljena okolina, dok je za uzrok od 20% do 40% zatajenja navedena računalna mreža. Za 10% do 30% zatajenja smatra se da su uzrokovani ljudskom pogreškom. Tablica 2-2 prikazuje broj zatajenja sustava koje su evidentirane u pojedinoj studiji unutar vremena njegova promatranja. Izračun broja zatajenja na godinu, koji je izrađen na temelju ukupnoga broja zatajenja i duljine promatranja sustava, pokazuje znatan porast broja i duljine perioda zatajenja.

Tablica 2-2. Analizirane studije zatajenja informacijskih sustava, Gibson (2006)

Godina provođenja studije	**Duljina promatranja sustava**	**Sustav**	**Ukupna broj zatajenja**	**Procjena broja zatajenja na godinu**
1986.	3 godine	2 IBM 370/169 *mainframe* računala	456	152
1990.	3 godine	Sustav Tandem	800	267
1990.	8 mjeseci	sustav VAX	364	546
1990.	22 mjeseca	13 VICE datotečnih poslužitelja	300	164
1999.	6 mjeseci	70 Window NT mail poslužitelja	1100	2200
1999.	4 mjeseca	503 čvora u poslovnim organizacijama	2127	6381
2002.	1 – 36 mjeseci	70 čvorova na sveučilištu i internetskom servisu	3200	1067
2003.	3 – 6 mjeseci	3000 računala u internetskom servisu	501	1002
2004.	1 godina	395 čvorova u poslužiteljskoj sobi	1285	1285

U istoj analizi [12] prikazani su rezultati analize zatajenja 22 informacijska sustava visokih performansi koja su promatrana devet godina. Pokazalo se da učestalost zatajenja varirala od 20 do 1000 na godinu.

Tablica 2-3. Učestalost napada na informacijski sustav

GODINA	BROJ NAPADA			
	1-5	6-10	> 10	Ne zna
2007	41%	11%	26%	23%
2006	48%	15%	9%	28%
2005	43%	19%	9%	28%
2004	47%	20%	12%	22%

Tablica 2-3 pokazuje da je preko 70 % anketiranih organizacija doživjelo barem jedan napad na svoj informacijski sustav [13]. To potvrđuje veliku raširenost napada na informacijske sustave i potencijalnog uzročnika njihova zatajenja.

Svi do sada prikazani podaci pokazuju značajnu učestalost zatajenja informacijskog sustava koji podržava informacijska i telekomunikacijska tehnologija, te tendenciju njezina porasta.

Zaključak uvodnog dijela jeste da poslovni sustavi već godinama ovise o informacijskoj tehnologiji i da su preko iste te tehnologije postali ranjivi. Razvojem informacijske tehnologije se razvijaju i metode zaštite informacijskih sustava, počevši od metoda zaštite informacijske tehnologije do naprednih i proaktivnih metoda. Mnoge metode zaštite informacijskih sustava ili bilo kojeg svojstva informacijske imovine se temelje na objektivnom odlučivanju. Odlučivanje je u povijesti bilo ograničeno na ljudsku odluku. Razvojem sustava umjetne inteligencije razvijaju se i sustavi za potporu odlučivanju koji temeljem objektivne obrade informacija nude rješenje ili opcije rješenja [71].

2.2. Raspodijeljeni informacijski sustavi

Raspodijeljeni informacijski sustav je takav sustav u kojemu komponente sustava locirane na umreženim računalima komuniciraju i koordiniraju svoje djelovanje isključivo prosljeđivanjem

poruka [14]. Današnji moderni informacijski sustavi se uglavnom smatraju raspodijeljenim jer imaju sve osobine takvih sustava. Osobine raspodijeljenih sustava su:

- **Dijeljenje resursa**

Pojam resursa ili sredstva je apstraktan, ali najbolje opisuje što je sve moguće dijeliti u raspodijeljenim sustavima. Klijent-poslužitelj model je najviše primjenjivan model raspodijeljenih sustava. Sastoji se od procesa poslužitelja koji su upravljači resursa određenog tipa i od procesa klijenta koji za izvršavanje svog zadatka zahtijevaju pristup dijeljenim resursima. Sami poslužitelji mogu trebati neke od dijeljenih resursa, pa tako mogu istovremeno biti klijenti nekim drugim poslužiteljima. Model zasnovan na objektima je sličan tradicionalnom objektnom modelu koji se koristi kod programiranja. Model promatra svaki izvršni dio programa kao objekt sustava za razmjenu poruka pomoću kojeg se pristupa do mogućnosti objekta. U objektnom raspodijeljenom modelu, svaki dijeljeni resurs promatra se kao objekt.

- **Otvorenost**

Otvorenost je osobina sustava koja definira mogućnost proširivanja na različite načine. Sustav može biti otvoren na sklopovskoj razini, npr. za dodavanje dodatnih vanjskih uređaja, memorije ili komunikacijskih uređaja, ili na programskoj razini, za dodavanje novih funkcija operacijskom sustavu, novih komunikacijskih protokola ili servisa za dijeljenje resursa. Osnovna pretpostavka za otvorenost su standardi koji definiraju sustav na taj način da se može proširivati neovisno o dobavljaču opreme ili programa.

- **Istovremenost**

Kada na istom računalu postoji nekoliko procesa, oni se odvijaju istovremeno. Ako je računalo opremljeno samo sa jednom centralnom upravljačkom jedinicom, onda se to postiže naizmjeničnim izvršavanjem procesa. Ukoliko računalo ima određeni broj centralnih upravljačkih jedinica, može se izračunati broj procesa koji se može izvršavati paralelno što također rezultira poboljšanjem u obliku istog faktora.

- **Skalabilnost**

Raspodijeljeni sustavi moraju djelovati učinkovito bez obzira na veličinu. Također mora postojati mogućnost proširivanja sukladno sa rastom potreba. Najmanji praktičan raspodijeljeni sustav sastoji se od dvije radne stanice i datotečnog poslužitelja. Raspodijeljeni sustavi sagrađeni oko lokalne mreže mogu imati više stotina radnih stanica i više poslužitelja različitih namjena. Više

lokalnih mreža može biti međusobno povezano tako da više tisuća računala zajedno čine jedan raspodijeljeni sustav koji omogućava dijeljenje resursa među njima.

- **Otpornost na pogreške**

Informacijski sustavi ponekad zataje. Kada se pogreška pojavi u sklopovlju ili programskoj podršci, mogu se dobiti pogrešne vrijednosti ili nepotpuni rezultati. Dizajn sustava otpornih na greške temelji se na dva osnovna načela, po jedno za svaki tip grešaka:

  - udvajanje sklopovlja: korištenjem više istih komponenti sklopovlja,
  - otklanjanje programskih grešaka: oblikovanje programa na način da se sami mogu oporaviti od grešaka.

- **Transparentnost**

Transparentnost se definira kao skrivanje pojedinih komponenti raspodijeljenih sustava od krajnjeg korisnika i programera aplikacija na način da se sustav shvaća kao cjelina, a ne kao skup nezavisnih dijelova.

Niti jedna od tih osobina nije posljedica raspodijeljenih sustava. Raspodijeljeni sustavi moraju biti pažljivo planirani i izvedeni na taj način da osiguraju svaku od tih osobina.

2.3. Komunikacija

Raspodijeljeni sustavi su sastavljeni od dijelova koji su fizički i logički odvojeni i koji moraju komunicirati da bi mogli međusobno djelovati. Komponente koje upravljaju ili trebaju resurse realizirane su kao procesi [15]. To je točna pretpostavka za klijent-poslužitelj model, dok kod objektnog modela praktično ostvarenje također može počivati na tom principu.

Komunikacija između dva procesa uključuje slanje i primanje informacija što ima za posljedicu:

- prijenos podataka iz procesa koji šalje, procesu koji prima i
- kod nekih komunikacija sinkronizaciju slanja s primanjem, tako da je proces koji šalje ili prima privremeno zaustavljen dok ne izvrši do kraja akciju koja je inicirala zaustavljanje (npr. pisanje na disk).

Kod prvog slučaja, oba procesa dijele isti komunikacijski kanal, dok je ponašanje opisano u drugom slučaju svojstveno za svaku vrstu komunikacije. Osnovni način realizacije su šalji (*send*) i primi (*receive*) dijelovi koji zajedno čine akcije za prijenos poruke između dva procesa. Akcijom prijenosa poruke se određeni podaci (poruka) koju stvara proces koji šalje, prenose korištenjem određenog komunikacijskog mehanizma (kanala ili porta), do procesa koji podatke prima. Taj mehanizam može biti sinkroni (*blocking*) što znači da pošiljatelj čeka dok primatelj ne primi poruku ili asinkroni (*non-blocking*) kod kojeg se poruka stavlja u niz poruka koje čekaju na primanje, dok proces koji šalje može nastaviti svoje izvršavanje.

Dva osnovna načina komuniciranja su klijent-poslužitelj komuniciranje između dva procesa i grupno slanje (*group multicast*) za komuniciranje između grupe procesa koji međusobno surađuju [15].

Klijent-poslužitelj komuniciranje je orijentirano prema pružanju usluge. Razmjena podataka se sastoji od koraka:

1. proces klijent šalje zahtjev procesu poslužitelju
2. obrada zahtjeva na poslužitelju
3. prijenos odgovora klijentu

Kod **grupnog komuniciranja** procesi razmjenjuju poruke na taj način da svaka poruka ide svim procesima u grupi, a ne samo jednom. Jednom *šalji* pozivu odgovara više *primi* poziva, po jedan na svakog člana grupe zbog toga jer dijele zajednički komunikacijski kanal. Takvo slanje naziva se *Multicast*. Grupno slanje ima sljedeće prednosti:

- Neovisno je o lokaciji objekta kojem je upućena poruka – poruka se šalje svim objektima, dok odgovara samo onaj kojem je namijenjena
- Otpornost na pogreške – poruka može biti poslana istovremeno na više poslužitelja, tako da na nju odgovara jedan ili više od njih. Kvar jednoga od poslužitelja klijent ne primjećuje.
- Istovremeno usklađivanje svih članova grupe – jedan poslužitelj može poslati vrijeme grupnim slanjem tako da se svi ostali poslužitelji i klijenti sinkroniziraju na to vrijeme.

Raspodijeljeni informacijski sustavi i općenito raspodijeljena okruženja komuniciraju razmjenom poruka. Današnji informacijski sustavi upravljaju s velikim brojem informacija koje često služe samo za forenzička istraživanja i različite vrste revizija i naknadnih provjeravanja. Cilj ovoga rada je iskoristiti obilježja raspodijeljenih sustava i utvrditi model koji će biti u stanju upravljati svima

ili velikim brojem informacija s ciljem optimizacije rada i predviđanja neželjenih događaja. Jedan od načina ili prethodnika optimizacije je potpora odlučivanju.

2.4. Sustav za potporu odlučivanju

Sustav za potporu odlučivanju (engl. *decision support system*) podrazumijeva informacijski sustav s mogućnosti pružanja podrške pri donošenju odluka u problemima visoke složenosti na temelju znanja pohranjenog u sustavu i na temelju sveobuhvatnog pregleda situacije (značajki promatranog problema). Potreba za podrškom u odlučivanju danas je prisutna u gotovo svim područjima ljudskog djelovanja. Općenito se može reći da su sustavi za podršku pri odlučivanju primjenjivi u situacijama koje imaju neke od sljedećih značajki:

- Visoka kompleksnost problema – problemi u kojima je potrebno promatrati mnogo čimbenika (varijabli) istovremeno te na temelju sveukupne situacije donijeti odluku.
- Potrebno je ekspertno znanje – mnogi problemi zahtijevaju poznavanje vrlo specifičnog znanja u promatranoj domeni.
- Potrebno je donositi odluke u stvarnom vremenu – često je potrebno odluke donositi u vrlo kratkom vremenskom periodu jer nije moguće uložiti vrijeme u detaljnije analize.
- Nije uvijek dostupan potpun uvid u značajke problema – često je potrebno donositi odluke na temelju nepotpune informacije u sustavu. U takvim situacijama odlučuje se na temelju pretpostavki i/ili statistike a često čak i na temelju subjektivnog osjećaja eksperta u domeni.

Ekspert je osoba koja ima superiorne rezultate pri rješavanju konkretnih instanci problema u svojoj domeni. Primjerice, administrator baza podataka je ekspert u svojemu području rada ako ima dobre rezultate pri upravljanju bazama. Pri tome uopće nije ključna razina stručne spreme ili starosna dob promatrane osobe. Važno je primijetiti kako je moguće da više eksperata za identičan problem može imati više međusobno različitih mišljenja. Dakle, nije neobično da ponekad pri donošenju odluke eksperti i pogriješe. Sustavi za potporu pri odlučivanju koji pokušavaju rješavati probleme za koje je u stvarnom svijetu potrebno ekspertno znanje nazivaju se ekspertni sustavi (engl. *expert systems*). Pri tome se raznim računalnim postupcima pokušava oponašati proces donošenja odluka kojeg obavlja ekspert pri rješavanju konkretnih problema. Jasno je da ključnu ulogu u ekspertnom sustavu igra upravo ekspertno znanje. Stoga se pri izgradnji sustava za potporu pri odlučivanju (ili ekspertnog sustava) mogu izdvojiti tri temeljne zadaće:

- Sakupljanje znanja (engl. *knowledge acquisition*),
- Predstavljanje znanja (engl. *knowledge representation*) i
- Korištenje znanja u trenutku potrebe.

Iako je iz formalne perspektive razumljivo konceptualno razdvajanje ovih pojmova, u praktičnim se realizacijama oni često isprepliću te je teško razlučiti jasnu granicu među njima. U ovom radu naglasak je stavljen na samu metodologiju predstavljanja znanja, ali se u određenoj mjeri dotiču i preostale dvije navedene točke. Sakupljanje znanja [16][17] podrazumijeva proces prikupljanja, analize, transformacije i organizacije znanja kako bi ono postalo prikladno za prikaz i korištenje u računalnim sustavima. Znanje je moguće prikupljati:

- iz raznovrsnih dostupnih medija (članci, smjernice, baze podataka, ...) i/ili
- razgovorima s ekspertima u području.

Izvori znanja razlikuju se u kvaliteti i obliku znanja kojeg pružaju, ali i u samoj složenosti postupka sakupljanja znanja.

Smjernice (engl. *guidelines*) predstavljaju najprikladniji medij za sakupljanje znanja jer sadrže znanje koje je u manjoj ili većoj mjeri formalizirano i eksplicitno izrečeno. Znanje u smjernicama obično pišu eksperti i namijenjeno je isto tako ekspertima, što zapravo znači da smjernice imaju visoku razinu znanja koje se među ekspertima u domeni podrazumijeva. Stoga primjerice smjernice za upravljanje sustavima za otkrivanje neželjenih upada nisu pisane za osoblje izvan tehničke struke. Nadalje, smjernice često sadrže samo prijedloge koji se moraju interpretirati ovisno o kontekstu (koji je često nejasan), što ne pruža dovoljnu podlogu za eksplicitnu formalizaciju u računalnom sustavu. Kako bi se znanje iz smjernica iskoristilo nužno ga je obogatiti implicitnim (skrivenim, intuitivnim, neeksplicitnim) ekspertnim znanjem [16]. Znanje koje posjeduju eksperti se može ugrubo podijeliti u dvije kategorije: eksplicitno i implicitno [18]. Eksplicitno znanje je znanje koje se može artikulirati prirodnim jezikom. Ono se izražava riječima, matematičkim i logičkim izrazima, grafovima i slično. Implicitno znanje je znanje koje je teško izreći formalnim jezikom. Ono je vlastito svojstvo svakog pojedinog eksperta i temelji se na individualnom iskustvu. Implicitno znanje u sebi uključuje subjektivna uvjerenja, subjektivni sustav vrijednosti i subjektivnu percepciju događaja koju percipira ekspert. Dok se eksplicitno znanje relativno lako sakuplja za to predviđenim tehnikama, implicitno znanje predstavlja mnogo složeniji problem.

Kako bi se postigao kvalitetan sustav za potporu pri odlučivanju potrebno je obuhvatiti obje kategorije znanja u maksimalnom mogućem obujmu. Predstavljanje znanja podrazumijeva formalizaciju sakupljenog znanja u obliku u kojem je ono pogodno za uporabu. Danas postoji velik

broj različitih formalizama za predstavljanje znanja sa različitim razinama izražajnosti. Pri tome se redovito javlja problem kompromisa između jednostavnosti prikaza znanja i izražajnosti formalizma. Korištenje znanja podrazumijeva uporabu sakupljenog i predstavljenog znanja u stvarnom okruženju. Pri tome se stavlja naglasak na mogućnost rasuđivanja, tj. na mogućnost izvođenja implicitnog (novog, ne-izrečenog) znanja iz onog koje je eksplicitno izrečeno (postojeće). Kako bi bilo moguće koristiti znanje u stvarnom okruženju ključno je sustavu za potporu pri odlučivanju omogućiti pristup svim potrebnim informacijama koje karakteriziraju promatrani problem kako bi se moglo korištenjem baze znanja rasuđivati na temelju stvarnih i aktualnih značajki problema. Tu se podrazumijevaju razna sučelja baza podataka, sučelja na raznu instrumentaciju i senzore koji očitavaju trenutne vrijednosti parametara, itd.

Znanje na kojemu se temelji model predstavljen u ovome radu je prikupljeno iz stvarnih sustava, a količina znanja ovisi o poznavanju modela i količini informacija uskladištenih u bazi podataka. Izračun vjerojatnosti nekog događaja ovisi o kombinacijama parametara snimljenih u jednakim ili sličnim uvjetima istog sustava. Princip je objašnjen u nastavku, a ispitivanje modela je detaljno analizirano u zadnjem dijelu rada.

3. OSNOVE VJEROJATNOSTI I BAYESOV TEOREM

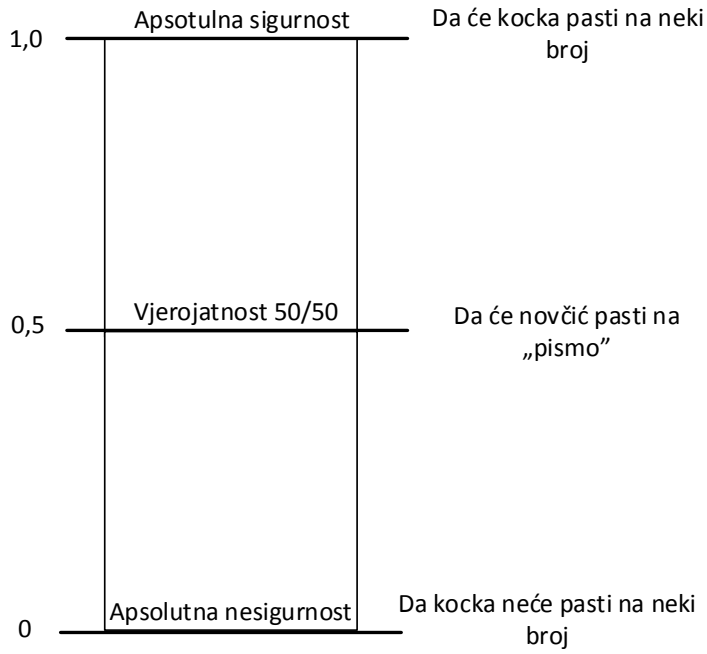
3.1. Uvod u teoriju vjerojatnosti

Teorija vjerojatnosti je matematička disciplina koja se bavi proučavanjem slučajnih pojava, odnosno empirijskih događaja čiji ishodi nisu uvijek strogo definirani. Jedan od osnovnih alata u teoriji vjerojatnosti je eksperiment pomoću kojeg se provodi ispitivanje veze između uzroka i posljedice. Na ishod eksperimenta često utječe više uvjeta i ako se eksperiment ponavlja više puta pod jednakim uvjetima, pojavljuje se određena zakonitost unutar skupa ishoda. Teorija vjerojatnosti se bavi takvim zakonitostima uvođenjem kvantitativne mjere u obliku realnog pozitivnog broja, odnosno vjerojatnosti. Vjerojatnost procjenjuje mogućnost, odnosno nemogućnost ostvarenja ishoda.

Postoje dokazi da su se već indijski matematičari (3. stoljeće prije Krista) bavili pitanjima koja pripadaju današnjoj teoriji vjerojatnosti te da je u 14. stoljeću postojala praksa pomorskog osiguranja koja je omogućila srednjovjekovnim trgovcima ocjenjivanje različitih faktora rizika koji se pojavljuju prilikom prekomorskog trgovanja.
Početak teorije vjerojatnosti se povezuje za XVII stoljeće i za imena francuskih matematičara *Pascala* i *Fermata* koji su proučavali problem vezan za kockarsku igru. Njihov rad iz 1654. godine smatra se početkom teorijskog razvoja vjerojatnosti. Tek poslije 1933. godine, kada je *N. A. Kolmogorov* objavio rad u kojem izlaže osnovne postavke aksiomatske ovisnosti, teorija vjerojatnosti razvija se u obliku moderne matematičke discipline. Ne oslanja se samo na empirijske i intuitivne metode već na formalnu teoriju povezanu s drugim matematičkim pojmovima.

Osnovni pojmovi vjerojatnosti mogu se razlikovati ovisno o točki gledanja te isto tako rezultati i interpretacije rezultata mogu biti različite. Zakoni vjerojatnosti nisu uvijek jednostavni i lako razumljivi. Svakodnevno iskustvo i logika koji se koriste u životu često nisu u skladu sa zakonima koje daje statistika. Pojam poznat pod imenom „*subjektivna vjerojatnost*“ kojim se opisuju spomenute razlike u pristupu pripada među psihološke, a ne statističke pojmove i stoga s matematičkom vjerojatnosti često nema mnogo zajedničkoga [19]. Najčešće korištenje vjerojatnosti je prilikom igranja lutrije. Često se vjeruje da će glavni zgoditak na lutriji biti dobiven, a praktički se ne razmišlja o vjerojatnosti događanja prometne nezgode iako je takva vjerojatnost daleko veća nego ona za dobitak na lutriji (Slika 3-1).
Osnovna pravila vjerojatnosti mogu se sažeti u nekoliko rečenica:

- ako je potpuno sigurno da će se nešto dogoditi onda je vjerojatnost tog događaja maksimalna (p=1), na primjer potpuno je sigurno da će čovjek koji je rođen danas jednoga dana umrijeti,
- ako je potpuno sigurno da se nešto neće dogoditi vjerojatnost tog događaja je minimalna ili jednaka nuli (p=0)
- vjerojatnost da će se između N događaja koji su jednako vjerojatni a međusobno nezavisni dogoditi jedan određeni među njima je $1/N$
- vjerojatnost da će se dogoditi bilo koji od nekoliko mogućih nezavisnih događaja suma je vjerojatnosti svakog pojedinačnog događaja,
- vjerojatnost da će se zajedno dogoditi dva ili više nezavisnih događaja produkt je vjerojatnosti svakog od tih događaja.



Slika 3-1. Svi slučajevi vjerojatnosti nalaze se između apsolutne sigurnosti (p=1) i apsolutne nesigurnosti (p=0)

3.1.1. Osnove vjerojatnosti

Osnovni pojam u teoriji vjerojatnosti je skup Ω koji predstavlja skup svih mogućih ishoda ω jednog eksperimenta. Skup Ω se naziva prostor elementarnim događaja. Slučajni događaj je definiran kao podskup od Ω. Događaj $A(\subset\Omega)$ se ostvaruje samo i samo ako se ostvaruje neki ishod ω koji pripada podskupu A. Skup svih događaja koji odgovaraju jednom eksperimentu nazivaju se poljem događaja i označavaju s F. Polje događaja uvijek sadrži $\Omega(\in F)$ što je moguć događaj i $0(\in F)$ kao

nemoguć događaj. Događaji su u nastavku navedeni s velikim početnim slovima (*A, B, C,* …) i smatraju se pripadnim polju događaja *F*.

Ako ostvarenje događaja *A* uzrokuje i ostvarenje događaja *B* može se reći da događaj *A* implicira događaj *B*, što u teoriji skupova znači $A \subset B$. Ako vrijedi $A \subset B$ i $B \subset C$ podrazumijeva se $A \subset C$, a ako je $A \subset B$ i $B \subset A$ tada su događaji ekvivalentni i piše se $A=B$. Za događaj A postoji suprotan (komplementarni) događaj Ā koji se ostvaruje ako se događaj A ne ostvaruje, odnosno $\bar{A}= \Omega \backslash A$.

Umnožak dva događaja *A* i *B* se označava s *AB* i predstavlja događaj koji se ostvaruje samo ako se ostvare oba događaja i *A* i *B*. Umnožak događaja *A* i *B* je presjek skupova *A* i *B*, odnosno $A \cap B$. Ako su *A* i *B* disjunktni skupovi, tj. $A \cap B = 0$ i kaže se da se događaji *A* i *B* isključuju. Zbroj dva događaja *A* i *B* se označava kao unija dva skupa $A \cup B$. Razlikom *A* i *B* se smatra događaj koji se ostvaruje ako se ostvari barem jedan od *A* ili *B* i operaciju označavamo s $A \setminus B$.
Definicija presjek i unije može se proširiti na konačan broj događaja. Ako je $A_1, A_2, \ldots A_n$ skup od konačno mnogo događaja i $I_n=\{1, \ldots, n\}$ indeksni skup, tada je:

$$\bigcap_{i=1}^{n} A_i = \{\omega | \; za\ svaki\ i \in I_n\ vrijedi\ \omega \in A_i\} \qquad (1)$$

$$\bigcup_{i=1}^{n} A_i = \{\omega | \; postoji\ i \in I_n\ tako\ da\ je\ \omega \in A_i\} \qquad (2)$$

Ako je $A_iA_j = 0\ (i \neq j)$, tada umjesto $\bigcup_i A_i$ pišemo $\sum_i A_i$.
Klasična definicija vjerojatnosti se temelji na predstavljanju vjerojatnosti događaja kao relativnoj učestalosti broja povoljnih ishoda. Na primjer, ako je *A* događaj u kojem se pri bacanju kocke pojavi broj *4*, a *n* i *n(A)* predstavljaju redom ukupan broj eksperimenata i broj pojavljivanja broja *4*, tada se nakon dovoljnog broja bacanja kocke može primijetiti da se učestalost događaja *A* izražena količnikom *n(A)/n* približava broju *1/6*. Taj broj se smatra mjerom vjerojatnosti ostvarenja događaja *A*.
Kada promatrajmo skup svih međusobno isključivih i jednako vjerojatnih događaja $\omega_1, \omega_2, \ldots, \omega_n$ koji čine potpuni skup događaja moguće je pisati:

$$\bigcup_{i=1}^{n} \omega_i = \sum_{i=1}^{n} \omega_i = \Omega. \qquad (3)$$

Što dovodi do definicija klasične vjerojatnosti:

Neka je $\Omega=\{ \omega_1, \ldots, \omega_n \}$ skup svih mogućih jednako vjerojatnih događaja koji su međusobno neovisni i neka je $A=\{ \omega_{i1}, \ldots, \omega_{im} \}$ događaj koji se sastoji od m elementarnih jednako vjerojatnih događaja koji imaju svojstvo koje definira događaj A. Vjerojatnost ostvarenja događaja A jednaka je:

$$P(A) = \frac{m}{n}. \quad (4)$$

Klasična definicija vjerojatnosti može se napisati i u obliku:
Vjerojatnost $P(A)$ događaja $A \subseteq \Omega$ jednaka je količniku broja povoljnih ishoda eksperimenta koji doprinose ostvarenja događaja A i broja svih ishoda.

3.1.2. Uvjetna vjerojatnost

Uvjetna vjerojatnost je pojam s kojim se svi svakodnevno susreću iako često i ne razmišljaju o njemu, barem ne na matematički način. Pretpostavi li se situacija u kojoj neka karakteristika jedne zamišljene varijable ima direktan utjecaj na neku karakteristiku te iste varijable. Na primjer, prisutnost ili ne postojanje kvara sustava besprekidnog napajanja ima direktan utjecaj na to hoće li ispitivanje tog uređaja dati pozitivne ili negativne rezultate.
Bayes je bio engleski svećenik koji se strastveno bavio problemima vjerojatnosti te je pronašao zakone koji se ponešto razlikuju od klasičnog pristupa pitanju vjerojatnosti. Konkretno on je izradio matematičke postupke koji omogućuju mijenjanje vjerojatnosti nekog ishoda pod utjecajem novih informacija. Bayesovi principi danas zauzimaju ključno mjesto u teoriji odlučivanja. Godinama se Bayes-ov teorem koristio kako bi se došlo do uvjetovanih zaključaka o spomenutoj i sličnim situacijama. U navedenom primjeru bio bi korišten teorem za izračunavanje uvjetne vjerojatnosti je li uređaj u kvaru i može li prouzročiti ispad cijele sistem sobe, a time i nedostupnost informacijske imovine.
Dalje se može pretpostaviti situacija u kojoj je više obilježja povezano kroz lance takvih zaključaka. Na primjer, da li su zabilježeni podaci koji upućuju na neispravnost uređaja za neprekidno napajanje kao što su zagrijavanje baterija, višestruki alarmi na sustavu ili je uređaj jednostavno star. Nadalje postojanje ili nepostojanje navedenih parametara upućuje na postojanje rizika od ispada. Jednako tako, ukoliko je uređaj za neprekidno napajanje u kvaru to ima utjecaj na parametre koji se bilježe u sustavu. U ovakvim i sličnim situacijama cilj je doći do spoznaja i donijeti uvjetovane zaključke koji nisu posljedica direktnih utjecaja. Na primjer, izračunati uvjetnu vjerojatnost pri kojoj je uređaj u kvaru na temelju pokazatelja koji opisuju njegov rad. Temperatura

pri tome nema nikakvog utjecaja na kapacitet baterije i naravno na starost uređaja. Slijedom toga, željene uvjetne vjerojatnosti nije moguće proračunati izravnom primjenom Bayes-ovog teorema. U želji za rješavanjem ovakvih problema razvijene su Bayes-ove mreže.

Istraživanjem uvjetnih ovisnosti lanaca odnosa moguće je uporabom Bayes-ovih mreža predstaviti velika područja na malom prostoru te istovremeno izvoditi uvjetovane zaključke između karakteristika atributa u prihvatljivom vremenu. Dodatno, mogućnost vizualnog prikazivanja Bayes-ovih mreža pruža daleko kvalitetniji i intuitivan pregled odnosa između varijabli.

Bayesove mreže predstavljaju grafičke strukture za predstavljanje uvjetnih vjerojatnosti između velikog broja varijabli (atributa) te donošenje uvjetovanih zaključaka a vezano na navedene varijable [73]. Tijekom 80-ih godina prošlog stoljeća naglo se povećava broj radova i relevantnih istraživanja vezano na Bayesove mreže (dijagrami utjecaja, kauzalne mreže, mreže temeljene na uvjetnoj vjerojatnosti). Tijekom 90-ih godina dolazi do naglog razvoja spoznaje o primjenjivosti raznih algoritama treniranja Bayesovih mreža iz podataka.
Promatrajmo eksperiment s konačnim brojem događaja. Označi li se s n_A, n_B, n_{AB} broj elementarnih događaja koji dovode do ostvarenja događaja *A*, *B*, *AB* u *n* ispitivanja. Prema klasičnoj definiciji vjerojatnosti vrijedi:

$$P(B) = \frac{n_B}{n}, P(AB) = \frac{n_{AB}}{n}. \quad (5)$$

Budući da je ostvarenje slučajnog događaja *A* uvjetovano ostvarenjem događaja *B*, tada pri određivanju uvjetne vjerojatnosti $P(A|B)$ broj n_B predstavlja broj svi mogućih elementarnih događaja za ostvarenje događaja *B*, a n_{AB} onaj broj tih događaja koji dovode do ostvarenja događaja *A*. Zato je:

$$P(A|B) = \frac{n_{AB}}{n_B} = \frac{\frac{n_{AB}}{n}}{\frac{n_B}{n}} = \frac{P(AB)}{P(B)}, P(B) > 0 \quad (6)$$

U slučaju da je događaj *B* uvjetovan ostvarenjem događaja *A*, analogno je doći do zaključka:

$$P(B|A) = \frac{P(AB)}{P(A)}, P(A) > 0. \quad (7)$$

Iz navedenog slijedi i suprotno:

$$P(AB) = P(B) \cdot P(A|B) = P(A) \cdot P(B|A) \quad (8)$$

Za slučajan događaj *A* kaže se da je neovisan o događaju *B* ako je uvjetna vjerojatnost ostvarenja događaja *A* pod uvjetom nastupanja događaja *B*, jednaka bezuvjetnoj vjerojatnosti događaja *A*, odnosno *P(A|B)=P(A)*. Iz definicije uvjetne vjerojatnosti (6) slijedi:

$$P(A|B) = \frac{P(AB)}{P(B)} = P(A), odakle\ je \quad (9)$$

$$P(AB) = P(A) \cdot P(B) \quad (10)$$

Dakle, u slučaju kada jedan događaj ne ovisi o drugom, vjerojatnost njihovog umnoška jednaka je umnošku njihovih vjerojatnosti. Iz izraza (10) slijedi:

$$P(B|A) = \frac{P(AB)}{P(A)} = \frac{P(A)P(B)}{P(A)} = P(AB) \quad (11)$$

Sada je vidljivo da ako događaj *A* ne ovisi o *B*, tada ni *B* ne ovisi o *A* i može se zaključiti da su događaji *A* i *B* neovisni ako je vjerojatnost njihovog umnoška jednaka umnošku njihovih vjerojatnosti.

3.1.3. Bayesov teorem

Ako su $H_1, \ldots, H_n$ međusobno neovisni događaji, $P(H_i)>0\ (i=1, \ldots, n)$ i $H_1 + \ldots + H_n = \Omega$, tada je:

$$P(A) = \sum_{i=1}^{n} P(H_i)P(A|H_i)\ za\ svaki\ događaj\ A \in F \quad (12)$$

Kako je

$$P(H_i|A) = P(H_i)P(A|H_i) = P(A)P(H_i|A)\ , (i = 1, \ldots, n) \quad (13)$$

slijedi:

$$P(H_i|A) = \frac{P(H_i)P(A|H_i)}{P(A)} \quad (14)$$

i primjenom (12) za dobiva se Bayesova formula (15):

$$P(H_i|A) = \frac{P(H_i)P(A|H_i)}{\sum_{j=1}^{n} P(H_j)P(A|H_j)}, (i = 1, \dots, n, A \in F) \quad (15)$$

Vjerojatnosti $P(H_i)$ su obično poznate unaprijed, prije provođenja eksperimenta pa se nazivaju *apriornim* vjerojatnostima, a događaji *hipotezama*. Hipoteze H_i pri tome čine potpuni skup događaja.

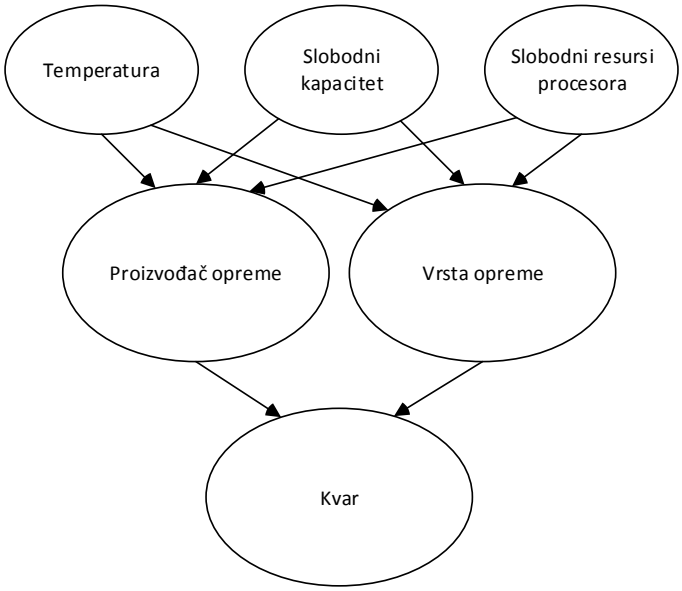
3.1.4. Bayesova mreža

Metode razlučivanja temeljene na vjerojatnosti postaju s vremenom sve zanimljivije. Na žalost, zbog svoje prirode, složenost procesa izgradnje modela prepreka je češćem korištenju. Osnovni koncept Bayesovih mreža počiva na uvjetnoj vjerojatnosti. Uvjetna se vjerojatnost definira kao:

$$P(A|B) = m \quad (16)$$

što se može interpretirati kao „*Vjerojatnost događaja A iznosi m uz dani uvjet B*“.

Uvjetna vjerojatnost umanjuje polje slučajnih događaja, te donosi dodatnu informaciju reducirajući pri tome stupanj neizvjesnosti ishoda događaja (Slika 3-2) [21].



Slika 3-2. Jednostavan grafički prikaz Bayesove mreže

Ovakvi grafički sustavi pogodni su modeli za automatizirano razlučivanje pod nepotpuno uređenim uvjetima.

Temeljno pravilo vjerojatnosti događaja *A* i *B* glasi:

$$P(A|B)P(B) = P(AB) \quad (17)$$

Ako se događaji *A* i *B* promatraju u kontekstu događaja *C*, to se može izraziti kao:

$$P(A|B,C)P(B|C) = P(A,B|C) \quad (18)\ [1]$$

Na osnovu temeljnog pravila uvjetne vjerojatnosti proizlazi:

$$P(A|B)P(B) = P(B|A)P(A) \quad (19)$$

iz čega proizlazi Bayesova formula u obliku:

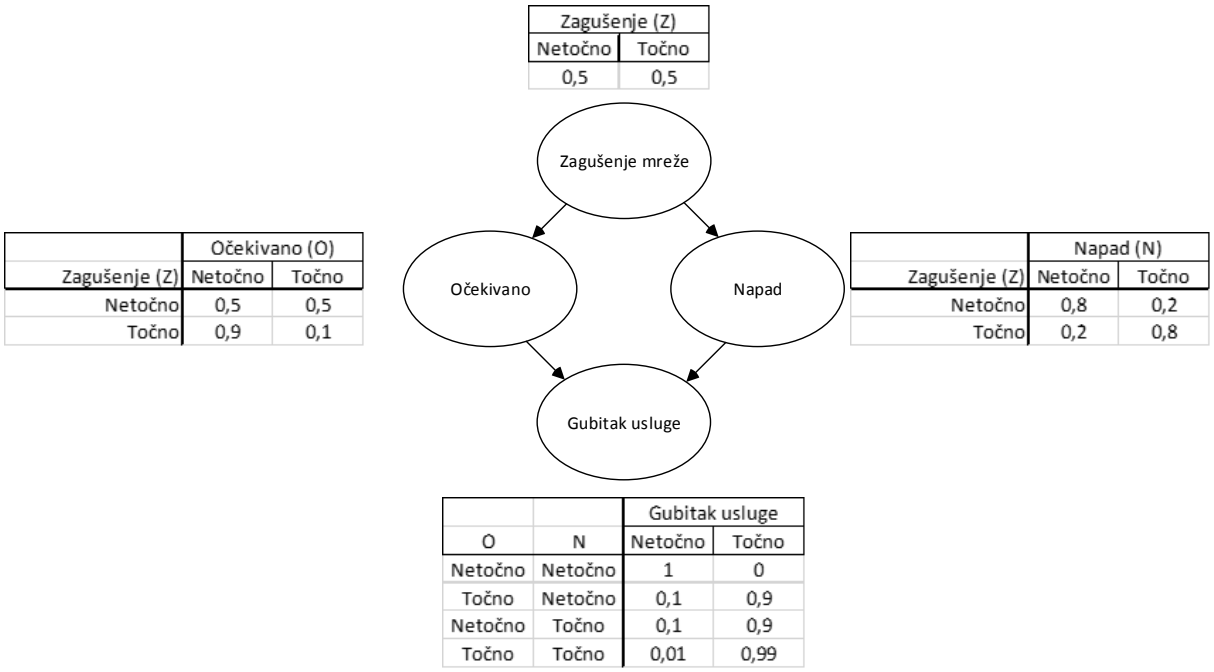
$$P(B|A) = \frac{P(A|B)P(B)}{P(A)} \quad (20)$$

odnosno gledajući u svjetlu događaja C:

[1] Uvedena je oznaka A,B umjesto A|B zbog umetanja događaja C i praktičnijeg prikaza

$$P(B|A,C) = \frac{P(A|B,C)P(B|C)}{P(A|C)} \quad (21)$$

Za složeniji prikaz Bayesove mreže potrebno je definirati distribuciju uvjetne vjerojatnosti (*Conditional Probability Distribution*) za svaku točku [73]. Ako su vrijednost varijabli diskretne mogu se prikazati tablicom koja prikazuje vjerojatnosti da sljedeća točka niza preuzima svaku od kombinacija vrijednosti roditelja, prethodnika (Slika 3-3).



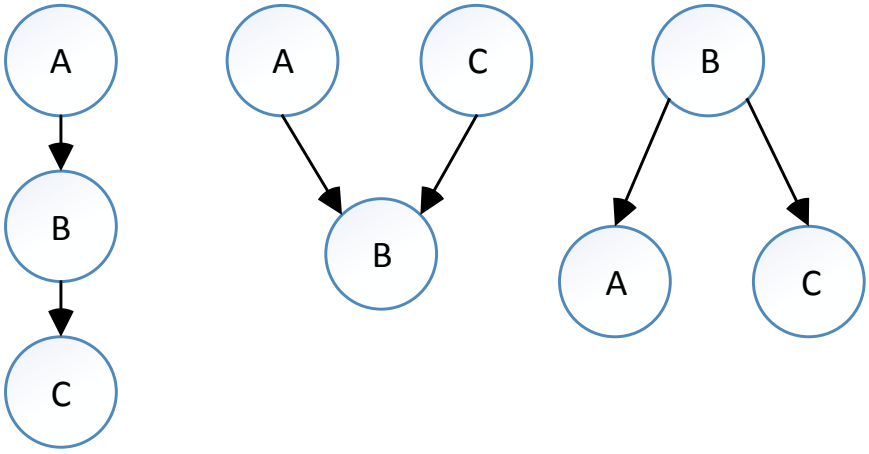
Slika 3-3. Grafički prikaz Bayesove mreže i tablica uvjetne vjerojatnosti

Iz navedene ilustracije moguće je zaključiti da izraz „*Gubitak usluge*“ (G= *istina*) ima dva moguća uzroka: ili se dogodilo očekivano zagušenje (O=*istina*) ili neočekivani napad (N=*istina*). Snaga tih odnosa prikazana je u pripadajućim tablicama pa tako vjerojatnost da je došlo do gubitka usluge (G=*istina*) pri činjenici da očekivanom zagušenju (O=*istina*) i napadu (N= *istina*) iznosi 0,99 ili 99%. Na ovaj način se Bayesov teorem vizualizira i prikazuje u grafičkom obliku. Model predstavljen u radu neće se baviti izradom i korištenjem Bayesovih mreža već pomoću Bayesovog teorema i upotrebom algoritma izračunavati vjerojatnosti neželjenih događaja na temelju poznatih vjerojatnosti ostvarenih događaja iz prošlosti.

Bayesove mreže predstavljene su takozvanim usmjerenim acikličkim grafovima [73]. Jedna od osobina ovakvog pristupa je to što potpuna specifikacija distribucije vjerojatnosti sadrži znatno manje vrijednosti. Za četiri varijable potpuna distribucija sadržavala bi (2^n-1), tj. 15 vrijednosti za

sve kombinacije. Spomenuti slučaj s gubitkom usluge sadrži ih devet. Za veći broj elemenata mreže značaj ovakvog pristupa postaje još veći.

Elementi mreže prikazani su kao ovisni o slijedu koji je naznačen strelicama, pri čemu smjer strelice određuje smjer odnosa, a vjerojatnosti se primjenjuju ovisno o vezama koje mogu biti linearne, konvergentne ili divergentne kako je prikazano na slici (Slika 3-4).



Slika 3-4. Tri vrste veza među elementima mreže

Vezama se unaprijed navodi na ovisnosti definirane kao značajne ili ovisne pri izgradnji modela. Elementi mreže putem vjerojatnosti prenose informacije, pri čemu se moguća rješenja generiraju kao aproksimativne vrijednosti. Ovaj pristup, ovisno o mreži, omogućava više puteva do istog rješenja uz mogućnost evaluacije rezultata tijekom analize. Time se pruža mogućnost rješavanja problema na način koji ne mora nužno pratiti eksponencijalni rast pravila porastom kompleksnosti modela kao što je slučaj pri tradicionalnim metodama.

Temelj za određivanje uvjetnih vjerojatnosti je strukturno učenje, odnosno, do navedenih vrijednosti dolazi se učenjem putem algoritama razvijenih u tu svrhu.

U ovom radu Bayesove mreže su predstavljene samo kao model koji opisuje pripadajući teorem na temelju kojega je izrađen algoritam modela procjene vjerojatnosti neželjenih događaja.

3.1.5. Upotreba Bayesovog teorema u modelu

U radu je predložen model za procjenu vjerojatnosti neželjenih događaja u informacijskim sustavima. Model se temelji na korištenju Bayesovog teorema (20) za izračun vjerojatnosti ostvarenja događaja *A* na temelju poznatih vjerojatnosti pojave događaja *B* o kojima je ovisan

događaj *A*. Pretpostavka za korištenje modela je mogućnost korištenja zapisa o prethodnih događajima ili baza znanja na temelju kojim je moguće korištenjem teorije vjerojatnosti izračunati iznose vjerojatnosti pojedinog događaja.

Tablica 3-1 prikazuje primjer baze podataka u kojoj je na temelju broja pojava praćenog parametra u nepovoljnim i u povoljnim događajima izračunata vjerojatnost nepovoljnog događaja s obzirom na ostvarenje pojedinog događaja.

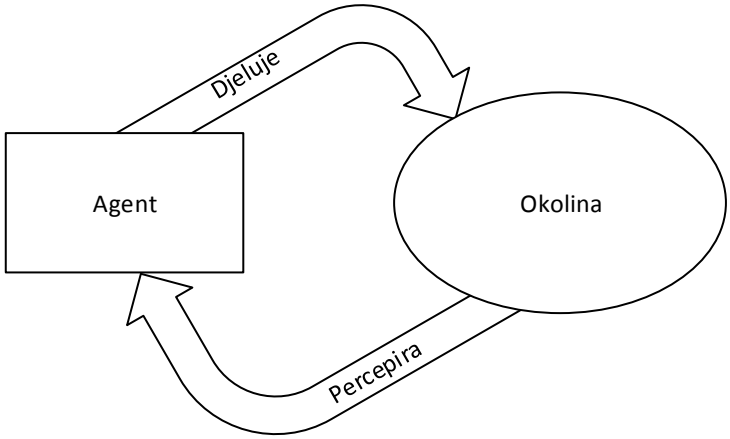
Tablica 3-1. Primjer baze podataka

Naziv parametra	**Broj pojava parametra u nepovoljnim događajima**	**Broj pojava parametra u povoljnim događajima**	**Vjerojatnost nepovoljnih događaja**	**Broj nesigurnih događaja**
Popunjenost mrežnog diska prosječna	70	389	51,20%	19
Iskorištenost pojasne brzine iznad 75% zakupljene	97	384	59,56%	23
Mrežni promet 75% veći od prosjeka	83	383	55,82%	18
Temperatura u serveru 50% iznad prosječne	67	373	51,16%	17
Obrada traje 25% dulje vremena od prosjeka	24	465	23,13%	9
Istom zapisu u bazi istovremeno pristupa 75% djelatnika više od maksimuma	90	363	59,11%	11

Tablica prikazuje samo dio praćenih parametara, a na temelju cjelokupnog skupa podataka izračunate su vjerojatnosti prikazane u tablici vjerojatnosti parametara praćenih u eksperimentu (Tablica 5-13). Svi eksperimenti su provedeni korištenjem istog algoritma kojim su računate vjerojatnosti.

3.2. Agenti u raspodijeljenom okruženju

Agent je svaki subjekt koji može opažati okolinu korištenjem senzora i djelovati na okolinu (Slika 3-5) korištenjem izvršnih uređaja naziva se agentom. Alternativna definicija agenta [22][23] kaže da je agent računalni sustav smješten u okolini i sposoban za autonomno djelovanje u svrhu ispunjenja zadanih ciljeva.



Slika 3-5. Međudjelovanje agenta i okoline

Inteligentni (racionalni) agent je agent sa svojstvima reaktivnosti, proaktivnosti i socijalne (društvene) sposobnosti [23].

- Reaktivnost – u slučaju potrebe, odgovara na situaciju unutar zadanih vremenskih ograničenja
- Proaktivnost – nastoji ostvariti vlastite ciljeve
- Socijalna sposobnost – ostvaruje interakciju s drugim agentima u svrhu ispunjenja ciljeva

Više-agentski sustav (engl. *multiagent system*) je sustav koji se sastoji od većeg broja agenata koji se mogu nalaziti u međusobnoj interakciji. Agent je rijetko samostalan sustav. U većini situacija on će postojati paralelno s drugim agentima i nalaziti se u interakciji s njima [22].

Koncept agenta postao je vrlo bitan, kako u području umjetne inteligencije (engl. *artificial inteligence*) tako i računarstva općenito [23][72]. Budući da potreba za digitalnim informacijama raste velikom brzinom, a proporcionalno tome raste i upotreba za računalnim resursima, potrebno je revidirati tradicionalne tehnike upravljanja resursima, topologijom i sustavima [22]. Kako bi se postigla željena razina visoke dostupnosti, brzine i usluga postoji trenutačno nekoliko računalnih infrastruktura koje osiguravaju dostupnost resursa [22][23]. Međutim, sva učinkovita komercijalna rješenja visoke dostupnosti imaju sljedeće nedostatke [22]:

- Mogu se primijeniti na samo određene tipove platformi,
- Skupa su i zahtijevaju specijalizirane administratore,
- Administrator/ekspert ne može jamčiti besprekidni uspješni rad sustava, budući da pojedinac ne može pokriti sve aspekte složenog sustava,

- Sustavi su otporni na greške, ali se ne mogu samostalno oporaviti od havarije. Postupci oporavka su često ručni i zahtijevaju interakcije operatera. Rješenje je u implementaciji sustava kontinuiranog poslovanja koje objedinjuje poslovne i tehničke procese i organizira procese s ciljem jamčenja besprekidnosti poslovanja [69],
- Budući da aplikacije nisu svjesne okruženja (nisu inteligentne), padom ključnih dijelova može doći do nedostupnosti cjelokupnog sustava.

Agenti su primarno dizajnirani kako bi nadgledali sustav, servise i ispravljali pogreške nastale prilikom rada uz manje izgubljenog vremena [24]. Agentom može biti nazvan bilo koji subjekt u sustavu koji provodi razmjenu informacija. Razmjena ne mora biti obostrana i dovoljno je da agent samo šalje informacije, ali u tome slučaju potrebno je u strukturi imati i centralni agentski sustav koji sadrži logiku upravljanja. Logika upravljanja definirana je algoritmima.

3.3. Algoritmi

Povećanjem složenosti mnogih problema pojavila se potreba za rješenjima koja se mogu prilagoditi pojedinim zadacima. Unutar područja umjetne inteligencije izdvojili su se neki pristupi u rješavanju kompleksnih problema koji koriste evolucijske algoritme. Evolucijski algoritmi su skup stohastičkih metoda koji djelotvorno pretražuju zadani prostor [10][71].

Metode koje spadaju u područje evolucijskih algoritama:

- genetski algoritmi,
- evolucijske strategije,
- genetsko programiranje,
- evolucijsko programiranje i
- sustavi klasifikacije sa sposobnošću učenja.

U ovome radu prikazan je model temeljen na sustavima klasifikacije sa sposobnošću učenja.

3.4. Terminologija učenja

Pokušaji definiranja pojma inteligencija upućuju na spoznavanje, razumijevanje, interpretaciju ili prikupljanje znanja učenjem, istraživanjem ili iskustvenim postupcima. Moguće ju je definirati i kao varijabilnost, fleksibilnost, raznovrsnost i snalažljivost subjekta novim okruženjima, situacijama ili zadacima temeljem apsorbiranog znanja ili iskustva. Teško je navesti općenito prihvaćenu definiciju inteligencije, ali u manjoj ili većoj mjeri sve postojeće ukazuju na neki vid prikupljanja znanja, što se ostvaruje različitim metodama učenja. Dakle, moguće je zaključiti kako je inteligencija u uskoj vezi s učenjem i kapacitetima subjekta koji uči. Subjekt može biti čovjek, životinja ili stroj. Ukoliko je potrebno stvoriti stroj koji će imati neke osobine inteligentnog ponašanja čovjeka [25] tada je riječ o umjetnoj inteligenciji [26], a ona dakako nije moguća bez učenja koje se u ovom slučaju naziva strojno učenje (*engl. machine learning*), [71].

U protekla dva desetljeća strojno učenje je unutar područja umjetne inteligencije izraslo u zasebno područje s vlastitim predmetom istraživanja, metodama i postupcima te teorijskim okvirom [74]. Riječ je o interdisciplinarnom području, budući da se naslanja na dostignuća iz brojnih drugih disciplina, kao što su statistika, teorija informacija, teorija upravljanja, teorija sustava, filozofija, psihologija, kognitivne znanosti, neurofiziologija i brojne druge. S druge strane, strojno učenje je sastavni dio brojnih drugih područja kao što su prepoznavanje oblika (*engl. pattern recognition),* rudarenje podacima *(data mining),* otkrivanje znanja u bazama podataka *(engl. knowledge discovery in databases),* inteligentna analiza podataka *(engl. intelligent data analysis)* [27][74]. Primjena je vrlo raznovrsna: od obrade signala [28], predviđanja cijena dionica [29] ili kreditnog rizika [30], prepoznavanju i detekcija teksta [31], govora [32] ili lica [33], segmentaciji tržišta [34], modeliranja web ponašanja korisnika [35], kreiranja spam filtera [36], komprimiranja podataka [37], analizi strukture proteina, genetici [38], robotici [39], medicinskoj dijagnostici, itd. Predmet ovoga rada je izrada i ispitivanje modela za procjenu vjerojatnosti neželjenih događaja s funkcionalnošću učenja. Učenje je predloženo kao dodatna funkcionalnost koja model proširuje u područje umjetne inteligencije. Cilj modela je na jednostavan način i upotrebom podataka koji se već prikupljaju i čuvaju te njihovom obradom, doći do zaključaka pomoću kojih je moguće optimizirati rad informacijskog sustava.

3.4.1. Strojno učenje

Strojno učenje (*engl. machine learning*) je područje unutar umjetne inteligencije koje predstavlja temelj za izradu bilo kakvog inteligentnog sustava [24]. Već iz inicijalnog pregleda bibliografskih i baza podataka s cjelovitim tekstom vidljivo je da se metode strojnog učenja koriste u mnogim područjima kako u tehničkim i informacijskim znanostima, tako i u ekonomiji, biologiji, biokemiji, ekologiji, medicini i drugim područjima.

Postoje brojne definicije strojnog učenja, a prema [40] strojno učenje predstavljeno je računalnim programom koji uči iz iskustva:

„Računalni program uči iz iskustva (*E – Experience*) izvođenje nekog zadatka (*T – Task*) prema utvrđenoj mjeri izvedbe (*P – Performance*) ukoliko se njegova izvedba zadatka *T*, mjerena s *P*, poboljšava s iskustvom *E*."

Neki autori [41] navode da se pod strojnim učenjem podrazumijeva izrada računalnih programa koji optimiziraju izabrani kriterij izvedbe upotrebom prikupljenih podataka ili temeljem prethodnih iskustava.

Osnova je dakle računalni program koji nema tipičnu algoritamsku strukturu, nego optimira izabrani kriterij (ili više njih) iz prikupljenih podataka ili drugačije definiranih iskustava. Ovdje je potrebno razlučiti što se misli pod tvrdnjom nepostojanja tipične algoritamske strukture. Dobro je poznato da je algoritam precizno definiran niz radnji koje je potrebno slijediti kako bi se ostvario željeni cilj. U kontekstu računarstva, pod algoritmom se podrazumijeva niz instrukcija koje se trebaju slijediti kako bi se transformirao ulaz u željeni izlaz. Tipičan primjer iz osnova programiranja su algoritmi sortiranja, pa se u tom slučaju može govoriti o efikasnosti tih algoritama s obzirom na broj instrukcija koje izvršavaju, vremenu pronalaska rješenja ili količini memorije koju alociraju i upotrebljavaju. Međutim, što je sa slučajevima u kojima nema dovoljnog znanja o tome koje korake je potrebno provesti i kojim slijedom kako bi traženi rezultat bio dobiven?

Općenito, riječ je o slučajevima u kojima nedostaje znanje o prirodi problema, odnosno slučajevima u kojima nije moguće definirati zakonitosti preslikavanja ulaza u odgovarajući izlaz. Tipični primjeri su sposobnost čovjeka da gotovo trenutno prepozna neku osobu iz različitih kutova i u slučajevima kada ista osoba nije viđena godinama u kojima su se dogodile znatne promijene u izgledu ili sposobnost ljudi da pročitaju raznovrsne rukopise iako su ih vidjeli po prvi puta, a znatno odudaraju od takozvane „klasične" forme [74]. U takvim primjerima moguće je poslužiti se drugačijim pristupom, a to je da se nedostatak u znanju nadoknadi analizom velike količine podataka. U primjeru prepoznavanja rukopisa moguće je promatrati tisuće redaka zapisa

različitih rukopisa kako bi se utvrdile sve morfologije pojedinih simbola čime računalo može naučiti razlikovati jedan simbol od drugog. Mjere izvedbe u navedenom primjeru mogle bi biti: brzina prepoznavanja, točnost i pouzdanost. Naravno da se ovdje pod analizom velike količine podataka i spomenutog promatranja tisuća redaka raznovrsnih zapisa podrazumijevaju aktivnosti koje obavlja računalo.

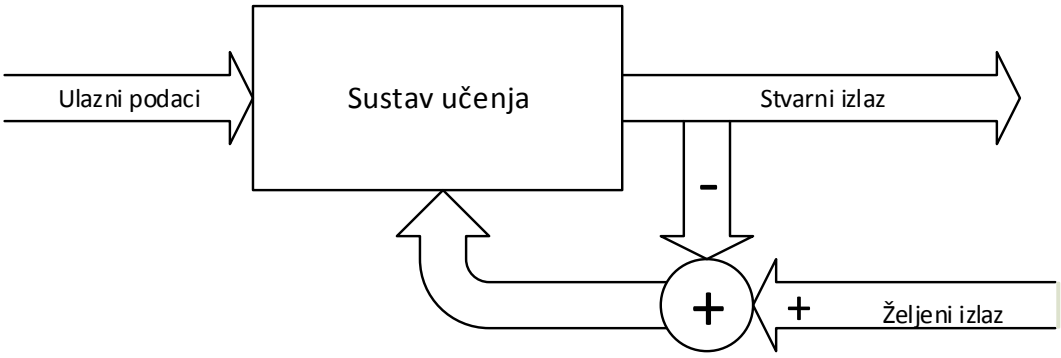
Iz navedenog moguće je zaključiti da je osnovna ideja strojnog učenja modeliranje procesa koji bi generirao prikupljene podatke. Modeli mogu biti raznovrsni, a njihov izbor prvenstveno ovisi o prirodi problema i vrsti podataka. Među najvažnije modele ubrajaju se raznovrsne funkcije, neuronske mreže, funkcije gustoće vjerojatnosti, asocijacije, stabla odluke, Bayesove mreže i dr. Nakon ugađanja parametara izabranog modela optimizacijom definiranog kriterija sam model se može koristiti za predviđanje, dijagnostiku, upravljanje, validaciju ili simulaciju. A u brojnim slučajevima i za objašnjenje samog principa koji stoji iza podataka [27].

3.4.2. Osnovna područja strojnog učenja

Različiti radovi [27][41][42][43] ukazuju da se do danas pod osnovnim područjima strojnog učenja podrazumijevaju:

- nadzirano učenje (*engl. supervised learning*)
- nenadzirano učenje (*engl. unsupervised learning*)
- pojačano učenje (*engl. reinforcement learning*)
- teorija učenja (*engl. learning theory*)

Kako se radi o teorijskom okviru strojnog učenja, u nastavku je navedena kompilacija svih područja. *Supervised learning* je oblik učenja u kojem računalo iz predočenih ispravnih parova ulaz-izlaz treba naučiti dodijeliti ulaznim vrijednostima odgovarajuće izlazne (*mapirati*). Proces učenja sastoji se od dvije faze – faze treninga i faze validacije (Slika 3-6). Cilj nadziranog učenja je izabrati takvu kombinaciju koja će najbolje vršiti generalizaciju nakon viđenih parova ulaznih i izlaznih vrijednosti dobivenih od strane eksperata Trening služi za određivanje hipoteze dodjeljivanja $h:X \rightarrow Y$ i ugađanja njezinih parametara, dok faza je validacije namijenjena za povećanje sposobnosti generalizacije iste, tj. što ispravnijeg dodjeljivanja primjera koji nisu bili dio testnog skupa podataka.



Slika 3-6. Nadzirano učenje

Parovi vrijednosti ulaznih veličina i željenih izlaznih dobiveni su procesom nadgledanja (*supervision*) gdje je više eksperata utvrdilo pripadajuće parove. Skup trening podataka je skup svih tako određenih parova ulaznih i izlaznih vrijednosti $S_t = (x^i, y^i)$ za sve *i = 1, ..., m*, gdje je *m* broj trening primjera. Analogno se definira i validacijski skup, ali broj primjera u njemu najčešće bude manji od broja primjera u skupu za učenje. Hipoteza *h*, koja je iz nekog skupa hipoteza *H* nije ništa drugo nego izabrani model za specifični problem.

Ulazni vektor *x* često ima više komponenti iz razloga što se u razmatranje uzima više atributa koji određuju izlaznu vrijednost. U tom slučaju formira se takozvana projektna matrica u kojoj svaki stupac predstavlja jedan ulazni primjer, a reci određuju atribute (*n*). Uz prethodnu oznaku u kojoj je *m* označavao broj ulaznih podataka skupa za treniranje nastati će *m* x *n* dimenzijska projektna matrica. Mjere izvedbe prema kojima se ugađa hipoteza *h* mogu biti raznovrsne, a najjednostavnije je shvatiti kvadrat odstupanja veličina dobivenih preko h^i u odnosu na stvarne vrijednosti y^i. Optimizacijski cilj u tom slučaju je smanjiti kvadrat odstupanja predviđenih od stvarnih vrijednosti, dok se sam optimizacijski postupak može provesti na različite načine (npr. *Gradient descent* ili *Newtonovom metodom*). Funkcija cilja u tom slučaju se može zapisati kao:

$$J(\Theta) = \frac{1}{2}\sum_{i}^{m}(h_\Theta(x^i) - y^i)^2 \qquad (22)$$

Za razliku od prethodnog modela učenja kod nenadziranog učenja nisu poznate vrijednosti izlazne (ciljane) varijable, već samo opisi i vrijednosti ulaznih podataka koji mogu i u ovom slučaju imati više atributa. Ulazni skup podataka opet se dijeli na skup za treniranje i za ocjenu (validaciju) u cilju što bolje generalizacije. Sada nastaje projektna matrica kojoj nisu pridružene pripadajuće izlazne vrijednosti. Cilj je dobiti hipotezu koja najbolje opisuje postojeće podatke i u skladu s tim opisom pridružuje nove, neviđene primjere.

U okviru pojačanog učenja riječ je o problemima koji se odnose na djelovanje autonomnog agenta u nekom okruženju s ciljem postizanja željenog cilja odabirući niz akcija. Problem je pronaći slijed akcija (ili jednu akciju) koji će dati najbolji rezultat u rješavanju postavljenog problema. Agent prima informacije o vlastitom trenutnom stanju u okolini (okruženju) i poduzima akcije kako bi ga promijenio do ostvarenja postavljenog cilja. Algoritam učenja je u ovom slučaju funkcija koja nagrađuje pozitivne akcije i kažnjava (negativna nagrada) loše. Nagrada ili kazna često nije rezultat samo jedne akcije, već čitavog niza. Kako je djelovanje funkcije nagrađivanja (pozitivna ili negativna) u tom slučaju sa zakašnjenjem to znači da je proces učenja prilično spor. Zadatak algoritma učenja je shvatiti način odabira akcije koje tijekom vremena donose veće nagrade. Pri tome može koristiti postojeće znanje ili može eksperimentirati s novim, nikad prije ili rijetko korištenim akcijama kako bi dobio znanje o novoj situaciji. Optimizacijski problem u ovom slučaju se može postaviti kao izbor sekvence akcija koje maksimiziraju kumulativnu nagradu. Uobičajeno su brža rješenja poželjnija (u smislu manjeg broja akcija). Ovo učenje nalazi široku primjenu u robotici, autonomnim letjelicama ili vozilima, selekciji marketinške strategije, indeksiranju web stranica, upravljanju raznovrsnim dinamičkim sustavima, računalnim igricama i slično.
Prije opisa područja koje se bavi teorijom učenja nužno je definirati još nekoliko pojmova koji predstavljaju osnovu svakog algoritma strojnog učenja neovisno u kojem području učenja se primjenjivao. Generalizacija nekog modela definirana je kao sposobnost tog modela da točno klasificira nove ulazne podatke koje mu prethodno nisu predočeni. To znači da je moguće definirati generalizacijsku pogrešku hipoteze h kao očekivanu pogrešku na primjere koji nisu dio skupa podataka za učenje. Kako bi bila određena što bolja generalizacija, na neki način je potrebno odrediti kompleksnost klase H iz koje je pojedina h sa stvarnom funkcijom f koja odgovara podacima. Kada je H premalo kompleksna u odnosu na f nastati će pojava neugođenosti (*underfitting*), dok u suprotnom slučaju nastaje problem preugođenosti (*overfitting*). U jednom i drugom slučaju generalizacijska pogreška će biti znatna, ali iz potpuno različitih razloga.

Među brojnim pretpostavkama kojima se može pribjeći jeste izbor modela, a zatim i odgovarajući odabir funkcije cilja i slično.
Iz dosadašnjeg izlaganja moguće je postaviti neka interesantna pitanja, kao što su:

- Koju klasu hipoteza je potrebno izabrati kako bi se izbjegao problem preugođenosti ili neugođenosti?
- Kolika je minimalna veličina skupa podataka za učenje da bi algoritam optimizacije ostvario konvergenciju?

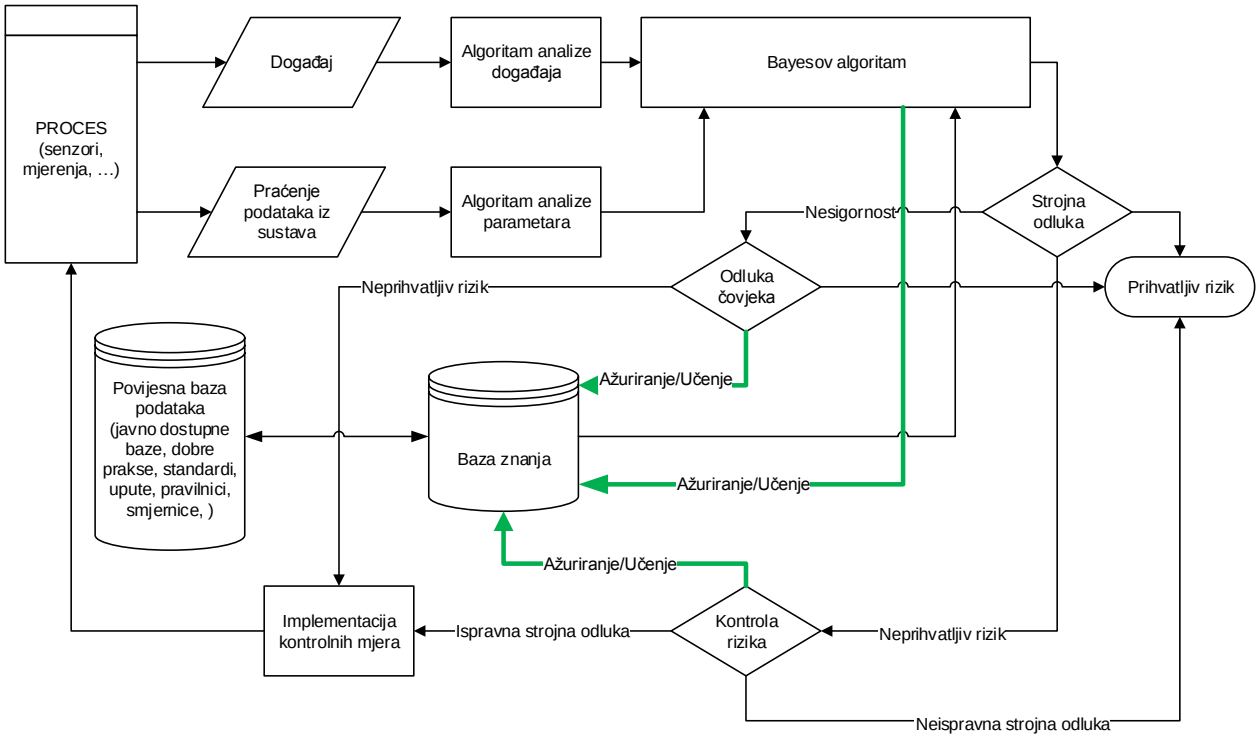
- Po kojim kriterijima izabrati model među dosljednim hipotezama koje nemaju probleme preugođenosti i neugođenosti?
- Kolika je važnost pojedinog atributa ulaznog vektora u procesu učenja U kakvoj su vezi empirijska i generalizacijska greška?

Odgovori na ova i slična pitanja ponuđeni su u eksperimentalnom dijelu rada gdje su prikazani rezultati ispitivanja u kojima su provedena mjerenja i simulacije s ciljem razjašnjenja nepoznanica i dokazivanja tvrdnji. Model predložen u radu će sadržavati najviše osobina nadziranog učenja jer je u procesu potpore odlučivanju vrlo važno imati pod kontrolom veze između ulaznih i izlaznih parametara.

4. MODEL PROCJENE VJEROJATNOSTI NEŽELJENIH DOGAĐAJA U INFORMACIJSKOM SUSTAVU

4.1. Prijedlog modela procjene vjerojatnosti neželjenih događaja

Model procjene vjerojatnosti neželjenih događaja se temelji na povratnim vezama između ulaznih i izlaznih podataka. Povratne veze zajedno s algoritmom izračuna vjerojatnosti događaja na temelju ulaznih mjerenja ili pokazatelja rezultiraju prijedlogom odluke koja može biti konačna ili sugerirana. Uključenost eksperta u procesu procjene vjerojatnosti neželjenih događaja je ključna u cjelokupnom vremenu rada modela, a posebno u početnom periodu učenja. Jedan od ciljeva eksperimenata je pokazati učinke dobivene smanjenjem opsega implementacije modela kako bi se umanjila potreba sudjelovanja eksperata i povećala automatiziranost rada modela.

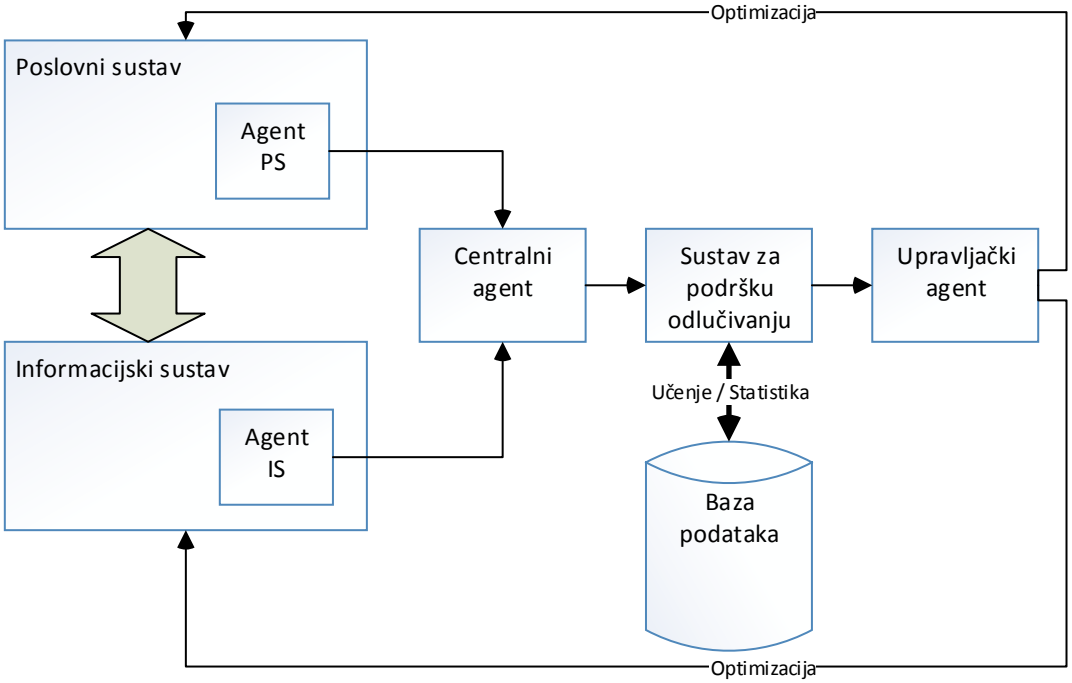


Slika 4-1. Primjer uporabe modela procjene vjerojatnosti neželjenog događaja

Slika 4-1 prikazuje blok dijagram rada modela s uključenim kontrolnim mjerama provjere odlučivanja. Eksperimentalni dio rada u potpunosti prati primjer sa slike, a slučajevi odstupanja su navedeni u opisu testa.

4.2. Agenti u modelu

Model procjene vjerojatnosti neželjenih događaja je adaptivan u smislu primjene i korištenja. Eksperimentalni dio rada će prikazati načine upravljanja različitim informacijskim sustavima i u različitim okruženjima. Slika 4-2 prikazuje primjer uporabe modela u informacijskom sustavu koji obuhvaća dijelove poslovnog sustava (ne nužno računalnog sustava). Primjer ovakvog korištenja je implementacija modela u svrhu procjene vjerojatnosti prijevare u poslovnim procesima.



Slika 4-2. Sustav s ugrađenim modelom za procjenu vjerojatnosti neželjenog događaja

Primjer opisan u poglavlju 4.1 u kojemu je agent pratio broj istovremeno prijavljenih korisničkih računa može biti primjenjiv i u preventivi prijevara (*Anti-Fraud*). Zadaća centralnog agenta (u nekim radovima se koristi naziv *Agent Manager*) je obrada i prosljeđivanje informacija. Dodatno,

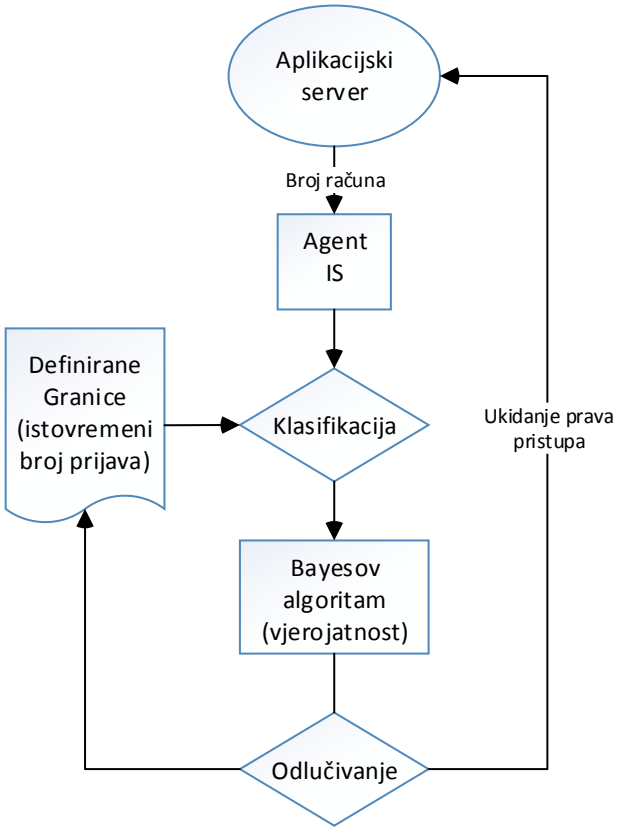
centralni agent može biti postavljen i za zadatak odbacivanja pogrešnih parametara. Eksperimentalni dio rada prikazuje primjer praćenja broja istovremenih korisničkih računa u kojemu je moguće modelirati funkciju ovisnosti parametra o vremenu. Odstupanje vrijednosti u određenim slučajevima može se smatrati pogrešnim podatkom i zahtijevati provjeru ili neku kontrolnu aktivnost. Na ovaj način se izbjegava spremanje vrijednosti parametara ekstremnih vrijednosti ili odstupanja u bazu podataka.

Rad modela je definiran algoritmom koji treba i može biti adaptivan i jednostavan za korištenje.

4.2.1. Zadaća agenta

Agenti predviđeni unutar modela mogu biti različiti sa stajališta izvedbe. Model je predviđen kao matematički i izračuni koje provodi se temelje na teoremu koji ovisi o količini povijesnih podataka pa izvedba agenta ne mora nužno biti napredne prirode. Agenti mogu biti mjerna mjesta, senzori, indikatori, korišteni agenti za indikaciju različitih mrežnih pokazatelja i slično. Komunikacija između agenata i ostatka sustava je ključan čimbenik u radu predloženog modela. Model je koncipiran tako da agenti, odnosno dodijeljeni izvori šalju informacije o vrijednostima parametara u određenom trenutku. Vrijednosti parametara se mogu promatrati kontinuirano ili u kvalitativnim vrijednostima što je razrađeno u eksperimentalnom dijelu rada. Uključivanje poslovnih procesa [69] u opseg mogućih implementacija modela proširuje mogućnosti načina komunikacije. Poznajući principe primjenjivane u metodologiji kontinuiteta poslovanja (BCM) koji osiguravaju neprekidnost i sigurnost procesa, moguće je u model uvesti mehanizme prilagođavanja vrijednosti prihvatljivosti parametara određenom periodu vremena. Eksperimentalni dio rada prikazuje simulaciju u kojoj su promatrane vrijednosti praćenja količine korisničkih računa prijavljenih na aplikacijski poslužitelj. Broj računa se tijekom dana mijenja i vrijednost ne može ovisiti o konstantnoj vrijednosti (*hipotezi*).

Slika 4-3 prikazuje blok dijagram algoritma rada agentskog dijela u modelu u kojem agent prati količinu istovremeno prijavljenih korisničkih računa na aplikacijski poslužitelj.



Slika 4-3. Algoritam rada agenta

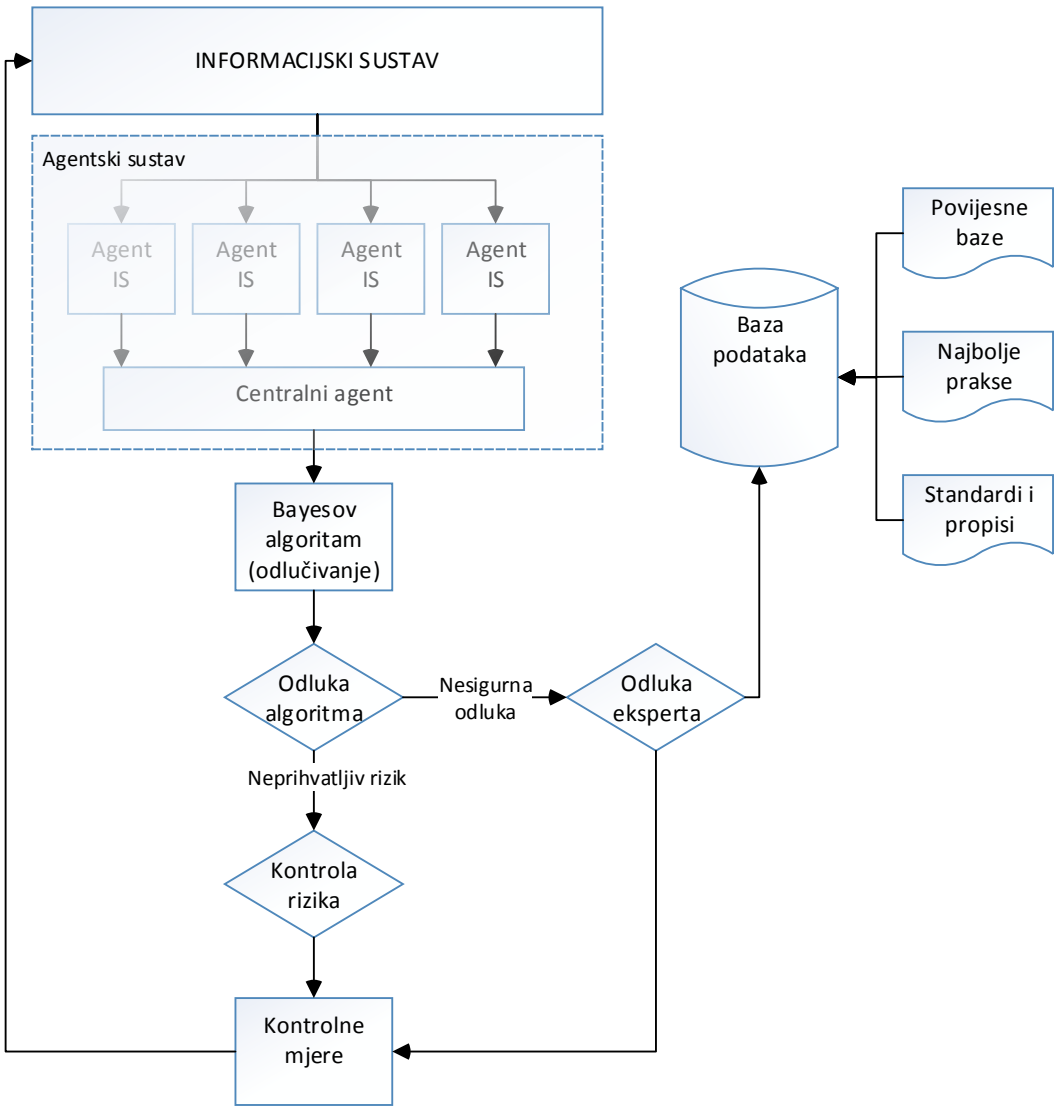
Zadaća agenta iz primjera je praćenje broja korisničkih računa prijavljenih istovremeno na poslužitelj, a svrha modela je upravljanje pristupom. Kontrolna mjera koja može biti implementirana u ovome slučaju je zabrana prava pristupa ili prekidanje trenutnih sjednica za račune koji su u određenom vremenskom periodu prekomjerni.

Način rada agenta prikazanog u ovome radu je sukladan načinima rada agenata korištenih u praksi. Prednost agenata u modelu procjene vjerojatnosti neželjenih događaja je mogućnost implementacije u različita okruženja uz korištenje postojeće infrastrukture. Agentski način rada omogućuje i umetanje preventivnih kontrola koje se pokreću u unaprijed određenim slučajevima. Sve aktivnosti su određene modelom i objektivne su naravi. Subjektivnost se izbjegava korištenjem matematičkog modela koji kao rezultat daje numeričku vrijednost vjerojatnosti. Algoritam sadrži i mogućnost korištenja kontrola poput odluke eksperta u slučajevima nesigurnosti.

4.3. Algoritam procjene vjerojatnosti neželjenog događaja

Algoritam se definira kao postupak ili skup pravila za sustavno rješavanje određene vrste problema ili zadataka. Sastoji se od opisa konačnog skupa koraka. Svaki od njih sadrži jednu ili više aktivnosti, a svaka aktivnost jednu ili više operacija. Algoritmima su u prvo vrijeme nazivana samo pravila računanja s brojevima zapisanim u dekadnom sustavu, da bi kasnije taj naziv postao korišten za pravila obavljanja raznovrsnih zadataka. Algoritmi su jasno definirani postupci za izvršavanje određenog problema, a algoritmi raščlanjeni na uzastopne korake prevode neki skup početnih (ulaznih) vrijednosti u skup završnih (izlaznih) vrijednosti. Početne i završne vrijednosti te eventualni međurezultati pohranjuju se u prikladne baze podataka. Algoritmi se koriste za jasno utvrđivanje pravila dostizanja nekog postavljenog cilja. Uz svaki algoritam moraju biti jasno definirana sva početna stanja objekta na kojima se obavljaju operacije. Algoritam bi trebao biti sastavljen od konačnog broja koraka koji utvrđuju slijed operacija koje je potrebno obaviti nad objektima kako bi se dobila završna stanja ili rezultati.

Slika 4-4 prikazuje blok dijagram algoritma rada modela procjene vjerojatnosti neželjenih događaja koji koristi Bayesov teorem.



Slika 4-4. Algoritam rada modela

Model procjene vjerojatnosti neželjenih događaja je na slici nadograđen kontrolnim mjerama provjere odluke eksperta i provjere predložene mjere zaštite u slučaju primjene modela za preventivne akcije. Primjer uporabe sličnog sustava je sustav za sprječavanje neželjenih upada (IPS, engl. *Intrusion Prevention System*). Eksperimentalni dio rada ne obuhvaća implementaciju preventivnih kontrolnih mjera, ali teorijski je moguće ugraditi određene mehanizme kojima se sprječava mogućnost ostvarenja neželjenih događaja.

4.3.1. Primjeri algoritama

Primjer uporabe modela procjene vjerojatnosti neželjenog događaja (Slika 4-1) opisan je pseudokodom koji predstavlja općeniti način rada modela. Temeljna je odluka eksperta prilikom ugradnje modela u informacijski sustav i ovisi o postojanju određenog događaja ili ne. U slučaju određenog događaja koji se može pratiti kao skup parametara analiza predstavlja provjeru svih definiranih parametara i izračun vjerojatnosti pomoću Bayesovog algoritma. Nakon izračuna provodi se provjera razine vjerojatnosti i provedba kontrolnih mjera. Kontrolne mjere mogu biti preventivne ili dojavne, što ovisi o postojanju i izvedbi agenata.

Neodređeni događaj uvjetuje provjeru definiranih postavki koje predstavljaju definiciju događaja. U slučaju postojanja kriterija za događaj, provodi se ista procedura kao i za određeni događaj. Kontrolne mjere koje mogu postojati u modelu su dodatne kontrole od strane eksperata. Široki pojasevi nesigurnosti kojima se postiže česta potreba za reakcijom eksperta dodatno povećavaju vrijeme učenja.

```
'Analiza događaja

MP=mjerenja u procesu
D=događaj
N=nesigurnost
RM=referentne vrijednosti mjerenja
By=Bayesov algoritam
BP=baza podataka
S=strojna odluka
OE=odluka eksperta
K=kontrola
M=mjera
G=Granica

Analiza neodređenog događaja:
      Ako je MP<>RM tada
      Analiza Di
      By
            Ako je Gi>G tada S=istina
            M ili K
            Ako nije tada N=istina
            OE
            Kraj ako
      Ažuriranje BP
      Kraj Ako

Analiza određenog događaja:
      Za svaki D
      Analiza Di
      By
            Ako je Gi>G tada S=istina
            M ili K
            Ako nije tada N=istina
            OE
            Kraj ako
      Ažuriranje BP
```

Primjer algoritma za analizu poruke pri otkrivanju neželjene pošte naveden je u nastavku:

```
'Analiza događaja (otkrivanje neželjene pošte)

Dim Razmak, Kraj, R
Duljina=2

Preuzmi cijelu poruku
Za j = 1 Do Kraj
str = Cells(j, 1).Value
    Razmak = " "
    R=Izbroji Razmak
    i = 1
    Čini Dok i < R + 2
    Novi red
'samo riječi dulje od 2 znaka!
    If Len(Razmak (i - 1)) > Duljina Tada
    Novi red
    i = i + 1
    Petlja
Sljedeći j
```

Izračun vjerojatnosti neželjenog događaja temelji se na korištenju Bayesovog teorema, a provodi se upotrebom algoritma:

```
'Bayesov algoritam
Pi=podatak
Vi=vjerojatnost
BV=Bayesova vjerojatnost
GP=granica prihvatljivosti
PV=početna vjerojatnost

i=1 Do n

Provjera analiziranih podataka:
    Ako podatak Pi postoji u bazi Tada
    Izračun vjerojatnosti
    Ažuriranje baze
    Ako Ne
    Ažuriranje baze
    Kraj Ako

Izračun vjerojatnosti:
Za svaki Vi
BV=PRODUCT(Vi)/(PRODUCT(Vi)+PRODUCT(1-Vi))

Ažuriranje baze:
    Ako podatak Pi postoji u bazi Tada
        Ako je BV>GP Tada Neželjeni događaj=Istina
        Ako Ne
        Neželjeni događaj=Greška
        Kraj Ako
    Ako Ne
    Pi=PV
    Kraj Ako
```

Sve dodatne mogućnosti modela, uključujući i agente, kontrole i eksperte, naglašene su u radu i njihovo korištenje je moguće uz opisana ograničenja i uvjete.

5. MJERENJA I ANALIZA MODELA

5.1. Uvod u eksperimentalnu analizu modela

Model procjene vjerojatnosti neželjenih događaja ispitan je kroz eksperimente u različitim okruženjima i provedene su evaluacije dobivenih rezultata. Model je ispitan unutar tri različita okruženja informacijskih sustava: filtriranje neželjenih poruka, otkrivanje upada i analizu rizika. Različiti informacijski sustavi odabrani su s ciljem dokazivanja primjenjivosti modela u funkcionalno nejednakim okruženjima. Parametri koji karakteriziraju rad modela su:

- veličina baze podataka i klasificiranih događaja,
- način klasifikacije događaja odnosno izračun početnih vrijednosti vjerojatnosti,
- identifikacija događaja i
- vrsta okruženja.

Namjera je u eksperimentu dokazati i objasniti ponašanje modela u slučajevima nedostupnosti veće količine podataka. Obrađeni su i slučajevi korištenja kvalitativnih i kvantitativnih podataka i njihove obrade za izračun vjerojatnosti.

Početna baza podataka sadrži parametre klasificirane prema događajima u smislu neželjenih i valjanih događaja. Simulacijama su ispitani različiti scenariji u kojima su početne vrijednosti određene na kvalitativan ili na kvantitativan način. Kvalitativan način određivanja razina vjerojatnosti je lakše provediv od traženja kvantitativnih vrijednosti.

Budući da je model utemeljen na događajima koji se klasificiraju i parametrima koji ga opisuju, vrlo je važno analizirati i ovaj aspekt u scenarijima mjerenja. Eksperimenti simuliraju okruženja u kojima su događaji definirani na različite načine. Cilj je utvrditi mogućnosti primjene u sustavima gdje događaj nije jasno određen, npr. primitak elektroničke pošta je jasno određen događaj, a praćenje mrežnog prometa ili stanja spremnika podataka nema jasno utvrđene događaje. U ovim slučajevima pribjegava se statističkim metodama praćenja rada i bilježenju odstupanja.

Posljednji aspekt koji se razmatra u scenarijima mjerenja je vrsta okruženja, odnosno primjena modela u poznatom ili suprotno, u nepoznatom okruženju. Poznato okruženje podrazumijeva poznate događaje i nema novih kombinacija parametara, dok se u nepoznatom okruženju mogu zbivati događaji opisani nekim novim kombinacijama ili čak novim vrijednostima parametara.

Okruženje predstavlja dio informacijskog sustava unutar kojega model radi ili područje poslovanja koje je upravljano modelom. Simulacijama su obuhvaćeni i scenariji implementacije modela u okruženje unutar kojega se prate parametri različitih kategorija (npr. obrada podataka, podaci, sklopovlje) i suprotno tome, okruženje u kojemu su svi praćeni parametri iste kategorije. Razlika u pristupu zadnjeg eksperimenta je i korištenje subjektivnih ocjena rizika. Subjektivno ili kvalitativno dodjeljivanje razina rizika pojedinim kombinacijama prijetnji i ranjivosti uklanja kvalitativni matematički aspekt u kojemu se pojavljuje problem definiranja granice za odlučivanje [44]. Točno definirane granice su u procesu odlučivanja stvarale konfuziju prilikom pojave događaja čija je vjerojatnost blizu ili na samoj granici. Kako bi se uklonile konfuzne situacije, uvedena je kategorija „Nesigurni događaj“ koja označava događaje na rubu odluke. Za ovakve događaje je potrebna dodatna analiza eksperta i naknadna klasifikacija. Tablica 5-1 prikazuje postojanje nesigurnosti u odlučivanju tijekom provedenih simulacija. Parametrizacijom modela tijekom perioda učenja moguće je povećati opseg nesigurnosti i time uključiti eksperte kao podršku za učenje modela. Broj parametara u bazi predstavlja broj dostupnih hipoteza čije su vjerojatnosti izračunate pomoću Bayesovog teorema i mijenjaju se s vremenom u kojemu se analiziraju novi događaji.

Tablica 5-1. Konfiguracija simulacije

Pregled:	**Broj događaja**	**%**
Nepovoljnih događaja	450	14,64%
Povoljnih događaja	2624	85,36%
Broj parametara u bazi	80	
Broj prijetnji	0	
Broj ranjivosti	0	
Nesigurnih događaja	**87**	2,83%

Korištenje dodatnih funkcionalnosti u modelu prikazuje modularnosti i mogućnost adaptacije u različita okruženja rada. Na kraju je ispitan scenarij ostvaren pomoću osobina s najboljim rezultatima. Evaluacija svih simulacija ocjenjuje valjanost modela u različitim okruženjima.

Okruženja u kojima je ispitan rad modela za izračun vjerojatnosti neželjenih događaja su:

- filtriranje neželjenih elektroničkih poruka (SPAM),
- otkrivanje neovlaštenih upada (IDS),
- praćenje rada informacijskog sustava (temeljen na analizi rizika).

Cilj svake provedene simulacije je valjana odluka dobivena od modela. Dobivenu odluku je nakon klasifikacije algoritma potrebno usporediti s rezultatima nekog modela korištenog u praksi. Filtriranje neželjenih poruka je uspoređeno s rezultatima Google spam filter rješenja što predstavlja adekvatan model korišten u praksi i čiji su rezultati dovoljno dobra referenca za usporedbu. Za ispitivanje je korištena baza elektroničke pošte i u njoj unaprijed klasificirane poruke. Rezultati simulacije otkrivanja neželjenih upada su uspoređeni s radom Snort programskog sustava. Sustav (aplikacija) Snort služi za otkrivanje neželjenih upada u informacijski sustav. Nadzor informacijskog sustava pomoću praćenja parametara temeljenih na procjeni rizika je uspoređen s mišljenjem eksperata iz područja informacijske tehnologije.

Konačni rezultat modela je odluka i kao takva je jedan od najvažnijih parametara u upravljanju informacijskim sustavima.

5.2. Podrška odlučivanju

Tehnologije pohrane podataka i velika rasprostranjenost Interneta, omogućila je pojedincima i organizacijama pristup velikom broju podataka. Ti su podaci često u raznovrsnog podrijetla i razlikuju se sadržajem i značenjem. Neki od tih podataka su komercijalne, financijske i administrativne transakcije, poruke elektroničke pošte, tekstovi, zapisi, mjerenja, rezultati testova, itd. Dostupnost tih podataka otvara razne mogućnosti, i postavlja pitanje: „*Je li moguće pretvoriti te podatke u informacije i znanja koji bi se mogli koristiti kao podrška za donošenje odluka pri upravljanju informacijskim sustavima*? [45][46]

Sustav za podršku odlučivanju može se definirati kao skup matematičkih modela i analiza koje koriste raspoložive podatke, te od njih stvaraju informacije i znanja koja su korisna u procesu donošenja odluka. U složenim organizacijama odluke se donose na dnevnoj bazi. Te odluke mogu biti više ili manje važne, mogu imati dugotrajan ili kratkoročan učinak, i mogu uključivati ljude na raznim hijerarhijskim razinama. Sposobnost za donošenje odluka, bilo pojedinca ili zajednice, je jedan od temeljnih čimbenika koji utječu na učinkovitost i konkurentnost organizacije.

Većina odluka se donosi korištenjem jednostavne i intuitivne metode, koja uzimaj u obzir specifične elemente kao što su iskustvo, znanje i dostupne informacije. Takav pristup dovodi do stagnacije načina donošenja odluka, koji je neprikladan za nestabilne uvjete nametnute učestalim i brzim gospodarskim promjenama. U današnjim organizacijama, procesi odlučivanja su često

presloženi i dinamični kako bi se radilo na intuitivan način. Umjesto toga zahtijevaju stroži pristup temeljen na analitičkim metodama i matematičkim modelima.
Glavna uloga sustava za podršku odlučivanju je pružanje alata i metoda koje omogućuju donošenje učinkovitih i pravodobnih odluka.
Primjena strogih analitičkih metoda omogućuje donositeljima odluka da se oslanjaju na informacije i znanja koja su pouzdanija. Rezultat toga je donošenje boljih odluka i planova djelovanja koji omogućuju učinkovitije postizanje ciljeva. Međutim, analitičke metode zahtijevaju eksplicitan opis kriterija za procjenu alternativa i mehanizama koji reguliraju problem. Nužan je temeljni pregled i razumijevanje temeljne logike procesa donošenja odluka.

Danas tvrtke posluju u gospodarskom okruženju koje karakterizira rast razine konkurencije i visoka dinamičnost. Zato je sposobnost brze reakcije na aktivnosti konkurencije i na nove uvjete tržišta kritični čimbenik za uspjeh ili čak opstanak tvrtke. Kada se donositelji odluka suočavaju s problemima postavljaju si niz pitanja i razvijaju odgovarajuće analize. Nekoliko opcija se ispituje i uspoređuje, te se s obzirom na uvjete koji su uzeti u obzir, odabire najbolja. Ako se donositelji odluka mogu osloniti na sustav za podršku odlučivanju, mogu se očekivati velika poboljšanja cjelokupne kvalitete procesa donošenja odluka.
Pomoću matematičkih modela i algoritama, moguće je analizirati veći broj alternativnih akcija, dolazi se do boljih zaključaka, te učinkovitijih i pravodobnih odluka. Stoga je moguće zaključiti da je glavna prednost koja proizlazi iz usvajanja sustava za podršku odlučivanju povećanje učinkovitosti procesa donošenja odluka.

5.3. Podaci, informacije, znanje

U informacijskim sustavima, javnih i privatnih organizacija, nakupljaju se velika količina podataka. Ti podaci potječu dijelom od internih transakcija administrativne, logističke i komercijalne naravi, te dijelom od vanjskih izvora. Međutim, čak i ako su prikupljeni i pohranjeni na sustavan način, ne mogu se izravno koristiti za donošenje odluka. Podaci trebaju biti obrađeni odgovarajućim alatima za ekstrakciju i analitičkim metodama, sposobnim transformirati ih u informacije i znanja, koja bi se mogla koristiti za donošenje odluka. U nastavku je prikazana razlika između podataka, informacija i znanja.

Podaci uglavnom predstavljaju kodifikaciju primarnog entiteta, kao i transakcije koje uključuju dva ili više primarnih entiteta. Primjerice, za trgovca primami entiteti mogu biti kupci, prodajna mjesta i roba koja se prodaje, dok račun predstavlja komercijalnu transakciju.
Informacije su rezultat izvoza i obrade podataka i imaju značenje onome kome su potrebne i tko ih obrađuje. Primjerice, voditelju organizacijske jedinice informacijske i komunikacijske tehnologije informacija o vremenu zastoja nekog sustava predstavlja značajnu informaciju koja može biti izvađena iz sirovih podataka koji su dobavljivi iz različitih izvora.
Informacija se pretvara u znanje kada se koristi za donošenje odluka i planiranje odgovarajućih akcija. Znanjem se smatra skup informacija iz nekog područja, potpomognutih iskustvom i kompetencijom donositelja odluka u rješavanju složenih problema. Analiza zastoja informacijskog sustava može otkriti da je određeni dio sustava dotrajao ili je potrebno planirati implementaciju neke kontrolne mjere. S vremenom će znanje prikupljeno na ovaj način dovesti do akcije koja će biti usmjerena na rješavanje problema, primjerice uvođenje zalihosti (redundancije) nekog dijela sustava. Znanje može biti prikupljeno iz podataka na pasivan način, analitičkim kriterijima ili aktivnom primjenom matematičkih modela, u obliku induktivnog učenja ili optimizacije.

Postoje različiti primjeri u praksi gdje su razvijeni formalni i sustavni mehanizmi prikupljanja, obrade i korištenja znanja. Mehanizmi prikupljanja sada se smatraju neprocjenjivom nematerijalnom imovinom pa čak i zasebnim dijelovima informacijskih sustava. Aktivnosti pružanja podrške u širenju znanja, kroz organizaciju, integracijom procesa donošenja odluka i usvajanjem informacijskih tehnologija obično se nazivaju upravljanje znanjem.
Očito je da sustav za podršku odlučivanju i upravljanje znanjem dijele neke sličnosti u svojim ciljevima. Glavni cilj obiju disciplina je razviti okruženje koje podupire donositelje odluka u procesu donošenja odluka i aktivnostima rješavanja složenih problema. Da bi se primijetila razlika između ove dvije discipline, potrebno je znati da se metode upravljanja znanjem primamo orijentiraju na obradu informacija koje su obično nestrukturirane, a ponekad implicitne i uglavnom se nalaze u dokumentima, zapisima i iskustvima. Sustav za podršku odlučivanju se temelji na strukturiranim informacijama, najčešće je kvantitativne prirode i obično je organiziran u baze podataka.

Tablica 5-2. Primjer baze podataka korištene u eksperimentu

Naziv parametra	**Broj pojava parametra u nepovoljnim događajima**	**Broj pojava parametra u povoljnim događajima**	**Vjerojatnost nepovoljnih događaja**	**Nesigurnost (0,85 – 0,9)**
Popunjenost mrežnog diska prosječna	70	389	51,20%	19
Popunjenost mrežnog diska iznad 50%	71	434	48,82%	30
Popunjenost mrežnog diska iznad 75%	84	385	55,99%	30
Popunjenost mrežnog diska iznad 90%	**124**	**333**	**68,47%**	**29**
Iskorištenost pojasne brzine prosječna	81	378	55,55%	13
Iskorištenost pojasne brzine iznad 50% zakupljene	60	390	47,29%	14
Iskorištenost pojasne brzine iznad 75% zakupljene	97	384	59,56%	23
Iskorištenost pojasne brzine iznad 90% zakupljene	123	352	67,08%	22
Pojasna brzina iskorištena prosječno	63	415	46,96%	24
Pojasna brzina iskorištena 25% više od prosjeka	36	453	31,67%	13
Pojasna brzina iskorištena 50% više od prosjeka	56	400	44,94%	12
Pojasna brzina iskorištena 75% više od prosjeka	96	391	58,88%	17
Pojasna brzina iskorištena 90% više od prosjeka	91	371	58,85%	23
Mrežni promet prosječan	38	422	34,43%	12
Mrežni promet 25% veći od prosjeka	51	445	40,06%	16
Mrežni promet 50% veći od prosjeka	35	414	33,02%	11
Mrežni promet 75% veći od prosjeka	83	383	55,82%	18
Mrežni promet 90% veći od prosjeka	124	345	67,70%	15

Tablica 5-2 je izvoz baze podataka korištene u eksperimentu opisanom u nastavku rada. Popunjenost mrežnog diska iznad 90% je parametar čija vrijednost 68,47% označava vjerojatnost da je događaj koji sadrži istoimeni parametar nepovoljan. Isti parametar se pojavio 124 puta u nepovoljnim, a 333 puta u povoljnim događajima.

5.4. Usporedba metoda klasifikacije

Vrlo je važno spomenuti neke osobine koje obilježavaju klasifikatore i od kojih ovisi odabir metode klasifikacije pa time i načina odlučivanja. Potpora odlučivanju se temelji na izboru klasifikatora čiji način rada je opisan parametrima od kojih su najvažniji [47]:

- Točnost klasifikacije prikazuje se postotkom točno klasificiranih instanci, iako se mogu dogoditi neke greške i stoga je vrlo važno kontrolirati pogreške
- Brzina klasifikatora u nekim slučajevima može biti izuzetno važna. Klasifikator točnosti 90% može biti bolji izbor od klasifikatora koji postiže točnost od 95% ako je puno brži. U

okruženju koje se izrazito brzo mijenja, vrlo je važna mogućnost brzog učenja klasifikacijskih pravila.

Prethodna istraživanja su pokazala je da priprema podataka (koja uključuje korake čišćenja podataka i redukcije broja atributa) usko grlo cjelokupnog procesa otkrivanja znanja u podacima [48]. Zbog toga se priprema podataka smatra najvažnijim korakom u procesu otkrivanja znanja u podacima te je selekcija atributa u fokusu interesa ovog rada jer dobra selekcija atributa može znatno ubrzati cjelokupni proces klasifikacije.

5.4.1. Evaluacija rezultata

Kao kriteriji evaluacije u ovom istraživanju koristit će se točnost klasifikacije i brzina provođenja selekcije atributa. Točnost klasifikacije odnosi se na sposobnost modela za ispravnim određivanjem pripadnosti klasi novih podataka [49]. Za mjerenje točnosti koristit će se matrica konfuzije (Tablica 5-3). Matrica konfuzije je koristan alat za analiziranje koliko se rezultati dobiveni razvrstavanjem uzoraka razlikuju od stvarnih vrijednosti [49]. Matrica konfuzije za dvije klase prikazana je u tablici u nastavku. Ako postoji *m* klasa, matrica konfuzije je tablica veličine najmanje *m***m*. Klasifikator daje dobru točnost ako je većina uzoraka na dijagonali, a vrijednosti izvan dijagonale blizu nula (0).

Tablica 5-3. Matrica konfuzije

Konfuzijska matrica		**Pretpostavljena klasifikacija**	
		Negativno	Pozitivno
Stvarna klasifikacija	Negativno	TN	FP
	Pozitivno	FN	TP

Matrica se sastoji od sljedećih vrijednosti:

- TN – broj ispravno predviđenih negativnih ishoda
- FP – broj pogrešno predviđenih pozitivnih ishoda
- FN – broj pogrešno predviđenih negativnih ishoda
- TP – broj ispravno predviđenih pozitivnih ishoda

Mjere koje se koriste kod matrice konfuzije su sljedeće [49]:

- **Točnost** (eng. *accuracy*) je omjer uzoraka kojima je razred točno predviđen i ukupnog broja uzoraka. Računa se prema sljedećoj formuli:

$$\frac{TN + TP}{TN + FP + FN + TP} \quad (23)$$

- **Opoziv** (engl. *recall*) ili mjera točno predviđenih pozitivnih uzoraka, (engl. *true positive rate*). Mjera se naziva a osjetljivost:

$$\frac{TP}{FN + TP} \quad (24)$$

- **Pogrešno predviđeni pozitivni uzorci**, (engl. *false positive rate*) je omjer uzoraka koji su pogrešno svrstani u pozitivan razred i ukupnog broja negativnih uzoraka:

$$\frac{FP}{TN + FP} \quad (25)$$

- **Točno predviđeni negativni uzorci**, (engl. *true negative rate*) ili specifičnost:

$$\frac{TN}{TN + FP} \quad (26)$$

- **Pogrešno predviđeni negativni uzorci**, (engl. *false negative rate*) je omjer uzoraka koji su pogrešno svrstani u negativan razred i ukupnog broja pozitivnih uzoraka:

$$\frac{FN}{FN + TP} \quad (27)$$

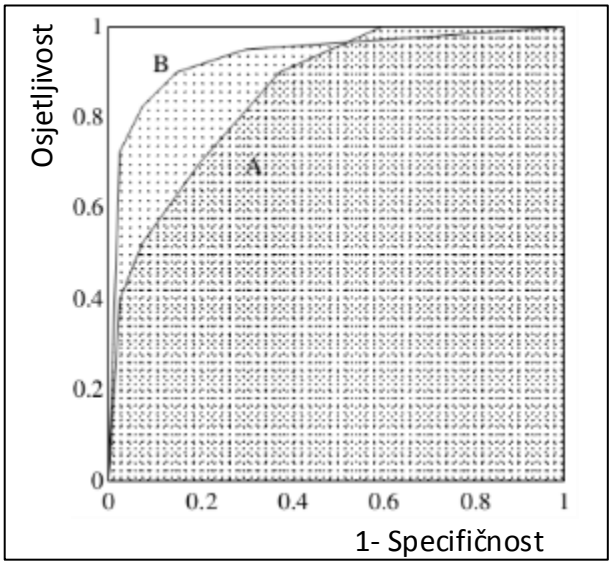
- **Preciznost** (engl. *precision*) je omjer točno predviđenih pozitivnih uzoraka i ukupnog broja uzoraka za koje je predviđen pozitivan razred:

$$\frac{TP}{FP + TP} \quad (28)$$

5.4.2. ROC analiza

Može se vidjeti da je valjanost testa složeni pokazatelj. Sastoji se od više komponenti, ali moguće je odvojiti dva pokazatelja čije su vrijednosti najvažnije u smislu posljedica neispravnih odluka: osjetljivost i specifičnost. Trebaju se, dakle, promatrati zajedno. S druge strane, kod kvantitativnih testova granica koja odvaja „test-pozitivne“ od „test-negativnih“ arbitrarno se određuje. Moguće je odrediti tu granicu na različitim razinama i tako definirati testove različite osjetljivosti i specifičnosti. Dakako, to vrijedi i za testove čije su vrijednosti kvalitativne (ukoliko ima više takvih vrijednosti).

Testiranje klasifikatora temelji se na određivanju *ROC* (engl. *Receiver Operating Characteristic*) krivulje. *ROC* krivulja je dijagram (Slika 5-1) koji grafički prikazuje kvalitetu klasifikatora u ovisnosti od parametra za odlučivanje. Originalno, *ROC* analiza je razvijena tijekom II svjetskog rata s ciljem otkrivanja neprijateljskih aviona pomoću radara, a kasnije je primijenjena i u drugim područjima, u psihologiji, medicini, biologiji, ekonomiji, prepoznavanju oblika [50], itd.



Slika 5-1. Primjer ROC krivulje

Kao ocjena kvalitete dva klasifikatora koristi se površina ispod *ROC* krivulje (*AUC* – engl. *Area under an ROC Curve*), i smatra se kako je klasifikator bolji ukoliko je *AUC* vrijednost veća. Za određeni skup (engl. *False Positive rate – FPR, True Positive rate – TPR*) vrijednosti, klasifikator s manjom *AUC* vrijednošću ima bolje osobine, npr. na slici klasifikator A za $FPR > 0.6$ daje i veću vrijednost *TPR*. Ipak, u praksi *AUC* vrijednost daje vrlo dobru ocjenu kvalitete klasifikatora [50][51], jer klasifikator s većom *AUC* površinom sadrži točku koja je najbliža koordinatama (*0,1*).

U ovome radu ROC krivuljom su uspoređeni rezultati svih eksperimenata i dodatnog scenarija s najboljim rezultatima osmišljenog s ciljem validacije i dokazivanja valjanosti metode procjene vjerojatnosti neželjenih događaja.

5.5. Primjena Bayesovog teorema u modelu procjene vjerojatnosti neželjenih događaja

Bayesovo učenje daje probabilistički pristup zaključivanju i odlučivanju. Nastavno [52], ono se temelji na pretpostavci da je pripadnost (teksta ili promatranog parametra) određena distribucijom vjerojatnosti (riječi ili praćenih varijabli) i da se optimalna klasifikacija može odrediti uzimanjem u obzir distribucije vjerojatnosti dijelova od kojih se sastoji klasificirana instanca i zatim svrstavanjem u toj distribuciji najsličniju kategoriju. Bayesovo učenje je vrlo važan dio područja strojnog učenja i to zbog kvantitativnog pristupa u vrednovanju različitih hipoteza. Isto tako, ovo učenje stvara osnovu za algoritme koji direktno kalkuliraju s vjerojatnostima, a mogu poslužiti i kao temelj za analizu rada drugih algoritama koji ne kalkuliraju izravno s vjerojatnostima nego koriste neke druge modele [70].

5.5.1. Najvažnija svojstva Bayesovog učenja

Gotovo svaka znanstvena metoda ima svoje prednosti i mane. Prednosti i mane će biti prikazane u eksperimentalnom dijelu rada, a u zaključku još jednom navedene s objektivnim dokazima. Prednosti Bayesovog učenja [52] su:

- Svaki naučeni primjer dodatno povećava ili smanjuje vjerojatnost točnosti neke od hipoteza. To pruža znatnu dozu fleksibilnosti u odnosu na algoritme koji potpuno eliminiraju hipoteze iz prostora hipoteza ako nisu konzistentne sa čak i samo jednim primjerom za učenje.
- Apriori znanje se može ugraditi u proces učenja na način da se prije početka procesa učenja to znanje modelira zadavanjem različitih a priori vjerojatnosti hipotezama. Dakle, konačno znanje se sastoji od apriori znanja na koje je učenjem dodana distribucija vjerojatnosti primjera za učenje.

- Bayesove metode učenja mogu baratati hipotezama koje imaju ishode ponderirane vjerojatnostima (npr. neko područje ima definirani rizika od 30% šansi za poplavu uzrokovanu podzemnim vodama i na temelju statistike moguće je odrediti vjerojatnost budućih katastrofa).
- Klasifikacija se može vršiti kombiniranjem više hipoteza koje su težinski određene svojim vjerojatnostima.
- U slučajevima gdje su Bayesove metode učenja računski prezahtjevne ipak mogu poslužiti kao teoretski najoptimalniji način odlučivanja s kojim se onda druge, praktično izvedive metode mogu uspoređivati.

Nedostaci Bayesovog učenja [52] su praktične prirode:

- Potrebno je poznavanje apriori vjerojatnosti za svaku od hipoteza prije početka procesa učenja. To može predstavljati problem jer je u većini primjena broj hipoteza značajan. Ukoliko nisu poznate apriori vjerojatnosti, one se mogu ili procijeniti na temelju prethodnog znanja o problemu, dostupnih podataka ili se mogu pretpostaviti. Za slučaj potpunog nedostatka informacija mogu se svim hipotezama dodijeliti jednake vjerojatnosti.
- U općem slučaju je za određivanje optimalne hipoteze potrebna značajna količina računalnog vremena – potrebno vrijeme raste linearno s povećanjem broja hipoteza. Ipak, u posebnim slučajevima je raznim postupcima moguće potrebnu količinu računalnog vremena smanjiti.

Eksperimentima provedenim i opisanim u ovome radu potvrditi će se navedene prednosti i nedostaci.

5.5.2. Primjer upotrebe Bayesovog teorema

Kao primjer uporabe Bayesovog teorema može poslužiti problem koji je čest u projektima izgradnje sistem soba gdje postoje dvije međusobno isključive hipoteze:

1. Sistem **soba će** biti ugrožena poplavama,
2. Sistem **soba neće** biti ugrožena poplavama.

Podaci geoloških istraživanja mogu biti pozitivni i negativni (pozitivan nalaz znači da je područje ugroženo poplavama ili podzemnim vodama, a negativan da nema velike opasnosti od niti jednog).

Također postoji podatak da na cijelom području samo 0,8% sličnih objekata ima problema (dakle statistička apriori vjerojatnost ostvarenja poplave jest 0,008). Također, geološka su podložna pogreškama. Skupa istraživanja daju pozitivan rezultat u 98% slučajeva i tada je područje stvarno ugroženo i postoje objektivni dokazi ta to, a negativan i točan u 97% slučajeva kada opasnosti nema. Greške prilikom istraživanja daju suprotan rezultat (područje je ugroženo, a istraživanje daje krive rezultate i tada je rezultat negativan, a ako područje nije ugroženo, a istraživanje griješi, tada je rezultat pozitivan). Dosad navedeni podaci se mogu izraziti pomoću vjerojatnosti na sljedeći način:

$$P(poplavno\ područje) = 0{,}008$$
$$P(\neg poplavno\ područje) = 0{,}992$$
$$P(pozitivni\ nalaz|\ poplavno\ područje) = 0{,}98$$
$$P(negativni\ nalaz|\ poplavno\ područje) = 0{,}02$$
$$P(pozitivni\ nalaz|\ \neg poplavno\ područje) = 0{,}03$$
$$P(negativni\ nalaz|\ \neg poplavno\ područje) = 0{,}97$$

Tvrtka je platila istraživanje i rezultati su pozitivni. Sada slijedi izračun donošenja odluke s obzirom na raspoloživo znanje. Korištenjem formule Bayesovog teorema za nalaženje MAP hipoteze slijedi:

$$P(pozitivni\ nalaz|\ poplavno\ područje)P(poplavno\ područje) = 0{,}98 * 0{,}008 = 0{,}0078$$

$$P(negativni\ nalaz|\ \neg poplavno\ područje)P(\neg poplavno\ područje) = 0{,}03 * 0{,}992 = 0{,}0298$$

Iz rezultata je vidljivo da MAP hipoteza za ovaj slučaj upućuje na zaključak da područje nije poplavno, jer je aposteriori vjerojatnost veća. S obzirom da je za izračun korištena pojednostavljena verzija Bayesovog teorema, a hipoteze jesu međusobno isključive, moguće je normalizirati rezultate tako da njihov zbroj bude jednak jedan (1):

$$P(poplavno\ područje|pozitivni\ nalaz) = \frac{0{,}0078}{0{,}0078 + 0{,}0298} = 0{,}21$$

$$P(\neg poplavno\ područje|negativni\ nalaz) = \frac{0{,}0298}{0{,}0078 + 0{,}0298} = 0{,}79$$

Primjer ilustrira kako Bayesovo zaključivanje jako ovisi o apriori vjerojatnostima hipoteza, koje trebaju biti definirane u slučaju direktne primjene Bayesovog teorema. Također je dobro pokazana

dobra strana ove metode – hipoteze se nikad ne eliminiraju iz prostora hipoteza, već samo novim predočenim primjerima postaju više ili manje vjerojatne.

5.5.3. Naivni Bayesov klasifikator – primjer

Rad klasifikatora se može pokazati na primjeru [52] scenarija „*Dan za građevinske radove*“. Radi se o problemu određivanja da li je pojedini dan pogodan za rad vani – moguće klasifikacije su „Da“ i „Ne“. Svaki dan se prikazuje nizom atributa:

„Vrijeme“, „Temperatura“, „Vlažnost“ i „Vjetar“.

Primjeri iz skupa za učenje (Tablica 5-4):

Tablica 5-4. Opis primjera iz skupa za učenje

Dan	**Vrijeme**	**Temperatura**	**Vlažnost**	**Vjetar**	**Dan za građevinske radove**
D1	Sunčano	Vruće	Visoka	Slab	Ne
D2	Sunčano	Vruće	Visoka	Jak	Ne
D3	Oblačno	Vruće	Visoka	Slab	Da
D4	Kišno	Ugodno	Visoka	Slab	Da
D5	Kišno	Hladno	Normalna	Slab	Da
D6	Kišno	Hladno	Normalna	Jak	Ne
D7	Oblačno	Hladno	Normalna	Jak	Da
D8	Sunčano	Ugodno	Visoka	Slab	Ne
D9	Sunčano	Hladno	Normalna	Slab	Da
D10	Kišno	Ugodno	Normalna	Slab	Da
D11	Sunčano	Ugodno	Normalna	Jak	Da
D12	Oblačno	Ugodno	Visoka	Jak	Da
D13	Oblačno	Vruće	Normalna	Slab	Da
D14	Kišno	Ugodno	Visoka	Jak	Ne

Vrijednosti parametara koji obilježavaju događaje su:

- **Vrijeme**: Oblačno, Kišno, Sunčano
- **Temperatura**: Ugodno, Vruće, Hladno
- **Vlažnost**: Visoka, Normalna
- **Vjetar**: Jak, Slab

Pretpostavka je da je Bayesov naivni klasifikator naučio skup primjera za učenje i da mu se sada za klasifikaciju predstavlja novi primjer:

(Vrijeme = sunčano. Temperatura = hladno, Vlažnost = visoka. Vjetar = jak)

Zadatak klasifikatora jest predvidjeti klasifikaciju primjera za naučeni ciljni koncept „*Dan za građevinske radove*“. Jednadžba naivnog Bayesovog klasifikatora za ovaj primjer:

$$v_{NB} = argmax\, p(v_j) \prod_{v_j \in [Da,Ne]} p(a_i|v_j) = argmax\, p(v_j) P(vrijeme = sunčano|\, v_j)$$
$$p(temperatura = hladno|v_j) p(vlažnost = visoka|v_j) p(vjetar = jak|v_j) \quad (29)$$

U drugom je redu varijabla *a* nadomještena s konkretnim vrijednostima. Za izračun je potrebno odrediti 10 različitih vrijednosti (po 4 vjerojatnosti za navedene vrijednosti atributa za svaku kategoriju, plus apriori vjerojatnosti za svaku od kategorija). Prvo se određuju apriori vjerojatnosti po kategorijama:

$$p(dan\ za\ radove = Da) = \frac{9}{14} = 0{,}64$$
$$p(dan\ za\ radove = Ne) = \frac{5}{14} = 0{,}36$$

Na sličan način se računaju i ostale potrebne vrijednosti, npr. za vjetar:

$$p(vjetar = jak|dan\ za\ radove = Da) = \frac{3}{9} = 0{,}33$$
$$p(vjetar = slab|dan\ za\ radove = Ne) = \frac{3}{5} = 0{,}6$$

Nakon što su izračunate sve potrebne vrijednosti, računaju se vjerojatnosti potrebne za klasifikaciju:

$$p(Da)p(sunčano|Da)p(hladno|Da)p(visoka|Da)p(jak|Da) = 0{,}0053$$
$$p(Ne)p(sunčano|Ne)p(hladno|Ne)p(visoka|Ne)p(jak|Ne) = 0{,}0206$$

Na temelju dobivenih vjerojatnosti, Bayesov naivni klasifikator daje odgovor „*Dan za građevinske radove*“ = „*Ne*“. Kao i u primjeru za Bayesov teorem, kategorije u ovom primjeru su neovisne i međusobno isključive, pa se njihove aposteriori vjerojatnosti mogu normalizirati tako da njihov zbroj bude jednak jedan:

$$p(Da|sunčano, hladno, visoka, jak) = \frac{0{,}0053}{0{,}0053 + 0{,}0206} = 0{,}2$$

$$p(Ne|sunčano, hladno, visoka, jak) = \frac{0{,}0206}{0{,}0053 + 0{,}0206} = 0{,}8$$

5.5.4. Procjena vjerojatnosti za naivni Bayesov klasifikator

Do sada su se vjerojatnosti računale kao broj pojavljivanja (vrijednosti atributa ili kategorije) podijeljeno sa ukupnim brojem primjera za učenje. Primjerice, vjerojatnost *p(Vjetar=jak|Dan za radove = ne)* iz prethodnog primjera se računala kao n_c/n gdje je $n = 5$ ukupan broj primjera kod kojih je *Dan za radove = Ne*, a $n_c = 3$ broj primjera (unutar onih 5) za koje vrijedi *Vjetar = jak*. Dok je spomenuti način izračuna u puno slučajeva sasvim zadovoljavajući, ipak daje loše rezultate uz mali broj n_c. Na primjer, scenarij u kojem je vjerojatnost *p(Vjetar=jak|Dan za radove = ne)* jednaka 8%, a u skupu primjera za učenje postoji samo 5 slučajeva za koje vrijedi „*Dan za radove = ne"*. U tom slučaju najvjerojatnija vrijednost n_c jednaka je nuli, što je problem. Prvo, omjer n_c/n daje 0, a to predstavlja pristranu procjenu (podcjenjivanje) vjerojatnosti. Sljedeće, nula se uvrštava u formulu za računanje klasifikacije i to u umnožak, što uzrokuje izračun vrijednosti atributa *Vjetar=jak* koji svakim sljedećim primjerom postaje dominantan i uzrokuje klasifikaciju svakog takvog primjera *Dan za radove = da*.

Da bi se ovakvi problemi izbjegli, potrebno je primijeniti Bayesov pristup procjenjivanju vjerojatnosti korištenjem *m* – procjene vjerojatnosti [52], koja se definira kao:

$$\frac{n_c + mp}{n + m} \qquad (30)$$

Ovdje n_c i n imaju jednako značenje kao i prije, p predstavlja procjenu apriori vjerojatnosti, a m se naziva ekvivalentna veličina uzorka i označava težinski faktor koji određuje važnost apriori vjerojatnosti vrijednosti atributa u odnosu na ukupan skup primjera za učenje. Uobičajen postupak za određivanje p u nedostatku informacije o apriori vjerojatnosti je raspodjela jednakih težina svim postojećim vrijednostima tog atributa. U slučaju da atribut ima k vrijednosti, tada sve vrijednosti tog atributa imaju težinu $p=1/k$. Primjerice, za procjenu *p(Vjetar=jak|Dan za radove = ne)* poznato je da atribut *Vjetar* ima dvije vrijednosti, dakle $p = 0{,}5$. Jasno je da se za $m = 0$ izraz za *m* – procjenu vjerojatnosti svodi na prethodno korišten n_c/n. Ako su i m i p različiti od nule, apriori vjerojatnost se kombinira sa n_c/n regulirano težinskim faktorom m. Razlog zašto se m zove ekvivalentna

veličina uzorka proizlazi iz činjenice da se on može interpretirati kao povećanje postojećih primjera za učenje s dodatnih *m* virtualnih primjera za učenje distribuiranih prema *p* [70].

5.5.5. Treniranje Bayesovih mreža

Posebni algoritmi koriste se za ekstrakciju parametara Bayesovih mreža vjerojatnosti iz podataka za treniranje. Za definiciju svake mreže bitna su dva temeljna parametra:

- Model međusobnih zavisnosti promatranih varijabli prikazan putem usmjerenog grafa
- Uvjetne vjerojatnosti koje kvantificiraju zavisnosti među pojedinim čvorovima Bayesove mreže vjerojatnosti

Ukoliko je poznata struktura mreže (npr. ukoliko ju je definirao ekspert iz domene upravljanja mrežama), te ukoliko su svi atributi za sve moguće instance vidljivi u podacima za treniranje, učenje tablica uvjetnih vjerojatnosti je jednostavno i provodi se istim putem kao i kod naivnog Bayesovog klasifikatora, koristeći frekvencije pojavljivanja atributa u podacima za trening. Ako je topologija mreže poznata, ali nije moguće promatrati sve atribute u podacima za treniranje, tada je situacija složenija i potrebno je koristiti posebne algoritme za slučajeve nedostajućih vrijednosti kao što je procjena maksimizacije (EM, *Estimation Maximization*) algoritam (5.5.6). Ukoliko nisu poznati ni topologija ni tablice uvjetnih vjerojatnosti, primjenjuju se najčešće heuristički algoritmi koji najbolje opisuju razdiobu vjerojatnosti vidljivu iz podataka za treniranje.

5.5.6. Algoritam procjene maksimizacije

Kako je i navedeno u prethodnom dijelu, čest slučaj u praktičnim primjenama je nemogućnost promatranja svih relevantnih atributa instanci. Jedan od načina uz koji je moguće učiti uz nedostatak svih potrebnih atributa je *Estimation Maximization* (EM) algoritam. Algoritam je moguće primijeniti u mnogim slučajevima gdje je potrebno izračunati skup parametara Θ koji opisuju skrivenu razdiobu vjerojatnosti, a kada je moguće promatrati samo dio atributa promatranih instanci.

Neka je skup $X = \{x_1,..,x_m\}$ skup promatranih atributa u m instanci, a skup $Z = \{z_1,..,z_m\}$ skup sakrivenih atributa u istim instancama, tada se skup svih atributa označava s $Y = X \cup Z$. Skup Z je moguće promatrati kao slučajnu varijablu čija razdioba vjerojatnosti ovisi o nepoznatim parametrima Θ i skupu promatranih atributa X. Također Y je slučajna varijabla jer je definirana

preko slučajne varijable *Z*. Ako je *h* trenutna hipoteza *Θ*, a *h′* nova hipoteza nastala nakon iteracije algoritma procjene maksimizacije. Algoritam procjene maksimizacije traži hipotezu *h′* koja će maksimizirati očekivanje *E[lnP(Y | h′)]*. Vrijednost *P(Y | h′)* predstavlja vjerojatnost od *Y* uz određenu hipotezu *h′* i logično je tražiti *h′* takvog iznosa da će se izraz maksimizirati. Prirodni logaritam *ln* se koristi jer se maksimizirajući ln*P(Y | h′)* ujedno maksimizira i izraz pod logaritmom *P(Y | h′)*. Očekivanje *E[lnP(Y | h′)]* je uvedeno jer je *Y* slučajna varijabla. Razdioba vjerojatnosti za slučajnu varijablu *Y* determinirana je poznatim vrijednostima u skupu *X* te sa razdiobom nad skupom *Z*. U većini slučajeva nije poznata razdioba nad *Y* jer je definirana upravo s parametrima *Θ* koje je potrebno izračunati. EM algoritam uzima trenutnu hipotezu *h* umjesto stvarnih parametara *Θ* kako bi procijenio distribuciju nad *Y*. Definirana je funkcija *Q(h′|h)* koja vraća E*[*ln*P(Y | h′)]* kao funkciju od *h′* s pretpostavkom i daje *Θ=h* uz uvjet promatranog podskupa atributa *X*.

$$Q(h'|h) = E[\ln p(Y|h')|h, X] \quad (31)$$

EM algoritam provodi i ponavlja dva koraka do konvergencije:

1. Korak procjene (*Estimation* E): Izračun funkcije *Q(h′| h)* korištenjem trenutne hipoteze *h* i promatranog podskupa atributa *X* kako bi se izračunala razdioba vjerojatnosti nad *Y*:

$$Q(h'|h) \leftarrow E[\ln p(Y|h')|h, X] \quad (32)$$

2. Korak maksimizacije (*Maximization*): Zamjena hipoteze *h* sa hipotezom *h′* koja maksimizira funkciju *Q*.

$$\leftarrow argmax_{h'} Q(h'|h) \quad (33)$$

Ukoliko je funkcija *Q* kontinuirana, EM algoritam će konvergirati u stacionarnu točku vjerojatnosne funkcije *P(Y|h′)*. Ukoliko *P(Y|h′)* ima jedinstven maksimum, EM algoritam će zajamčeno pronaći globalni maksimum. Ukoliko *P(Y|h′)* ima više lokalnih maksimuma EM algoritam će konvergirati u lokalni maksimum koji ne treba biti i globalni.

5.6. Filtriranje neželjenih elektroničkih poruka

Najpoznatiji sustav u kojemu se koristi Bayesov teorem je filtriranje neželjenih elektroničkih poruka. Porastom digitalnog tekstualnog sadržaja s kojim se susrećemo u svakodnevnom radu (Web, poruke elektroničke pošte, društvene mreže) raste i vrijeme i trud koji je potrebno uložiti kako bi se odabrao i klasificirao kvalitetan sadržaj. Bayesove metode često se koriste se kao robusne i u praksi dokazano efikasne metode za rješavanje ovakvih problema.

Jedno od trenutno najaktivnijih područja primjene je klasifikacija poruka elektroničke pošte, sa naglaskom na filtriranje neželjenih poruka (SPAM).

Postoji gruba definicija spam poruke kao neželjene komercijalne poruke elektroničke pošte [68]. Dodatak toj definiciji bi moglo biti da je slanje same poruke automatizirano i da se obavlja u ogromnim količinama. Upravo količina neželjenih poruka predstavlja veliki problem, te nije rijedak slučaj da u svakodnevnom korištenju količina neželjenih poruka elektroničke pošte višestruko nadmašuje koristan sadržaj, što uzrokuje i ogromne financijske gubitke. Proračuni o ukupnom gubitku se mjere u milijardama dolara samo na području SAD-a, te o udvostručivanju količine neželjenih poruka svakih 6 mjeseci potaknuli su intenzivan razvoj metoda i programskih rješenja za detekciju i filtriranje poruka elektroničke pošte.

Prije početka intenzivnog korištenja vjerojatnosnih metoda detekcije neželjenih poruka, većina *anti-spam* alata radila je na principu heurističkih pravila, crne i bijele liste, detekcije uz korištenje karakterističnih fraza unutar poruka elektroničke pošte te praćenja baze poznatih poruka. Ovakve metode davala su zadovoljavajuće rezultate, ali postajale su sve nedostatnije sa sve većom količinom i znanjem zlonamjernih pošiljatelja (*spammera*). Poseban problem kod detekcije navedenim metodama predstavljaju lažni pozitivni rezultati (*False Positive*) koji su višestruko opasniji od lažnih negativnih rezultata (*False Negative*). Lažni pozitivni rezultati su legitimne poruke elektroničke pošte koje bivaju proglašene za neželjene, dok su lažno negativni rezultati SPAM poruke koje su neopaženo prošle kroz mehanizam [68]. U tablici (Tablica 5-5) je prikazana statistika točnosti i pojave lažnih pozitivnih za različite metode detekcije:

Tablica 5-5. Statistika točnosti i pojave lažnih pozitivnih za različite metode detekcije (podaci tvrtke MessageLabs specijalizirane za anti-virus i anti-spam filtriranje e-mail poruka)

	DNS blacklists	**Detekcija fraza**	**Heurističke metode**	**Bayes metode**
Točnost	0 – 60%	80%	95%	99%+
Lažni pozitivni	10%	2%	0.5%	0.1%
Lažni negativi	8%	3%	0.6%	0.2

Kao što se vidi u rezultatima, trenutno najbolje rezultate, kako po točnosti tako i po broju lažnih pozitivnih rezultata daju metode temeljene na vjerojatnosnim tehnikama. Druge metode i alati za klasifikaciju poruka elektroničke pošte često su neprimjenjivi u borbi protiv neželjene pošte. Razlozi su brojni, danas je vrlo jednostavno stvoriti veliku količinu pretinaca i lažnih imena (engl. *aliasa*), fraze je teško detektirati jer su često korišteni pravi izrazi i rječnici, a heurističke metode se također pokazuju sve lošijim izborom.

5.6.1. Klasifikacija poruka neželjene pošte

U ovom poglavlju opisan je način rada klasifikatora neželjenih poruka temeljenog na primjeni naivnog Bayes klasifikatora [53]. Koraci algoritma učenja su:

- Odabir dva skupa poruka elektroničke pošte: legitimne poruke i neželjene poruke.
- Pregledavanje cjelokupnog sadržaje svih poruka elektroničke pošte
- Žeton (*Token*) je tekst koji se sastoji od kombinacije alfanumeričkih znakova, brojeva, apostrofa i specijalnih znakova. Sve ostalo se smatra separatorom između pojedinih žetona.
- Žeton koji su sastavljeni od isključivo numeričkih znakova i žetoni kraći od 2 znaka se ignoriraju.
- Pojavljivanja pojedinog žetona unutar skupova legitimnih i neželjenih poruka elektroničke pošte se broje te se kreiraju dvije tablice, svaka za pojedini skup poruka, u kojima se povezuje pojedini žeton s brojem pojavljivanja.
- Na temelju tablica s brojem pojavljivanja pojedinog žetona u spam i u legitimnim porukama elektroničke pošte gradi se tablica koja povezuje svaki žeton i vjerojatnost da je e-mail poruka u kojoj se ovaj nalazi neželjena.

Žeton kojemu se izračunava vjerojatnost, označena s *OK* i *NOK* u tablicama s brojem pojavljivanja pojedinog žetona u skupovima spam i legitimnih poruka, a *nOK* i *nNOK* su brojevi spam i legitimnih poruka unutar skupova. U tablicu se ubacuju samo oni žetoni koji se pojavljuju unutar oba skupa i to ukupno više od 5 puta. Žetonima koji se pojavljuju samo u jednom skupu poruka dodijeljene su vrijednosti vjerojatnosti 0,1 i 0,99 [68].

Prilikom računanja vjerojatnosti koriste se brojevi poruka unutar svakog skupa umjesto njihove zajedničke duljine, iako se prilikom brojanja pojavljivanja žetona unutar skupova za treniranje

poruke promatraju kao neprekidni tekst. Ovo se pokazalo korisno za dodatno smanjenje broja lažnih pozitivnih klasifikacija.

Nakon ovog postupka dobiva se tablica koja sadrži vjerojatnosti *p(S|X)* za pojedini žeton *X*, tj. vjerojatnosti da je e-mail poruka koja sadrži žeton spam poruka.

Kada se primi nova e-mail poruka, za klasifikaciju se koristi sljedeći algoritam:

- Cjelokupni sadržaj poruke skenira se u žetone
- 15 najvažnijih žetona se izdvaja, pri čemu se važnost pojedinog žetona mjeri tako što se uzimaju žetoni koji najjače određuju da li je poruka legitimna ili spam, tj. oni žetoni čija je vjerojatnost zapisana u tablici najudaljenija od neutralne vjerojatnosti 0,5. Žetoni koji se ne pojavljuju u tablici dobivaju vjerojatnost 0,4.
- Na temelju vjerojatnosti vezanih za pojedine žetone izračunava se kombinirana vjerojatnost da je poruka koja se klasificira upravo neželjena.

Ovakav algoritam računa kombiniranu vjerojatnost po formuli:

$$P(S|X_1, \dots, X_{15}) = \tag{34}$$
$$= \frac{P(S|X_1) * \dots * P(S|X_{15})}{P(S|X_1) * \dots * P(S|X_{15}) + \big(1 - P(S|X_1)\big) * \dots * (1 - P(S|X_{15}))}$$

Opravdanje za ovakvo izračunavanje rezultantne vjerojatnosti moguće je dobiti ukoliko se primijeni ograničenje da su a-priori vjerojatnosti pojavljivanja spam i legitimnih poruka jednake. Tada se može primijeniti sljedeći izvod iz osnovnog Bayesovog teorema. Za slučaj dvije varijable *X* i *Y* izračunava se vjerojatnost da je poruka spam uz evidenciju varijabli *X* i *Y*:

$$P(S|X,Y) = \frac{P(X|S) * P(Y|S) * P(S)}{P(S) * P(X|S) * P(Y|S) + P(\neg S) * P(X|\neg S) * P(Y|\neg S)} \tag{35}$$

Budući da u izrazu korištenom za izračun vjerojatnosti nema izraza *P(X|S)* i *P(Y|S)*, koristi se jednakost:

$$P(X|S) = \frac{P(S|X) * P(X)}{P(S)} \tag{36}$$

te proizlazi:

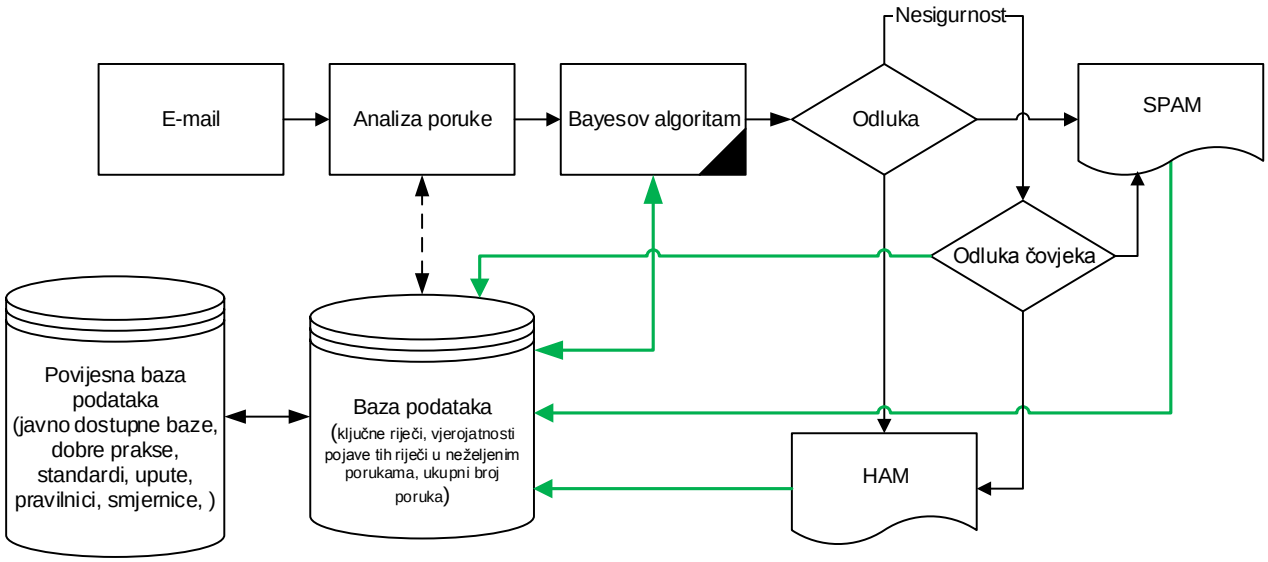
$$P(S|X,Y) = \frac{\frac{P(S|X) * P(S|Y)}{P(S)}}{\frac{P(S|X) * P(S|Y)}{P(S)} + \frac{P(\neg S|X) * P(\neg S|Y)}{P(\neg S)}} \tag{37}$$

Ukoliko se ovdje primijeni pretpostavka da je vjerojatnost ostvarenja ili neostvarenja događaja jednaka *P(S)=P(¬S)=0,5* izrazi se mogu dalje kratiti i dolazi do izraza koji odgovara formuli korištenoj u klasifikacijskom algoritmu:

$$P(S|X,Y) = \frac{P(S|X) * P(S|Y)}{P(S|X) * P(S|Y) + (1 - P(S|X)) * (1 - P(S|Y))} \quad (38)$$

5.6.2. Primjena modela za procjenu vjerojatnosti neželjenog događaja u otkrivanju neželjene elektroničke pošte

Slika 5-2 prikazuje blok dijagram eksperimenta u kojemu je model ispitan za potrebe otkrivanja neželjene pošte. Važno je napomenuti da se Bayesov teorem inače koristi u sličnim sustavima i da je ovaj primjer namjerno odabran kako bi se provela evaluacija rezultata predloženog modela s postojećim referentnim rješenjima.



Slika 5-2. Blok dijagram eksperimenta korištenja modela na otkrivanju neželjenih poruka

Baza elektroničkih poruka koja je analizirana i čijim je podacima popunjena baza znanja za korištenje modela u eksperimentu je pretinac elektroničke pošte otvoren prije 10 do 12 godina i korišten za registracije na različite domene. Elektronička pošta u ovom pretincu je klasificirana (filtrirana) s Google Spam filtrom i broj neželjenih poruka je veći od najvećeg korištenog u eksperimentu (16000). Poruke ispitane modelom su preuzete iz sadržaja drugog (različitog) pretinca elektroničke pošte.

5.6.3. Otkrivanje neželjene pošte uz korištenje baza znanja klasificiranih poruka različite veličine

Otkrivanje neželjene pošte uz korištenje baze znanja od 500 do 8000 klasificiranih poruka

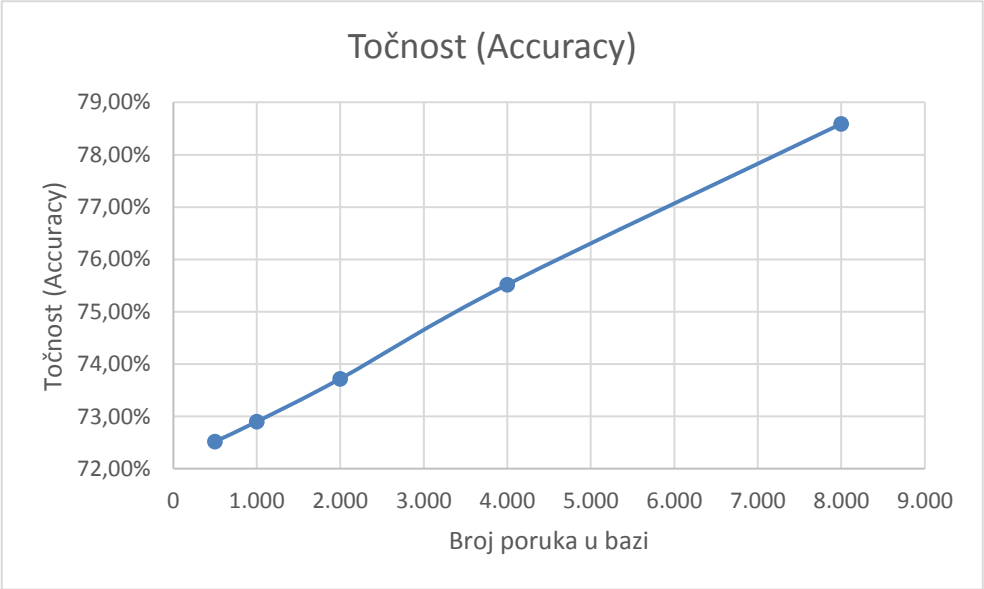
Provedena su dva eksperimenta. U prvom je korišteno najviše 8000 poruka u bazi znanja, a druga baza je sadržavala 16000 klasificiranih poruka.

Tablica 5-6 prikazuje rezultate dobivene ispitivanjem modela za otkrivanje neželjene pošte na temelju baze znanja od najviše 8000 klasificiranih poruka. Poruke su analizirane prema riječima koje sadrže i riječi (žetoni) su svrstani u bazu znanja.

Tablica 5-6. Rezultati dobiveni ispitivanjem modela za otkrivanje neželjene pošte s 500 do 8000 poruka u bazi znanja

Broj poruka u bazi	Točnost (Accuracy)	TP (True Positive Rate)	FP (False Positive Rate)	TN (True Negative Rate)	FN (False Negative Rate)	Preciznost (positive predictive value)
500	72,52%	73,40%	29,44%	70,56%	26,60%	84,71%
1.000	72,90%	73,75%	29,00%	71,00%	26,25%	84,97%
2.000	73,72%	74,45%	27,89%	72,11%	25,55%	85,57%
4.000	75,52%	75,90%	25,33%	74,67%	24,10%	86,94%
8.000	78,59%	78,05%	20,22%	79,78%	21,95%	89,56%

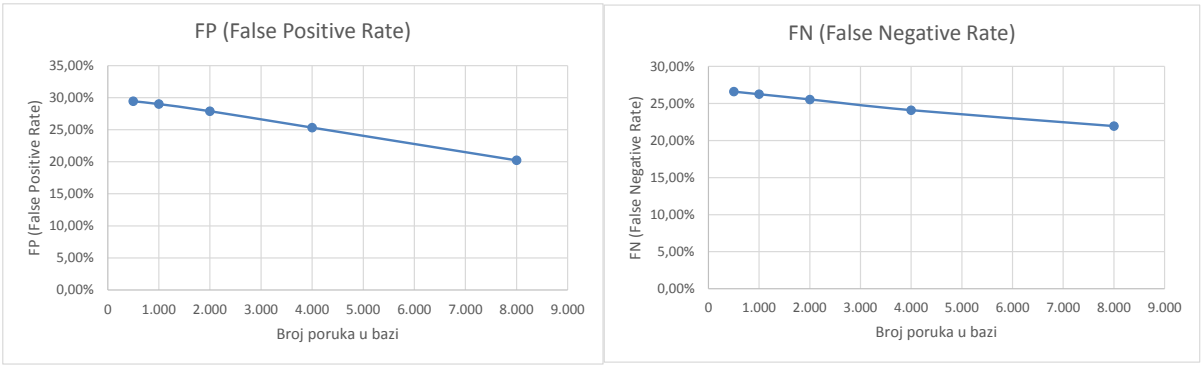
Slika 5-3 prikazuje ovisnost pokazatelja točnosti (*Accuracy*) o količini klasificiranih poruka. Očekivani rezultati su i dobiveni, odnosno pokazano je da se s povećanjem količine klasificiranih informacija povećava i točnost predikcije događaja.



Slika 5-3. Točnost kroz eksperimente otkrivanja neželjene pošte (500-8000 uzoraka)

Najznačajniji pokazatelj uspješnosti metode predviđanja, a što je u ovom slučaju procjena vjerojatnosti nekog događaja su pogrešno predviđeni pozitivni i pogrešno predviđeni negativni uzorci (FPR i FNR). Cilj je minimizirati navedene pokazatelje i time izbjeći pogreške i krive odluke.

Na slikama (Slika 5-4) su prikazani pogrešno predviđeni pozitivni i negativni uzorci u ovisnosti o broju uzoraka u bazi podataka (bazi znanja).



Slika 5-4. Pogrešno predviđeni pozitivni i negativni uzorci (FPR i FNR) kroz eksperimente

Preciznosti (*Positive predictive value*) je u prvom eksperimentu dosegla maksimalnu vrijednost od 89% za slučaj predviđanja s 8000 uzoraka. U nastavku su prikazani rezultati istovrsnih eksperimenata s maksimalnim brojem uzoraka od 16000.

Otkrivanje neželjene pošte uz korištenje baze znanja od 1000 do 16000 klasificiranih poruka

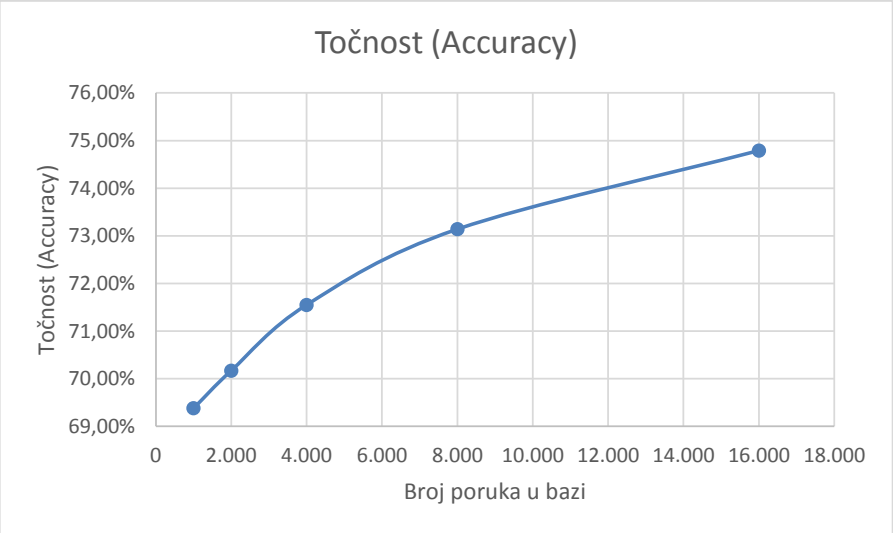
Provedeno je dodatno ispitivanje baze uz korištenje novih slučajno odabranih poruka, ali ovaj puta s dvostruko većom količinom podataka. Dobiveni rezultati ne odstupaju od prethodnih i dvostruko veća količina podataka (16000) rezultira promjenom statističkih pokazatelja (Tablica 5-7). Želja je bila utvrditi trend rasta pokazatelja ispravnosti odlučivanja.

Tablica 5-7. Rezultati dobiveni testiranjem modela za otkrivanje neželjene pošte s 1000 do 16000 poruka u bazi znanja

Broj poruka u bazi	Točnost (Accuracy)	TP (True Positive Rate)	FP (False Positive Rate)	TN (True Negative Rate)	FN (False Negative Rate)	Preciznost (positive predictive value)
1.000	77,14%	78,55%	26,00%	74,00%	21,45%	87,04%
2.000	77,66%	79,05%	25,44%	74,56%	20,95%	87,35%
4.000	78,69%	80,00%	24,22%	75,78%	20,00%	88,01%
8.000	80,90%	81,85%	21,22%	78,78%	18,15%	89,55%
16.000	84,41%	84,60%	16,00%	84,00%	15,40%	92,16%

Točnost izračunata za najveći broj uzoraka je 84% što je proporcionalno i za očekivati u usporedbi s prethodnim eksperimentom i manjim brojem uzoraka (Slika 5-5).

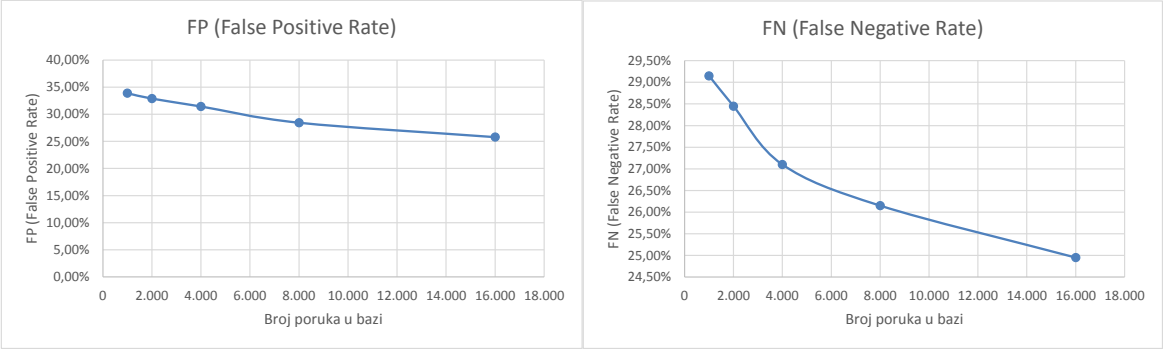
Slika 5-5 prikazuje točnost ovisnu o broju uzoraka, odnosno eksperimentu (na osi apscisa). Točnost se nije znatno popravila korištenjem dvostruko veće količine podataka, ali na slici je vidljiva različita dinamika učenja. Korištenjem veće količine znanja ili bržim stjecanjem znanja se brže dolazi do veće točnosti. Cilj rada je prikazati sve ovisnosti i optimirati model.



Slika 5-5. Točnost kroz eksperimente

Pogrešno predviđeni pozitivni i negativni uzorci su pri maksimalnom broju klasificiranih poruka dosegli vrijednost od 16% i 15%.

Slika 5-6 prikazuje pogrešno predviđene pozitivne i negativne uzorke u ovisnosti o broju klasificiranih poruka u bazi.



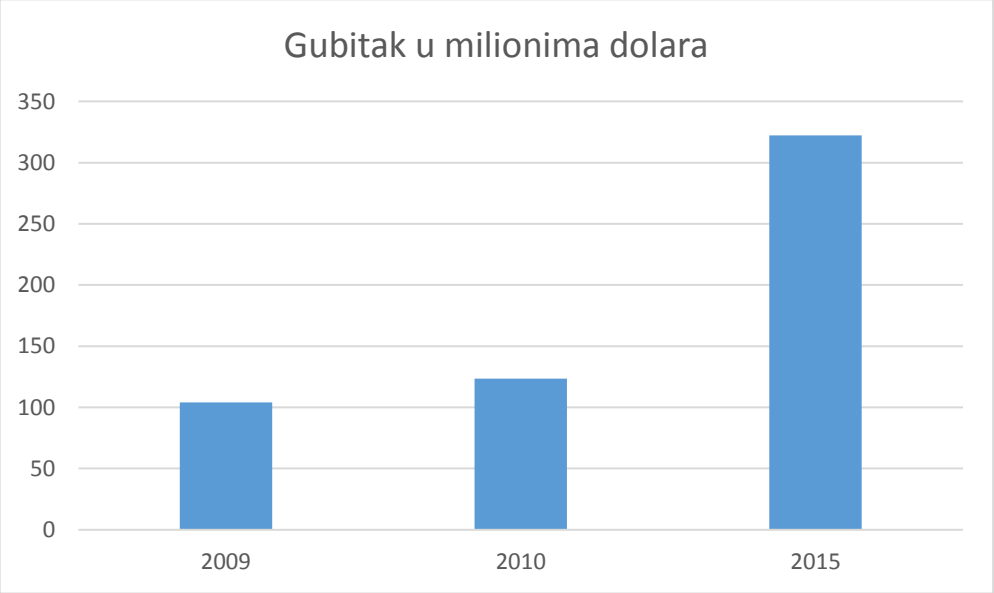
Slika 5-6. Pogrešno predviđeni pozitivni i negativni uzorci (FPR i FNR) u eksperimentu otkrivanja neželjene pošte (1000-16000 uzoraka)

Pokazatelj preciznosti je pri najvećem broju uzoraka dosegao vrijednost od 92%. Eksperimenti procjene vjerojatnosti neželjene pošte su ukazali na povećanje pokazatelja ispravnosti odluke za scenarije s većim brojem klasificiranih podataka u bazi znanja. U nastavku su prikazani i opisani rezultati eksperimenata otkrivanja neželjenih upada u računalnu mrežu. Navedeni scenariji predstavljaju okruženje u kojemu događaj nije egzaktno definiran (kao što je pristigla poruka pošte).

5.7. Otkrivanje neovlaštenih upada

Brzi razvoj Interneta i tehnologija potiče razvoj računalnih virusa i povećanje broja pokušaja upada u sustav te se zbog toga razvija sve više tehnika za računalnu sigurnost. Upadi u sustav su neovlašteni pristupi informacijama uz njihovo korištenje ili mijenjanje. Skoro svakodnevno se otkrivaju nove vrste upada i propusti u sustavima koji se iskorištavaju. Prema podacima iz organizacije CERT (engl. *Computer Emergence Response Team*) u 15 godina broj prijavljenih sigurnosnih aktivnosti porastao je gotovo 1.000 puta [54], a udvostručuje se svake sljedeće godine (Slika 5-7).

Pristup Internetu postaje sve jednostavniji i pristupačniji te je zbog toga teško nadzirati promet pa dolazi do raznih propusta koji se iskorištavaju sa svrhom zlonamjernih upada u sustave [75]. Uvođenje novih tehnologija donosi veliki broj sigurnosnih propusta pa napadači imaju prostora za razvoj alata s kojima će moći neovlašteno ući ili onesposobiti rad ranjivog sustava. To se događa zbog toga što se tehnologije i trendovi jako brzo razvijaju, a proizvođači na tržište puštaju alate koji imaju velike sigurnosne propuste. Jedan od poznatijih primjera je protokol WEP (engl. *Wired Equivalent Protocol*) kojem su nakon samo dvije godine pronađeni veliki sigurnosni propusti te je izrađen veliki broj alata koji su to iskorištavali. Velikim napretkom Interneta, kao i time što je postao dostupan svakome, mnoge tehnologije za narušavanje sigurnosti se mogu pronaći njegovim jednostavnim pretraživanjem (Slika 5-7).



Slika 5-7. Troškovi sigurnosnih incidenata i planiranje za 2015. godinu[2]

Porastom broja korisnika povećao se i mrežni promet te ga je jako teško nadzirati. Jedna od prvih tehnika za zaštitu je vatroštit (eng. *firewall*) koji je sklopovsko ili programsko rješenje i radi na principu filtriranja paketa. Moguće je propuštati određene pakete kroz mrežu ili u potpunosti zabraniti promet. Glavni nedostatak vatroštita je taj što je moguće propuštanje ili zabranjivanje prometa samo ovisno o podacima dostupnim na mrežnom i prijenosnom sloju.

Za bolju zaštitu potrebna je neka nova tehnologija koja će moći analizirati sadržaj paketa na aplikacijskom sloju i na osnovu toga odlučiti može li paket proći dalje (do korisnika) ili će ga sustav za zaštitu odbaciti. Tehnologija je sustav za otkrivanje upada – IDS (engl. *Intrusion*

[2] izvor: http://www.statista.com/statistics/203119/market-development-of-intrusion-detection-services-since-2009

Detection System) [67] koja analizira pakete tako što ih uspoređuje s njihovim potpisima koji se nalaze u bazi podataka ili provjerava određene nepravilnosti [55]. Postoji i novija tehnologija za sprječavanje upada u sustav – IPS, i koristi se za sprečavanje napada na mrežu.

Snort je besplatni alat otvorenog koda koji predstavlja mrežni sustav za otkrivanje upada – NIDS (engl. *Network Intrusion Detection System*), [66]. Jedna od velikih prednosti je ta da se Snort svakim danom nadograđuje, odnosno svakim otkrivanjem novih načina upada u sustav i/ili sigurnosnih propusta on povećava broj (ili korigira postojeća) pravila. Dodatna prednost je mogućnost prilagodbe alata specifičnim potrebama korisnika.

Model predložen u ovome radu se ne nadograđuje planirano iz centralne baze podataka, već ima sposobnost učenja na prethodnim događajima.

5.7.1. Sustavi za otkrivanje i sprječavanje neovlaštenog upada

Sustavi za otkrivanje i sprječavanje upada su nove tehnike za zaštitu od zlonamjernih upada u računalni sustav. IDS nadgleda promet u mreži kako bi mogao otkriti neželjene aktivnosti. Dijeli se na:

- mrežni IDS – NIDS, može analizirati mrežni promet i usporediti s datotekom u kojoj se nalazi baza potpisa napada;
- uređaj u računalnoj mreži (engl. *Host*) s IDS-om – HIDS , njegovi zadaci su analizirati zapise sustava i aplikacija koji se nalaze u datotekama te prepoznati netipične aktivnosti koje bi mogle biti označavati upad;
- distribuirani sustav za otkrivanje upada – DIDS, sastoji se od sustava NIDS, HIDS ili oba.

Glavne funkcije sustava za sprječavanje upada su identificiranje zlonamjernih aktivnosti, zapisivanje informacija o tome i pokušavanje blokiranja tih aktivnosti [67].

Prezentacija sustava za otkrivanje neželjenih upada predviđena je s ciljem upoznavanja načina rada modela čije osobine treba sadržavati model procjene vjerojatnosti neželjenih događaja. Rezultati predloženog modela su uspoređeni s rezultatima IDS sustava radi utvrđivanja sukladnosti i dokazivanja ispravnosti modela.

5.7.2. Sustav za otkrivanje neovlaštenog upada – IDS

Otkrivanje upada je skup tehnika i metoda koje se koriste za otkrivanje sumnjivih aktivnosti na mreži, odnosno otkrivanje neželjenog mrežnog prometa.

Sustav za otkrivanje upada može biti implementiran programski, sklopovski ili kao kombinacija sklopovlja i programa. On nadgleda promet u mreži kako bi mogao otkriti neželjene aktivnosti i događaje kao što su ilegalni, zlonamjerni promet te promet koji narušava sigurnosnu politiku. Mnogi IDS alati zapisuju otkrivanje takvog događaja u bazu podataka kako bi se kasnije mogli pregledati ili kako bi kombinirali ovaj događaj s drugim podacima [67]. Na temelju vlastite izgrađene baze podataka o napadima mogu se donositi odluke o politici sustava ili o provjeri štete. Glavni cilj otkrivanja upada je nadgledati mrežu kako bi se mogle otkriti nepravilnosti u ponašanju i zlouporaba. Ovaj koncept postoji skoro dvadeset godina, ali je tek nedavno doživio dramatičan rast popularnosti i konstruiranja u ukupnoj infrastrukturi informacijske sigurnosti.

Trenutno, statistika tržišta pokazuje da su sustavi IDS među najprodavanijima tehnologijama za sigurnost, a taj bi se trend trebao nastaviti. Nadalje, vlada inicijativama također dodaje poticaj za razvoj takvih sustava. Napredak u sustavima IDS u konačnici će postaviti sigurnosnu tehnologiju u novo poprište automatizirane sigurnosne inteligencije. Sustav za otkrivanje upada dijeli se na dvije osnovne kategorije:

- sustav za otkrivanje upada koji se temelji na potpisu,
- sustav za otkrivanje nepravilnosti.

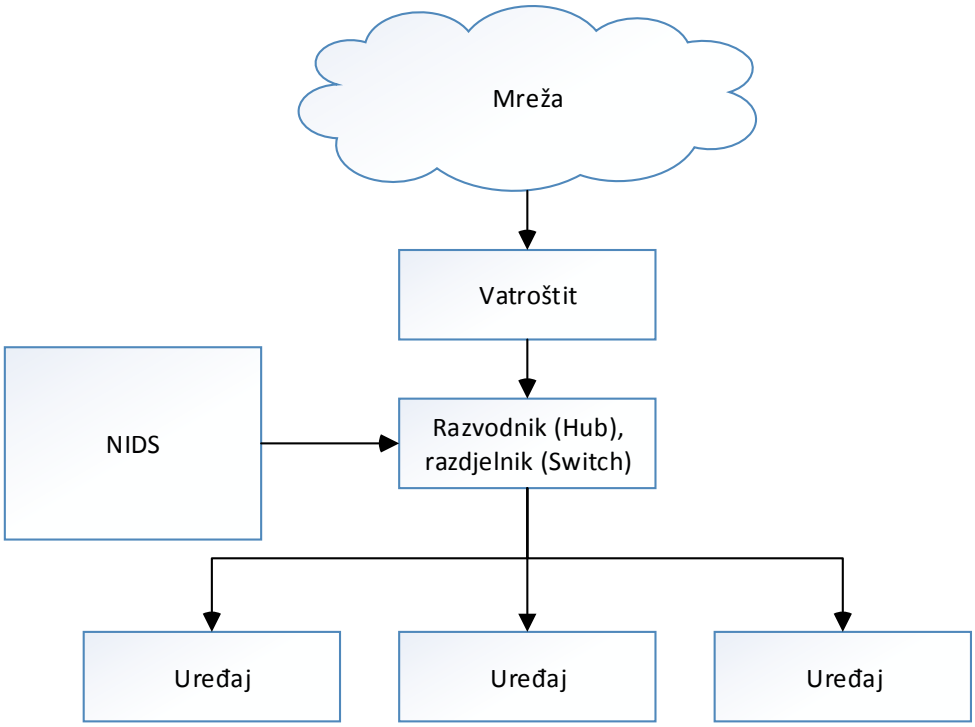
Svaka aktivnost koja se provodi na računalnoj mreži ima svoj potpis, baš kao i računalni virusi, te se on može otkriti pomoću odgovarajućeg programa. Sustav funkcionira tako da se pokuša pronaći paket podataka koji sadrži bilo koji poznati potpis koji je povezan s upadima u sustav ili nepravilnosti koje su povezane s internetskim protokolima. Sustav za otkrivanje temelji se na skupu potpisa i pravila te se mogu pronaći i zapisati sumnjive aktivnosti i stvoriti upozorenja. Sustavi za otkrivanje nepravilnosti rade tako da traže nepravilnosti u paketima. Nepravilnosti se obično nalaze u jednom dijelu naslova paketa. U nekim slučajevima ova metoda daje bolje rezultate od metode koja se temelji na potpisima. Obično otkrivanje upada u sustav „snima“ podatke iz mreže i primjenjuje pravila za tu vrstu podataka ili otkriva nepravilnosti u njemu.

Model predložen u ovome radu je ispitan u načinu rada za otkrivanje neželjenih upada uz korištenje postojeće baze podataka i ograničenog skupa napada. Rezultati analizirani u nastavku su dobiveni istim simulacijama na dva različita sustava za otkrivanje upada.

5.7.3. Podjela IDS sustava

IDS sustavi se mogu podijeliti na:

- Mrežni IDS – NIDS (engl. *Network Intrusion Detection System*) može analizirati mrežni promet i usporediti ga s datotekom u kojoj se nalazi baza potpisa napada. Mrežni IDS koristi mrežne priključnice koje su postavljenje u tzv. Promiscué modu rada (primaju sve mrežne pakete, ne samo one adresirane za to računalo/uređaj) kako bi mogao „uhvatiti“ pakete koji su namijenjeni drugim uređajima u mreži. Zadatak ovog sustava je stvarati upozorenja ako dođe do napada (i to se mora napraviti u stvarnom vremenu) te stvarati zapise za pomoć kod analize napada nakon što se napad već dogodio. Slika 5-8 prikazuje jedan tipičan primjer rada mrežnog IDS-a (*Snort*). Vatroštit propušta pakete u računalnu mrežu u kojoj se nalaze uređaji koji su spojeni s mrežnim sustavom IDS.



Slika 5-8. Mrežni IDS

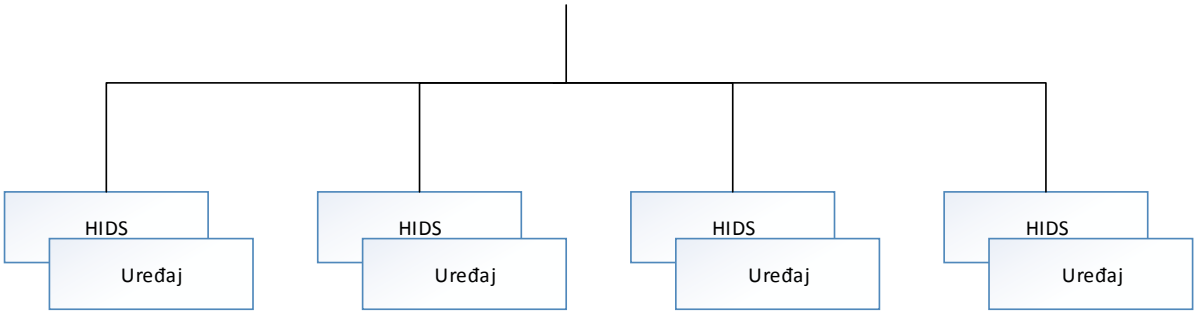
Postoje dva osnovna tipa mrežnih IDS sustava:

1. Grubi sustav za analizu – dohvaća pakete podataka iz mreže i uspoređuje ih s potpisima napada koji se nalaze u bazi podataka te provjerava podudarnost. Opisani proces se naziva analiziranje potpisa. Ovakav sustav ne obavlja obradu podataka paketa koje dohvati, već

jednostavno pretražuje podatke i traži nizove znakova koji označavaju potencijalni napad. Zbog ograničene brzine rada, ovi sustavi se ne obavezuju da će uspjeti provjeriti sve podatke.

2. Pseudo inteligentni sustavi isto kao i prethodno opisani sustavi dohvaćaju podatke iz mrežnog prometa, ali oni mogu prepoznati protokole i pravila koja upravljaju njihovim radom. Kad dohvate promet s mreže, pseudo inteligentni sustavi pokušavaju oponašati uređaj u računalnoj mreži i otkrivaju aplikacije koje se zasnivaju na mrežnom protokolu. Ovaj način rada pruža sustav koji smanjuje broj lažno pozitivnih prijava i omogućuje prepoznavanje složenijih napada. Pseudo inteligentni sustavi ne mogu obaviti svoje zadatke ako rade na mreži s velikom propusnosti jer im je potrebno znatno više vremena za analizu prikupljenih podataka.

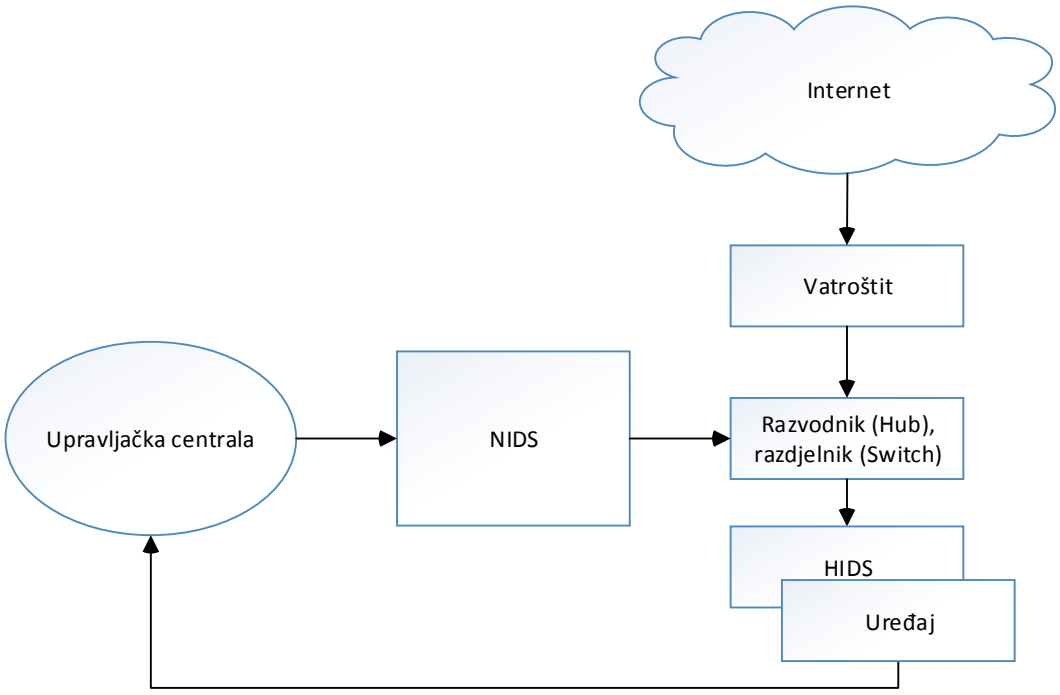
Uređaj u računalnoj mreži sa sustavom za otkivanje neovlaštenog upada – HIDS (engl. *Host Based Intrusion Detection System*) nalazi se instaliran na uređajima u računalnoj mreži (Slika 5-9). Njegovi zadaci su analizirati zapise sustava i aplikacija koji se nalaze u datotekama te prepoznati netipične aktivnosti koje bi mogle upućivati na upad. On prati promet koji ulazi u mrežu na jednom računalu kako bi mogao detektirati upade i pri tome koristi otkrivanje upada koje je temeljeno na nepravilnostima ili potpisima. Ako se primijeti neobično ponašanje na mreži, HIDS analizira zapise sustava. Primjer ovakvog neobičnog događaja je pokušaj višestrukog nepravilnog prijavljivanja u neki sustav. Provjeravaju se i datoteke u sustavu tako da se prati je li bilo promjena u njima i jesu li stvorene ili izbrisane.



Slika 5-9. Host sustav s IDS-om

Distribuirani sustav za otkrivanje upada – DIDS (engl. *Distributed Intrusion Detection System*) sastoji se od sustava NIDS, HIDS ili oba, a njegov način rada prikazuje Slika 5-10. DIDS se sastoji od senzora smještenih po cijeloj mreži koji šalju izvještaje u središnju upravljačku jedinicu te središnje upravljačke jedinice koja sadrži bazu potpisa [56]. Ako za to dođe potreba, ti se potpisi

šalju do određenog senzora kako bi on mogao provesti određenu akciju. Između središnje upravljačke jedinice i senzora koristi se kriptirana virtualna privatna mreža (engl. *Virtual Private Network, VPN*).



Slika 5-10. Distribuirani sustav za otkrivanje upada

5.7.4. Sustav za sprječavanje upada – IPS

Sustav za sprječavanje upada – IPS (engl. *Intrusion Prevention Systems*) poznat je kao sustav za otkrivanje i sprječavanje upada – IDPS (engl. *Intrusion Detection and Prevention Systems*) zbog toga što u sebi već sadrži tehnike za otkrivanje upada [57]. IPS je tehnika za sigurnost mreže i ona nadzire mrežu i/ili aktivnosti sustava zbog potrage za zlonamjernim aktivnostima. Glavne funkcije sustava za sprječavanje upada su identificirati zlonamjerne aktivnosti, zapisati informacije o tome i pokušati blokirati/zaustaviti tu aktivnost te ju prijaviti. Sustavi IPS smatraju se proširenjem sustava IDS zbog toga što oba sustava mogu nadzirati promet u mreži i/ili aktivnosti sustava u potrazi za zlonamjernim aktivnostima. Glavna razlika je u tome što IPS za razliku od sustava IDS može aktivno spriječiti/blokirati upade koji su otkriveni [58]. Točnije, IPS može poduzimati određene aktivnosti slanjem obavijesti, ispuštanjem zlonamjernih paketa, ponovnim uspostavljanjem veze i/ili blokiranja prometa s IP (engl. *Internet Protocol*) adresama povezanih s

napadom. Sustav IPS može ispraviti pogreške cikličke provjere redundancije te „očistiti“ neželjene opcije mrežnog sloja. Većina sustava IPS koristi jednu od tri metode otkrivanja upada [59] [60]:

1. Otkrivanje upada temeljeno na potpisu – koristi potpise koji su uzorak za napad te su unaprijed postavljeni i definirani. Ova metoda promatra mrežni promet i uspoređuje ga s tim potpisima. Jednom kad se pronađe poklapanje IPS sustav poduzima odgovarajuće mjere.
2. Otkrivanje upada temeljeno na anomalijama – metoda koja stvara osnovu, a kasnije sustav povremeno pomoću statističke analize ispituje mrežni promet kako bi se mogli usporediti uzorci s ranije stvorenom bazom podataka. IPS poduzima odgovarajuće radnje ako se aktivnosti razlikuju od podataka iz baze.
3. Otkrivanje upada inteligentnom analizom protokola – identificira odstupanja od stanja protokola tako da uspoređuje promatrane događaje s unaprijed definiranim profilima općeprihvaćenih definicija.

Sličnost modela predloženog u ovome radu i IPS sustava je u tome što se model predviđen za agentski rad u kojemu je moguće definirati preventivne akcije na temelju prošlih događaja i izračunatih vjerojatnosti pojave novih na temelju trenutnih vrijednosti mjernih pokazatelja.

5.7.5. Programski alat za otkrivanje mrežnih napada Snort

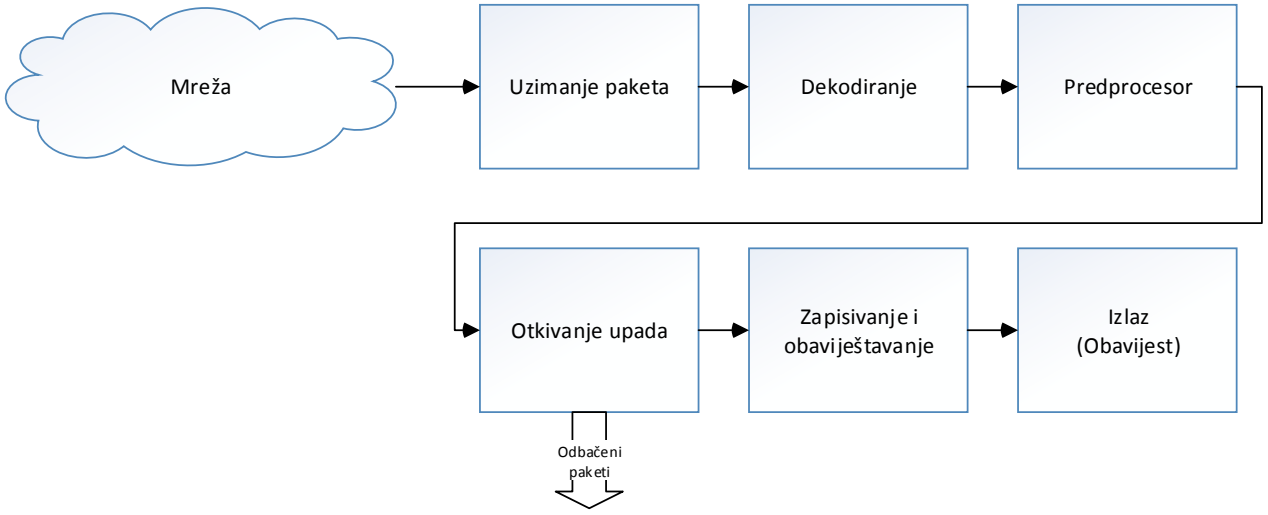
Aplikacija Snort može analizirati mrežni promet na IP mrežama i stvarati zapise u stvarnom vremenu. Radi pomoću pravila, ali postoje i dodaci (eng. *plug-ins*) koji mogu pronaći nepravilnosti u jednom paketu [66]. Pravila pomoću kojih Snort otkriva neovlaštene upade u sustav zapisuju se u tekstualnim datotekama tako da ih korisnici mogu sami prilagođavati (nadopunjavati, brisati) prema svojim potrebama. Pravila se grupiraju u kategorije kako se za vrijeme nadziranja mreže ne bi trebalo prolaziti kroz sva pravila, nego kroz određenu kategoriju. Svaka kategorija spremljena je u svoj zasebni tekstualni dokument.
U eksperimentima je korištena aplikacija Snort u načinu rada za otkrivanje neželjenih upada.

Komponente programskog alata Snort

Snort je logički podijeljen na više komponenata koje međusobno surađuju kako bi otkrile napad u mreži. Alat se sastoji od sljedećih komponenata:

- dekoder paketa (engl. *packet decoder*),
- predprocesori (engl. *preprocessors*),
- mehanizam otkrivanja (engl. *detection engine*),
- sustav stvaranja zapisa i obavijesti (engl. *logging and alerting system*),
- izlazni moduli (engl. *output modules*).

Slika 5-11 prikazuje raspored komponenata alata Snort i slijed akcija nad paketom koji se analizira. Nakon preuzimanja paketa iz mreže isti se prosljeđuje dekoderu. Preuzimanje paketa obavlja poseban dio programa, a nakon toga se obavlja i samo dekodiranje. Paketi podataka nakon obrade u dekoderu dolaze u predprocesore, koji služe kako bi pakete podataka sortirali ili promijenili prije nego što dođu do mehanizma za otkrivanje. Mehanizam za otkrivanje najvažniji je dio alata Snort i on mora otkriti maliciozne pakete (koje su napadači stvorili).
Koristi pravila koja su učitana u interne strukture podataka. Kada dođe do poklapanja paketa s nekim pravilom, obavlja definirane radnje nad tim paketom ili se on jednostavno odbacuje. Radnja koja se može obavljati nad paketom je zapisivanje paketa ili stvaranje obavijesti, a mogu se i obje radnje izvoditi istovremeno. Ovisno o tome što mehanizam za otkrivanje otkrije, sustav za stvaranje zapisa i obavijesti obavlja zapis podataka u datoteku ili se stvara odgovarajuća obavijest. Izlazni moduli mogu obavljati različite radnje ovisno o tome kako se želi sačuvati izlaz iz sustava stvaranja zapisa i obavijesti. Mogu se zapisivati podaci u datoteke, slati poruke, zapisivati u bazu podataka i slično.



Slika 5-11. Komponente programskog alata Snort

Načini rada alata Snort su:

- *Praćenje prometa (engl.sniffer)* – najjednostavniji način rada koji se pokreće u početku korištenja alata. U ovom načinu rada alat Snort prati promet paketa na mreži i objavljuje rezultate. Pokretanje ovog načina rada obavlja se naredbom „*snort-v*“, a na zaslonu se dobije ispis prometa paketa u mreži. Naredbe koje se još koriste u ovom načinu su:
    - „*snort-w*“ – ispisuje popis mrežnih kartica u mreži koju alat Snort nadzire,
    - „*snort-v-i**“ – pokretanje alata Snort, * označava mrežnu karticu s kojom se nadziru paketi
- *Stvaranje zapisa paketa (engl. packet Llogger)* – način rada u kojem se ispituju mogućnosti stvaranja zapisa paketa alatom Snort sljedećom naredbom „*snort-dev-l SnortpathMog*“. Bolja mogućnost od ove bila bi zapisati pakete u binarnu datoteku jer se s njima može brže raditi, a naredba za provođenje toga je „*snort-b-l SnortpathMog*“. Na računalu se mogu pronaći, otvoriti i provjeriti datoteke koje je alat Snort stvorio. Kad se paketi zapisu u binarnu datoteku, mogu se čitati s bilo kojim alatom koji podržava „*tcpdump*“ format.
- Mrežni IDS je najsloženiji način rada i za njegovo ispravno funkcioniranje potrebno je postaviti neke opcije: mrežne postavke (eng. *network settings*), postavke pravila (eng. Rules Settings), postavke izlaza (eng. *output settings*) i postavke uključivanja (eng. include settings).

Mrežne postavke su mjesto gdje se određuje koji dio IP adrese treba nadzirati. Osnovna postavka konfiguracije datoteke obavlja se naredbom „*varHOME-NET any*“ pomoću koje alat Snort nadzire cijelu mrežu na koju je priključen.

U postavkama pravila alatu Snort se pokazuje lokacija gdje se nalazi datoteka koja sadrži pravila (naredba „*varRULE_PATH SnortPath\rules*“).

Postavke izlaza služe kako bi se odredilo kako će izlazne informacije biti predstavljene, a to su zapisivanje s naredbom „*output logdir*“ (mjesto gdje je instaliran Snort) i obavijest naredbom „*output alert_fast:alert.ids*“.

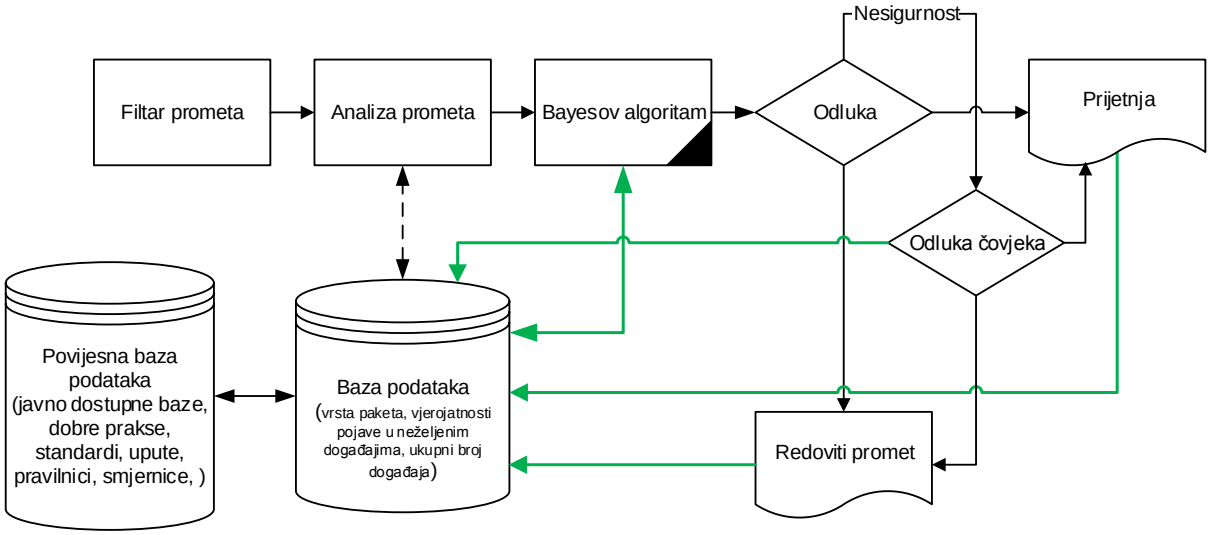
5.7.6. Primjena modela za procjenu vjerojatnosti neželjenog događaja u otkrivanju napada na informacijski sustav

Model za procjenu vjerojatnosti je u sljedećim eksperimentima ispitan u načinu rada otkrivanja neželjenih upada u računalni sustav.

Rad modela u sustavu za otkrivanje neželjenih upada u informacijski sustav je bio ograničen nekim tehničkim nedostacima. Sva mjerenja su provedena u kućnoj računalnoj mreži i uz korištenje besplatnih alata. Baza podataka je preuzeta na korištenje od strane komercijalnog alata tvrtke IBM čiji su opisi dostupni na www.iss.net.

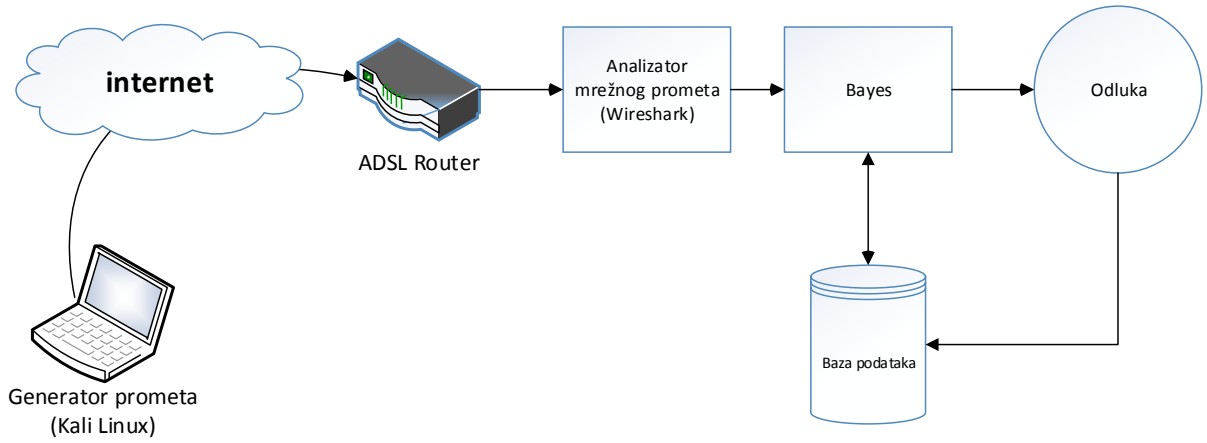
Kao filtar prometa korišten je alat Wireshark (www.wireshark.org) [65].

U ovome eksperimentu događaj nije egzaktno definiran već je potrebno model prilagoditi na način primjeren slučaju. Događaj je bila svaka promjena čije je odstupanje od prosjeka veće od 10%. Prosjek je izračunat na temelju snimljenog prometa u periodu od 10 dana.



Slika 5-12. Blok dijagram eksperimenta korištenja modela na otkrivanju neželjenih upada

Eksperiment je proveden na kućnoj mreži s ADSL pristupom Internetu uz redovito korištenje računala i mobilnih uređaja od strane istih korisnika. Povremeno je broj korisnika povećavan i to u slučajevima korištenja bežične infrastrukture. Promet je generiran korištenjem Kali Linux distribucije pri čemu je simuliran napad u kojemu je ispitan proboj WEP enkripcije (Slika 5-13).



Slika 5-13. Tehnički prikaz izvedbe eksperimenta

U ovome eksperimentu nisu definirane povratne veze za slučajeve nesigurnosti odluke. Svi rezultati su dobiveni korištenjem osnovnog algoritma modela i baze znanja s naznačenim količinama podataka.

5.7.7. Simulacija detekcije napada na informacijski sustav uz korištenje baze znanja različite veličine

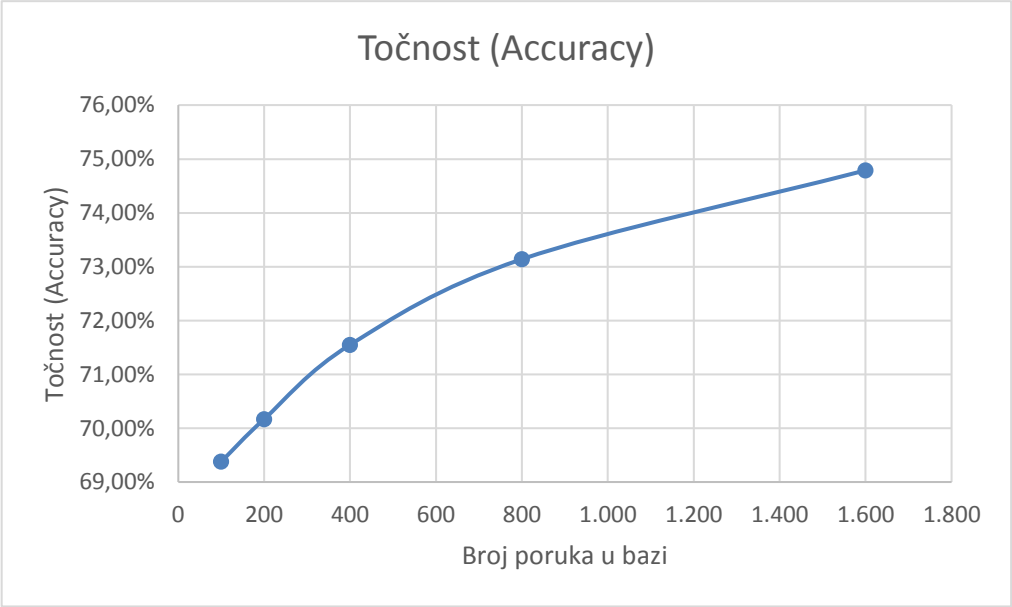
Simulacija detekcije napada na informacijski sustav uz korištenje baze znanja od 100 do 1600 zapisa

Tablica 5-8 prikazuje rezultate eksperimenta otkrivanja neželjenog upada u računalnu mrežu s bazom podataka od 100 do najviše 1600 definicija.

Tablica 5-8. Simulacija detekcije napada na informacijski sustav uz korištenje baze znanja od 100 do 1600 zapisa

Broj poruka u bazi	Točnost (Accuracy)	TP (True Positive Rate)	FP (False Positive Rate)	TN (True Negative Rate)	FN (False Negative Rate)	Preciznost (positive predictive value)
100	69,38%	70,85%	33,89%	66,11%	29,15%	82,29%
200	70,17%	71,55%	32,89%	67,11%	28,45%	82,86%
400	71,55%	72,90%	31,44%	68,56%	27,10%	83,74%
800	73,14%	73,85%	28,44%	71,56%	26,15%	85,23%
1.600	74,79%	75,05%	25,78%	74,22%	24,95%	86,61%

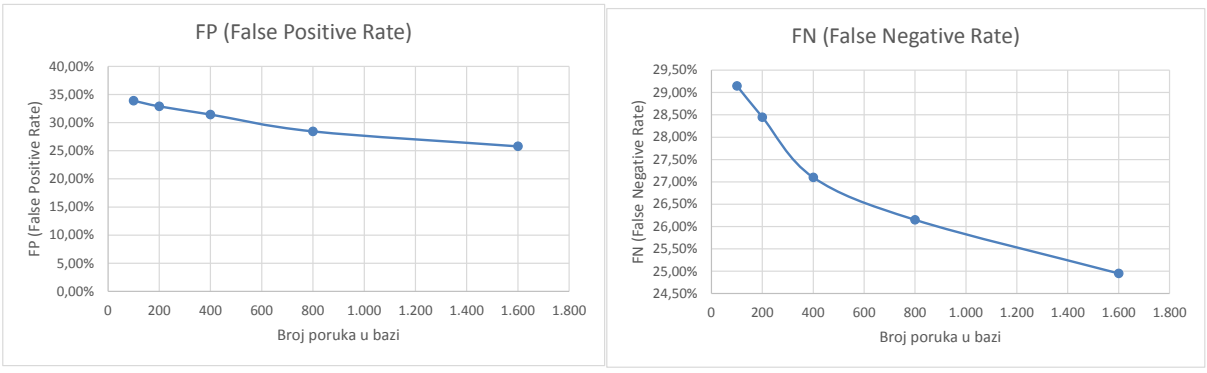
Točnost izračunata u eksperimentu i ovisnost pokazatelja točnosti i broja definicija je prikazana na slici u nastavku (Slika 5-14).



Slika 5-14. Točnost kroz eksperimente

Pogrešno predviđeni pozitivni i negativni uzorci su za manji broj definicija rezultirali vrlo sličnim pokazateljima kao i u eksperimentu otkrivanja neželjenih poruka.

Pogrešno predviđeni pozitivni i negativni uzorci u ovisnosti o broju definicija u bazi znanja prikazani su i na sljedećim slikama (Slika 5-15).



Slika 5-15. Pogrešno predviđeni pozitivni i negativni uzorci (FPR i FNR) u eksperimentu otkrivanja upada (100-1600 uzoraka)

Preciznost predviđanja neželjenih upada je 86% pri korištenju baze znanja od najviše 1600 definicija.

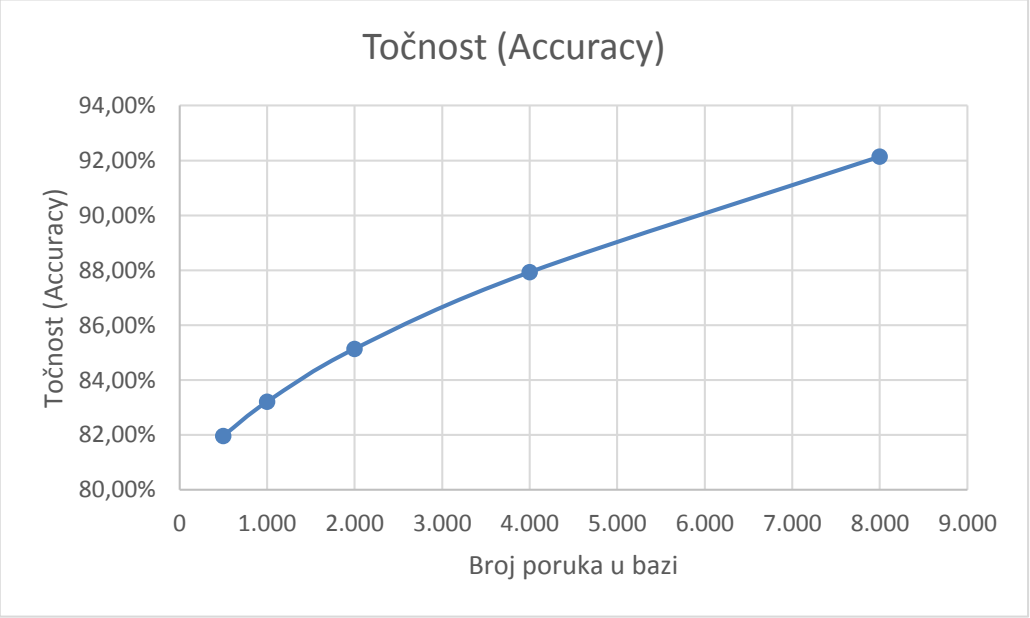
Simulacija otkrivanja napada na informacijski sustav uz korištenje baze znanja od 500 do 8000 zapisa

Tablica 5-9 prikazuje rezultate istog eksperimenta, ali uz povećan broj definicija u bazi znanja.

Tablica 5-9. Simulacija detekcije napada na informacijski sustav uz korištenje baze znanja od 500 do 8000 zapisa

Broj poruka u bazi	Točnost (Accuracy)	TP (True Positive Rate)	FP (False Positive Rate)	TN (True Negative Rate)	FN (False Negative Rate)	Preciznost (positive predictive value)
500	81,97%	86,60%	28,33%	71,67%	13,40%	87,17%
1.000	83,21%	87,75%	26,89%	73,11%	12,25%	87,88%
2.000	85,14%	89,40%	24,33%	75,67%	10,60%	89,09%
4.000	87,93%	91,50%	20,00%	80,00%	8,50%	91,04%
8.000	92,14%	94,90%	14,00%	86,00%	5,10%	93,77%

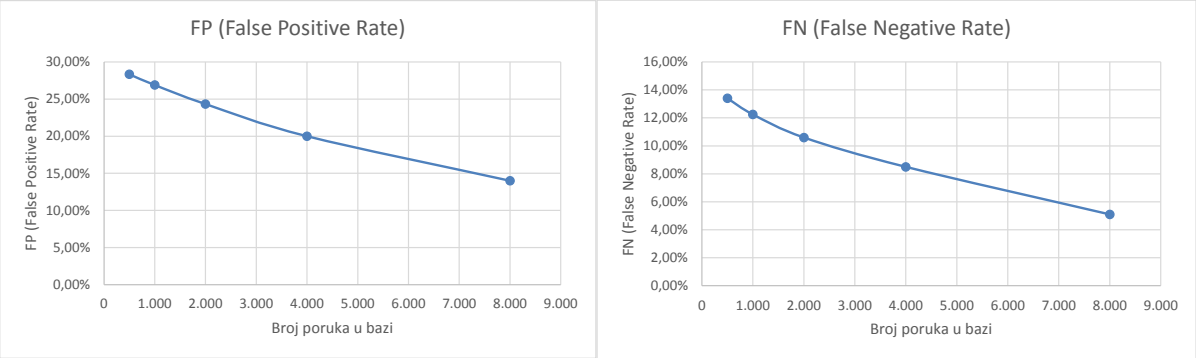
Povećan broj definicija je rezultirao većom točnošću (Slika 5-16). Pokazatelji pogrešno predviđenih pozitivnih i negativnih uzoraka su za 1% bolji od eksperimenta otkrivanja neželjene pošte s najviše 16000 uzoraka. Točnost u ovisnosti o broju definicija eksperimenta je prikazana na slikama u nastavku (Slika 5-16).



Slika 5-16. Točnost kroz eksperimente (500-8000 uzoraka)

Pogrešno predviđeni pozitivni i negativni uzorci eksperimenta otkrivanja neželjenih upada s 8000 definicija je 14% i 5%. Ispitivanje sustava s nepoznatom definicijom događaja je rezultiralo boljim

pokazateljima od prethodnog eksperimenta kada je povećavana baza znanja na 16000 uzoraka. Pretpostavka je da količina riječi klasificiranih u porukama elektroničke pošte nije dovoljno relevantan parametar u ispitivanju novih događaja (poruka elektroničke pošte) jer su se u porukama pojavljivale nove riječi i njihove kombinacije (Slika 5-17).



Slika 5-17. Pogrešno predviđeni pozitivni i negativni uzorci (FPR i FNR) u eksperimentu otkrivanja upada (500-8000 uzoraka)

Pokazatelj preciznosti za eksperiment otkrivanja neželjenih upada je 93% što je očekivani trend porasta pokazatelja s povećanjem baze znanja.

5.8. Analiza i procjena rizika

Suvremena se analiza informacijskih sustava temelji na sustavnom i sveobuhvatnom promatranju i analizi procesa i okruženja i međusobnoj interakciji mjerenih parametara. Prevenciju od neželjenog događaja, uz primjenu tradicionalnih mjera zaštite, nužno je provoditi i prepoznavanjem opasnosti, procjenom rizika te smanjivanjem ili uklanjanjem uzroka i mogućih posljedica rizika.

5.8.1. Temeljni pojmovi i definicije teorije rizika

U literaturi, različitim analizama i istraživanjima tehnoloških rizika primjetna je poprilična nedosljednost u smislu nazivlja i definicija. Tako se pojmovi kao što su rizik i opasnost ponekad pojavljuju kao sinonimi, dok su ponekada autori skloni među tim pojmovima nalaziti veću ili

manju razliku. Slična se nedosljednost primjećuje i kod definiranja pojmova kao što su pouzdanost, procjena rizika, ocjena rizika, šteta, vjerojatnost i slično.

Iako postoji veliki broj definicija termina „rizik“ većini je zajedničko to da povezuju vjerojatnost pojave neželjenog događaja, tj. scenarija i moguće posljedice koje takav scenarij, ukoliko se pojavi, može izazvati. Različiti su pristupi procjeni rizika informacijskih sustava, od jednostavnih i površnih pristupa, pa do složenih i sveobuhvatnih.

Analiza vjerojatnosti rizika korištena u ovome radu provodi se odgovaranjem na tri temeljna pitanja, prikazana u tablici 1.1.

Tablica 5-10. Tri pitanja za analizu i određivanje rizika

Pitanje:	**Oznaka:**
Koji su to mogući neželjeni događaji (scenariji)?	N
Kolika je vjerojatnost pojave neželjenih događaja?	P_N
Koje su i kolike su potencijalne posljedice (štete i vjerojatnost)?	C_N

Kako je vidljivo iz tablice 1.1. oznakom N označen je neželjeni događaj, sa p_N označena je vjerojatnost njegove pojave, a sa c_N posljedice njegove realizacije. Ukoliko su N_1, p_{N1} i c_{N1} poznati tada se uređena trojka (N_1, p_{N1}, c_{N1}) može smatrati jednim od mogućih odgovora na postavljena tri temeljna pitanja. Ukoliko je skup trojki kompletan tj. ukoliko uključuje cjelovitu analizu svih mogućih neželjenih događaja, vjerojatnost njihove pojave i potencijalne posljedice njihove realizacije, tada se taj skup može smatrati potpunim odgovorom na prethodno postavljena tri pitanja.

Temeljem navedenog formalna se definicija rizika može napisati na sljedeći način [61]:

$$R = \{(N_i, p_{Ni}, c_{Ni})\}, \quad i = 1,2, \dots, n \tag{39}$$

Važno je primijetiti da izraz definicije rizika razmatra samo neželjene scenarije odnosno neželjene učinke. Činjenica da svaki scenarij može rezultirati i ishodom koji nema neželjene učinke, s naslova tehničke primjene nije posebno značajna te će u ovom radu biti zanemarena.

Izraz „sigurnost“ često je korišteni pojam u tehničkim procesima. Tako se npr. zahtijeva da podatkovni centri u prostorima ugroženim vanjskim utjecajima rade „na siguran način“. Sigurnost i rizik komplementarni su pojmovi, manji rizik znači veći stupanj sigurnosti. U analizama rizika sigurnost se često definira kao mjera prihvatljivog rizika. Odnos sigurnosti i rizika može se prikazati izrazom:

$$sigurnost = 1 - p_R * rizik \quad (40)$$

gdje je p_R percepcija rizika. Percepcija odnosno prihvatljivost rizika iznimno je složena i važna komponenta u procesu određivanja rizika, te kasnije kod upravljanja rizikom. Prihvatljivost rizika se više temelji na iracionalnim odrednicama (npr. sociološkim i psihološkim) nego na racionalnim (tehničkim). Za najjednostavniji slučaj, odnosno kada je percepcija rizika neutralna (p_R=1), sigurnost može biti prikazana izrazom:

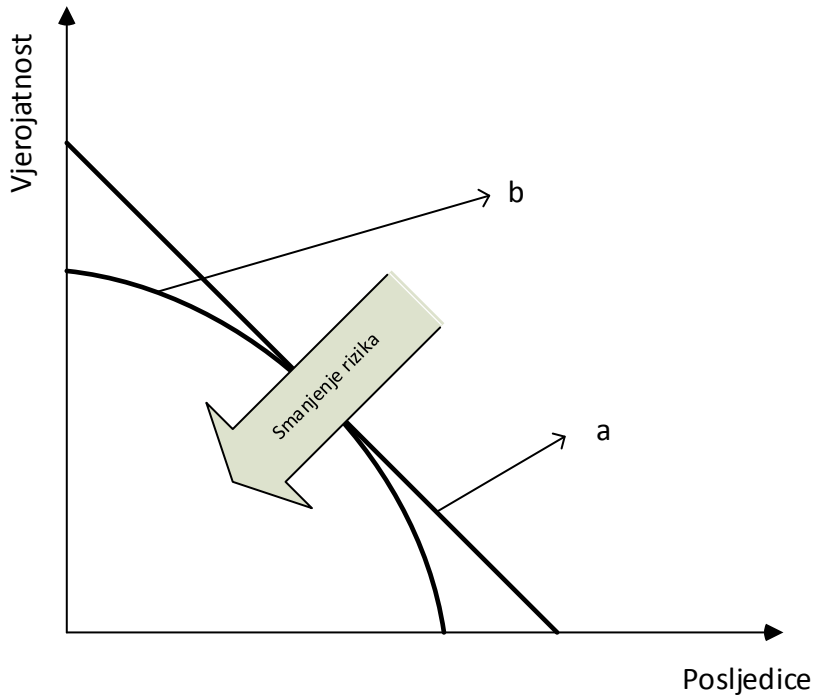
$$sigurnost = 1 - rizik \quad (41)$$

Procjena rizika, sigurnosti, opasnosti i pouzdanosti, u osnovi, može biti kvalitativna i kvantitativna. U kvantitativnim (matematičkim) procjenama [62] pouzdanost je „matematička" vjerojatnost zadovoljavajućeg ponašanja (rada, djelovanja, funkcioniranja), uz definirane radne uvjete, tijekom predviđenog vremena, dok se rizik može definirati kao mjera povezanosti vjerojatnosti zbivanja neželjenog događaja (događanja, opasnosti) i posljedice takvog neželjenog događaja (događanja, opasnosti). Općenito, inženjerska definicija rizika glasi:

RIZIK [*funkcija očekivanog gubitka i vremena****] = VJEROJATNOST [****funkcija neželjenog događaja i vremena****] x POSLJEDICA [****funkcija očekivanog gubitka i neželjenog događaja****]***

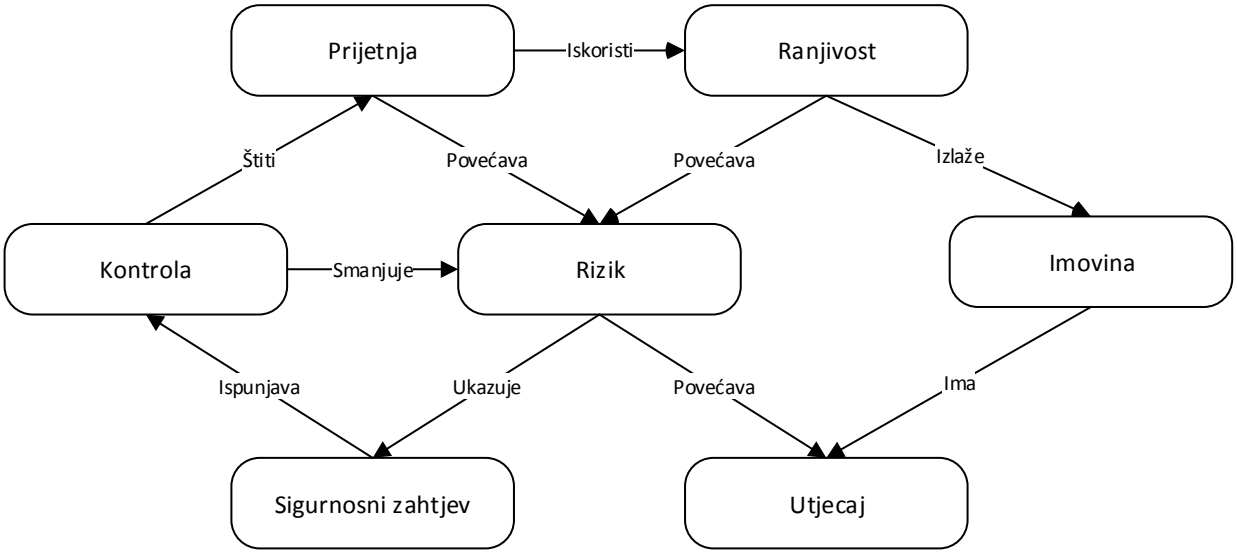
Za vjerojatnost iz prethodne definicije obično se koristi sintagma „matematička vjerojatnost". Matematička iz razloga jer je nužno izračunati tu vjerojatnost, dakle ne samo procijeniti je, a „vjerojatnost" jer je očekivanje povezano s budućnošću. Budućnost se povezuje s neizvjesnošću i neodređenošću, a ova neodređenost s vjerojatnosti. Vjerojatnost je, najjednostavnije rečeno, mjera ostvarivosti slučajnog događaja.

Ako se za određeni sustav odredi prihvatljivi rizik (područje prihvatljivog rizika) tada se može dati i grafički prikaz rizika [62], kako je prikazano na slici (Slika 5-18):



Slika 5-18. Grafički prikaz krivulje rizika

Područje ispod pravca *a* na slici predstavlja područje prihvatljivog rizika. Pravac *a* grafički je prikaz linearizacije rizika koji je jednak sumi produkata vjerojatnosti i posljedica za svaki pojedinačni scenarij, dok se za krivulju *b* općenito smatra da svojim konkavnim oblikom bolje aproksimira rizik. Egzaktan prikaz krivulje je hiperbola. Proces smanjenja rizika prikazuje Slika 5-19 na kojoj su grafički prikazani svi elementi procesa upravljanja rizicima informacijskog sustava.



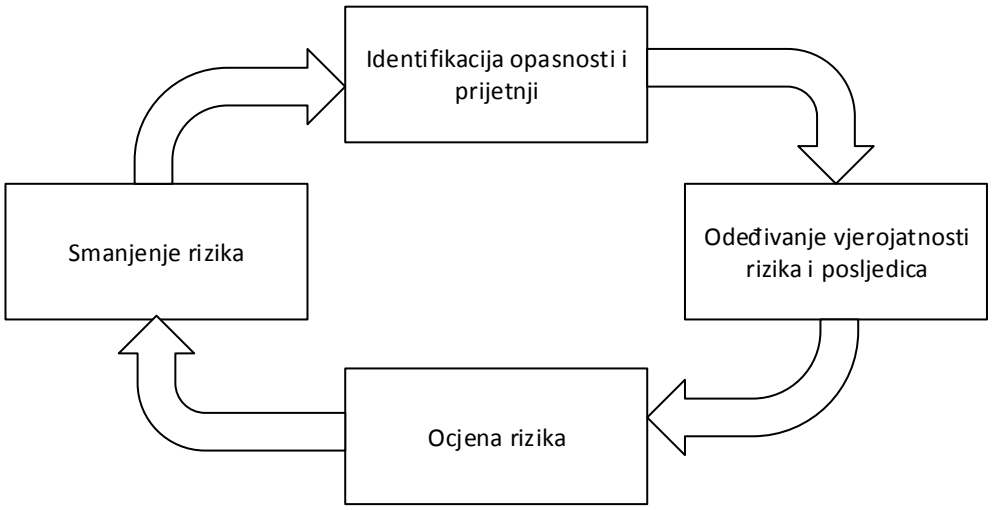
Slika 5-19. Proces upravljanja rizicima

5.8.2. Postupci u procesu procjene rizika

Težnja da se odgovori na pitanja: „Koliko je nešto sigurno?“, „Koliko sigurno je dovoljno sigurno?“ i slična razvila je novu znanstveno-tehničku disciplinu nazvanu procjena rizika (*Risk Assessment*). Procjena rizika je svojim kvalitativnim i kvantitativnim procedurama omogućila pretvorbu različitih vrsta opasnosti i subjektivnih percepcija u objektivne veličine. Cilj je procjene rizika osigurati vezu između vjerojatnosti, odnosno učestalosti frekvencije pojave neželjenog događaja i posljedica očekivanih gubitaka, a u svrhu postizanja zahtijevane razine sigurnosti, sukladno stanju tehnike, tehničkim i ekonomskim zahtjevima i slično. Procjena rizika objedinjuje postupke identifikacije opasnosti, analiza opasnosti i ocjene (proračuna) rizika, a sve s ciljem dovođenja rizika u područje prihvatljivosti, uzimajući pri tome u obzir gospodarske, psihosocijalne i slične aspekte. Identifikacija (prepoznavanje) potencijalnih opasnosti (engl. *hazard identification*) podrazumijeva izradu popisa svih mogućih neželjenih scenarija.

Danas je razvijen cijeli niz tehnika za strukturiranje i kategorizaciju neželjenih scenarija. Neke od raširenih metoda su analiza HAZOP (engl. *Hazard Operability Analysis*), postupak FMEA (engl. *Failure Mode and Effect Analysis*), analizu „što-ako“ (*What-if-Analysis*), stablo kvara i stablo događaja (engl. *Fault Tree and Event Tree Analysis*) i slično. Određivanje rizika (engl. *Risk Estimation*) je utvrđivanje učestalosti (vjerojatnosti) s kojom može biti ostvarena prepoznata opasnost, koja će prouzročiti neželjenu posljedicu (oštrinu štete). Ocjena rizika (engl. *Risk Evaluation*) uspoređuje rizike s određenim kriterijima prihvatljivosti. Postupak smanjenja rizika

definira nužne mjere za svođenje rizika u područje prihvatljivosti. Osnovnu strukturu odnosno osnovni tijek postupka procjene rizika se može prikazati slikom (Slika 5-20), [63], Procjena rizika iterativan je postupak.



Slika 5-20. Osnovna struktura postupka procjene rizika

Prepoznavanje potencijalnih opasnosti podrazumijeva izradu popisa svih mogućih neželjenih scenarija što nije nimalo jednostavan posao.

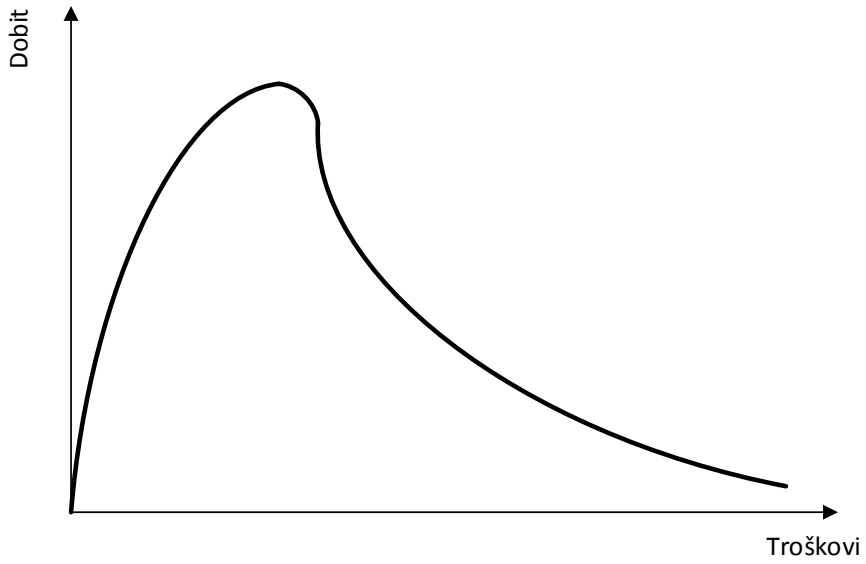
Određivanje rizika (*Risk Estimation*) odnosno tumačenje vjerojatnosti pojave nekog neželjenog scenarija još uvijek, u znanstvenim i stručnim krugovima, nema jedinstveni pristup. Dva su najznačajnija/dominantna pogleda odnosno pristupa pojmu vjerojatnosti. U objektivnim analizama rizika vjerojatnost je definirana kao eksperimentalna ili statistička vrijednost. Takvo određivanje vjerojatnosti pretpostavlja postojanje stvarne vrijednosti i vjerojatnost je rezultat eksperimenta koji se bez većih poteškoća može ponoviti nebrojeno puta. Tada se rezultat naziva frekvencijom [63]. Prema ovom pristupu vjerojatnost egzistira u stvarnom svijetu i mjerljiva je dovoljnim uzorkovanjem i statističkom analizom. Ova se interpretacija vjerojatnosti često naziva statističkom ili objektivističkom.

Nasuprot ovoj teoriji subjektivisti o vjerojatnosti govore kao o pojmu koji odražava stanje znanja odnosno razinu uvjerenosti o problemu koji se analizira. Prema ovom pristupu subjektivizam se ogleda u stanju znanja, a ne izražava individualnost razmišljanja. Vjerojatnost, prema ovom načinu razmišljanja, nije samo funkcija slučajne varijable kao takve nego i količine i kvalitete raspoloživih informacija kojima raspolaže analitičar. Ovaj se pristup uobičajeno naziva Bayesovim ili subjektivističkirn.

Obje teorije imaju svoju opravdanost i utemeljenost. Objektivistička teorija govori o frekvenciji. Frekvencija je objektivna i mjerljiva i u određenim slučajevima aproksimira vjerojatnost na sasvim

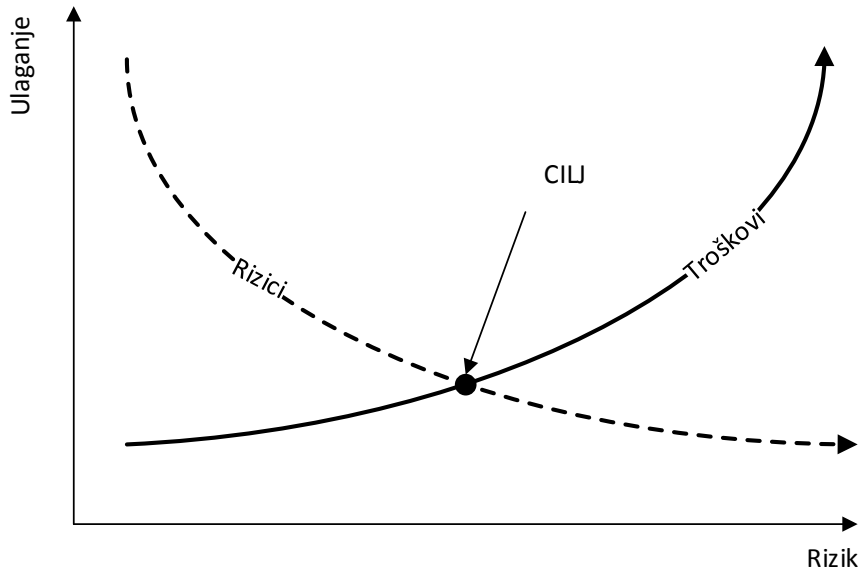
zadovoljavajući način. Vjerojatnost je nasuprot tome, subjektivna i teško mjerljiva. U tom smislu potrebno je raditi razliku između pojmova statistike i teorije vjerojatnosti. Načelno i općenito, statistika je vještina korištenja podataka, dok bi teorija vjerojatnosti bila umijeće logičkog zaključivanja u uvjetima nedostupnosti podataka.

Primjena Bayesovog odnosno subjektivističkog pristupa ima neupitnu vrijednost u slučajevima kada se promatraju i analiziraju pojave s velikim brojem podataka [64]. Razmatrajući korištenje Bayesovog teorema u procesu procjene rizika s aspekta cijene koju nose implementacije različitih sustava zaštite je također neupitna jer predloženi model ne iziskuje velike potrebe za financijskim implementacijama u opremu i okruženje. Slika 5-21 prikazuje odnos troškova i dobiti prilikom ulaganja u sigurnost informacijskog sustava.



Slika 5-21. Odnos troškova i dobiti

Dodatni argument je mogućnost implementacije modela u poslovne sustave u kojima je moguće izračunavati vjerojatnosti neželjenih događaja u poslovnim procesima. Slika 5-22 prikazuje točku optimuma između ulaganja u smanjenje i veličine preostalog rizika.



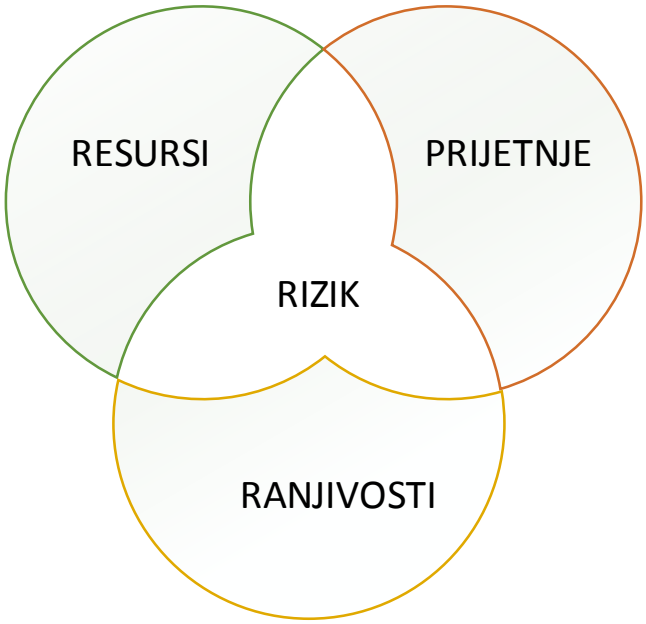
Slika 5-22. Optimizacija ulaganja i rizika

Upravljanje rizicima je pitanje optimizacije s ciljem dovođenja sustava u najpovoljnije stanje i upravo je to jedan od razloga provođenja eksperimenata s rizicima upravljanim informacijskim sustavom. Ocjena rizika (*engl. Risk Evaluation*) i s njom povezani postupci za smanjenje rizika subjektivistička su kategorija i ovise o sociološkim, tehničkim, financijskim i sličnim uvjetima. Ocjena rizika je usporedba rizika s određenim kriterijima prihvatljivosti, koji mogu biti manje ili više definirani i/ili regulirani.

Procjena rizika korištena u ovome radu je kombinacija više metoda za dobivanje konačne ocjene rizika koja predstavlja vjerojatnost ostvarenja neželjenog događaja. Neželjeni događaj je opisan vjerojatnošću iskorištavanja ranjivosti na temelju postojeće prijetnje.

Rizik se matematički može promatrati kao funkcija tri parametra: prijetnji, ranjivosti i vrijednosti resursa (Slika 5-23).

$$\boldsymbol{Rizik} = \boldsymbol{f}\ (\boldsymbol{Prijetnje}, \boldsymbol{Ranjivosti}, \boldsymbol{Vrijednost\ resursa}) \quad (42)$$



Slika 5-23. Grafički prikaz elemenata sigurnosnog rizika

Što je sustav više izložen prijetnjama, što je veći broj ranjivosti i što je resurs značajniji za organizaciju, to je i sigurnosni rizik veći. Naravno, jasno je da se sigurnosni rizik nikada neće uklanjati umanjivanjem vrijednosti resursa, već implementacijom odgovarajućih sigurnosnih kontrola koje će utjecati na parametre ranjivosti i prijetnji. Vrijednost resursa koji je ovdje naveden kao jedan od parametara o kojemu ovisi razina sigurnosnog rizika, može se promatrati i na drukčiji način. Naime, vrlo često se umjesto vrijednosti resursa kao treći parametar u obzir uzima potencijalni gubitak za organizaciju u slučaju gubitka ili neraspoloživosti resursa o kojem se govori. Bez obzira o kojem je od dva navedena parametra riječ, ishod je identičan, budući da su vrijednost resursa i posljedice u slučaju gubitka dvije izravno vezane veličine.

5.8.3. Identifikacija i klasifikacija resursa

Prvi korak u postupku procjene rizika je identifikacija, odnosno klasifikacija informacijskih resursa. U ovom koraku potrebno je identificirati sve one resurse koji predstavljaju značaj za organizaciju te im pridijeliti odgovarajuću vrijednost. Ukoliko postoji mogućnost, svakom resursu potrebno je pridijeliti konkretnu novčanu vrijednost, budući da to uvelike može pridonijeti kvaliteti rezultata cijelog postupka. Identifikaciju i pridjeljivanje vrijednosti pojedinim resursima potrebno je obaviti kako bi se u konačnici implementirale samo one sigurnosne kontrole koje su financijski

isplative. Postupku pridjeljivanja vrijednosti resursima potrebno je posvetiti posebnu pažnju, budući da loše procjene u ovom slučaju mogu cijeli proces odvesti u krivom smjeru. Prilikom određivanja vrijednosti potrebno je u razmatranje uzeti brojne druge čimbenike, osim inicijalnih troškova njegove nabave. Neki od tipičnih resursa koji predstavljaju važnost za organizaciju su:

- sklopovlje (engl. *hardver*),
- programska podrška (engl. *softver*),
- podaci,
- ljudski resursi i slično.

5.8.4. Identifikacija prijetnji

Pod sigurnosnim prijetnjama (engl. *threat*) smatraju se svi oni neželjeni faktori koji se mogu negativno odraziti na integritet, povjerljivost i dostupnost resursa. Izvori prijetnji mogu se podijeliti u osnovne skupine:

- **Namjerne** – oni izvori koji ciljano iskorištavaju nedostatke u sustavima u svrhu ostvarivanja neovlaštenog pristupa. U ovu skupinu najčešće spadaju neovlašteni korisnici, razni maliciozni programi (crvi, virusi…) i slično.
- **Nenamjerne** – izvori koji uključuju slučajne neželjene događaje za čije ostvarenje je zadužen nemar, nepažnja, slučajne štete, itd.
- **Viša sila** – oni izvori koji rezultiraju slučajnim iskorištavanjem ranjivosti u sustavu, npr. elementarne nepogode kao što su požari, poplave, potresi, udari groma itd.

U okviru procjene rizika vrlo je važno generirati listu svih onih prijetnji, namjernih i nenamjernih, koje predstavljaju potencijalnu opasnost za informacijski sustav. Prilikom identifikacije prijetnji poželjno je u obzir uzeti sve ranije incidente i ostale neželjene događaje, motive koji mogu biti podloga za provođenje napada, lokaciju na kojoj se nalaze resursi te ostale čimbenike koji na bilo koji način predstavljaju prijetnju za IT sustav. Neke od prijetnji koje su tipične za informacijske sustave uključuju:

- neovlaštene korisnike,
- maliciozne programe (virusi, crvi, trojanski konji,…),
- elementarne nepogode (poplave, potresi, požari,…),
- korisničke pogreške (namjerne i slučajne),
- krađu,
- greške u programiranju (namjerne i slučajne),

- neispravno rukovanje resursima,
- industrijsku špijunažu,
- interne napade i slično.

Za svaku od identificiranih prijetnji potrebno je odrediti povezanost sa resursima organizacije, motive koji stoje iza svake od njih te načine na koje prijetnje mogu utjecati na poslovne procese. Što je detaljnije razrađena lista prijetnji to je jednostavnije odrediti sigurnosni rizik povezan s odgovarajućim resursom.

5.8.5. Identifikacija ranjivosti

Pod pojmom ranjivosti (engl. *vulnerability*), smatraju se svi propusti i slabosti u sustavu sigurnosti koji omogućuju provođenje neovlaštenih aktivnosti. Ranjivosti mogu biti posljedica pogrešaka u procesu dizajna ili implementacije sustava, kao i propusta u sustavu provođenja sigurnosnih pravila i procedura. Iako se ranjivosti najčešće povezuju uz greške u programskom kodu, mogući su i brojni drugi primjeri, kao što su površno implementirana fizička sigurnost, nepoznavanje i neprikladan odabir tehnologija i alata, propusti u održavanju sustava i slično. Bez adekvatne analize ranjivosti, gotovo je nemoguće pouzdano određivanje sigurnosnog rizika. Ovisno o broju i karakteru ranjivosti u sustavu, sigurnosni rizik može biti veći ili manji. Implementacijom sigurnosnih kontrola kojima će se umanjiti broj ranjivosti u sustavu, izravno je moguće utjecati na umanjivanje sigurnosnog rizika. Kada se govori o procjeni rizika, iznimno je važno da se ranjivosti analiziraju u kombinaciji sa identificiranim prijetnjama, budući da su ova dva parametra međusobno povezana. Ukoliko ne postoji prijetnja koja bi iskoristila određenu ranjivost, tada ne postoji niti sigurnosni rizik. Tamo gdje nema rizika ne isplati se ulagati u zaštitu, što je osnovni cilj postupka upravljanja sigurnosnim rizikom: implementacija samo onih zaštitnih mjera koje će biti opravdane i smislene u pogledu zaštite poslovnih ciljeva organizacije.

Ono što se nameće kao osnovno pitanje kada se raspravlja o identifikaciji i analizi ranjivosti je način na koji je najbolje provesti njihovu detaljnu i temeljitu analizu. Neki od mogućih pristupa su:

- analiza rezultata ranije provedenih procjena rizika (ukoliko postoje),
- analiza internih izvještaja i dokumentacija vezanih uz ispitivanje, analizu i unaprjeđenje sigurnosti,
- provođenje specijaliziranih sigurnosnih ispitivanja (*Vulnerability Scanning, Pentration Testing, Application Testing* i slično),

- pretraživanje javnih baza ranjivosti (BUGTRAQ, CERT, itd.),
- intervjui sa zaposlenicama i sistem administratorima itd.

Rezultat ove faze treba biti detaljna lista ranjivosti prisutnih u sustavu, kao i njihova povezanost sa prijetnjama identificiranim u prethodnom koraku.

5.8.6. Analiza postojećih kontrola

U ovom koraku cilj je analizirati one sigurnosne kontrole koje su već implementirane ili koje se namjeravaju implementirati u svrhu zaštite informacijskih resursa. Ukoliko se želi izračunati vjerojatnost iskorištavanja pojedine ranjivosti od strane identificiranih prijetnji, što je sljedeći korak procesa procjene rizika, potrebno je u obzir uzeti sve postojeće kontrole prisutne u sustavu. Vrlo je mala vjerojatnost da će određena slabost ili nedostatak biti iskorišteni, ukoliko su implementirane kvalitetne sigurnosne kontrole ili ukoliko postoji mali interes za njenim iskorištavanjem. Sustavi koji rukuju povjerljivim podacima kao što su naprimjer brojevi kreditnih kartica, obračuni plača i slično, predstavljaju puno veći izazov za neovlaštene korisnike u odnosu na ostale sustave koji rukuju manje povjerljivim podacima. Sigurnosne kontrole mogu biti tehničke i ne-tehničke prirode. Pod tehničkim sigurnosnim kontrolama smatraju se sve one kontrole koje su implementirane u oblik sklopovlja, programske podrške ili nekog drugog sličnog rješenja (npr. vatroštiti, IDS sustavi, antivirusna zaštita, sustavi kontrole pristupa i slična rješenja). Pod ne-tehničkim kontrolama smatraju su kontrole poput sigurnosnih politika, preporuka i procedura i koje su najčešće rezultat usmene ili pismene predaje. Još jedna od podjela, koja je više prisutna u krugovima koji se bave računalnom sigurnošću, je ona koja sigurnosna rješenja mehanizme dijeli na:

- **Preventivne** (engl. *prevention*) – ona rješenja koja djeluju preventivo u smislu sprječavanja neovlaštenih aktivnosti (npr. antivirusni programi, vatroštitovi, kontrola pristupa i slično)
- **Detekcijske** (engl. *detection*) – sustavi koji omogućuju detekciju neovlaštenih aktivnosti (npr. IDS sustavi, alati za provjeru integriteta, i slično);
- **Reakcijske** (engl. *reaction*) – oni mehanizmi koji pomažu pri reakciji na detektirane neovlaštene aktivnosti (npr. forenzička analiza);

Rezultat ovog koraka je lista postojećih ili predviđenih sigurnosnih kontrola kojima je cilj zaštiti informacijske resurse organizacije. Implementirane kontrole umanjuju ukupnu vjerojatnost ostvarenja rizika, odnosno umanjuju vjerojatnost ostvarenja prijetnje.

5.8.7. Vjerojatnosti iskorištavanja ranjivosti

Sljedeći korak u procesu procjene rizika je određivanje vjerojatnosti iskorištavanja pojedine ranjivosti od strane pripadajućih sigurnosnih prijetnji. Vjerojatnost iskorištavanja ranjivosti od strane određenog izvora prijetnji najbolje je izraziti stupnjevito: npr. visoki, srednji i niski stupanj, pri čemu svaki od definiranih stupnjeva ima određeni značaj i smisao.
U sljedećoj tablici (Tablica 5-11) dan je primjer jedne takve podjele, s time da je moguće ići i na precizniju podjelu, ovisno o potrebama.

Tablica 5-11. Vjerojatnost iskorištavanja ranjivosti

Vjerojatnost	**Definicija**
Visoka	Izvor prijetnje je posebno motiviran za iskorištavanje ranjivosti s obzirom na mogućnost dolaska do povjerljivih podataka. Postojeće sigurnosne kontrole su nedovoljne ili sadrže slabosti koje omogućuju zaobilaženje definiranih sigurnosnih mjera.
Srednja	Izvor prijetnje je djelomično motiviran. Iako postoje mogućnosti za iskorištavanje ranjivosti postojeće kontrole to otežavaju.
Niska	Izostanak motivacije za iskorištavanje ranjivosti. Sigurnosne kontrole kvalitetno su implementirane i iskorištavanje ranjivosti prilično je otežano

Rezultat ovog koraka sadrži vjerojatnosti iskorištavanja pojedinih ranjivosti identificiranih u prethodnom koraku, s obzirom na navedene prijetnje.

5.8.8. Određivanje rizika

Ključni korak cijelog procesa je određivanje vrijednosti rizika. Rizik je potrebno odrediti za sve parove prijetnja/ranjivost, pri čemu u obzir treba uzeti sljedeće elemente:

- vjerojatnost iskorištavanja pojedine ranjivosti od strane pripadajuće prijetnje,
- posljedice u slučaju uspješne realizacije,
- kvaliteta i pouzdanost postojećih i planiranih sigurnosnih kontrola.

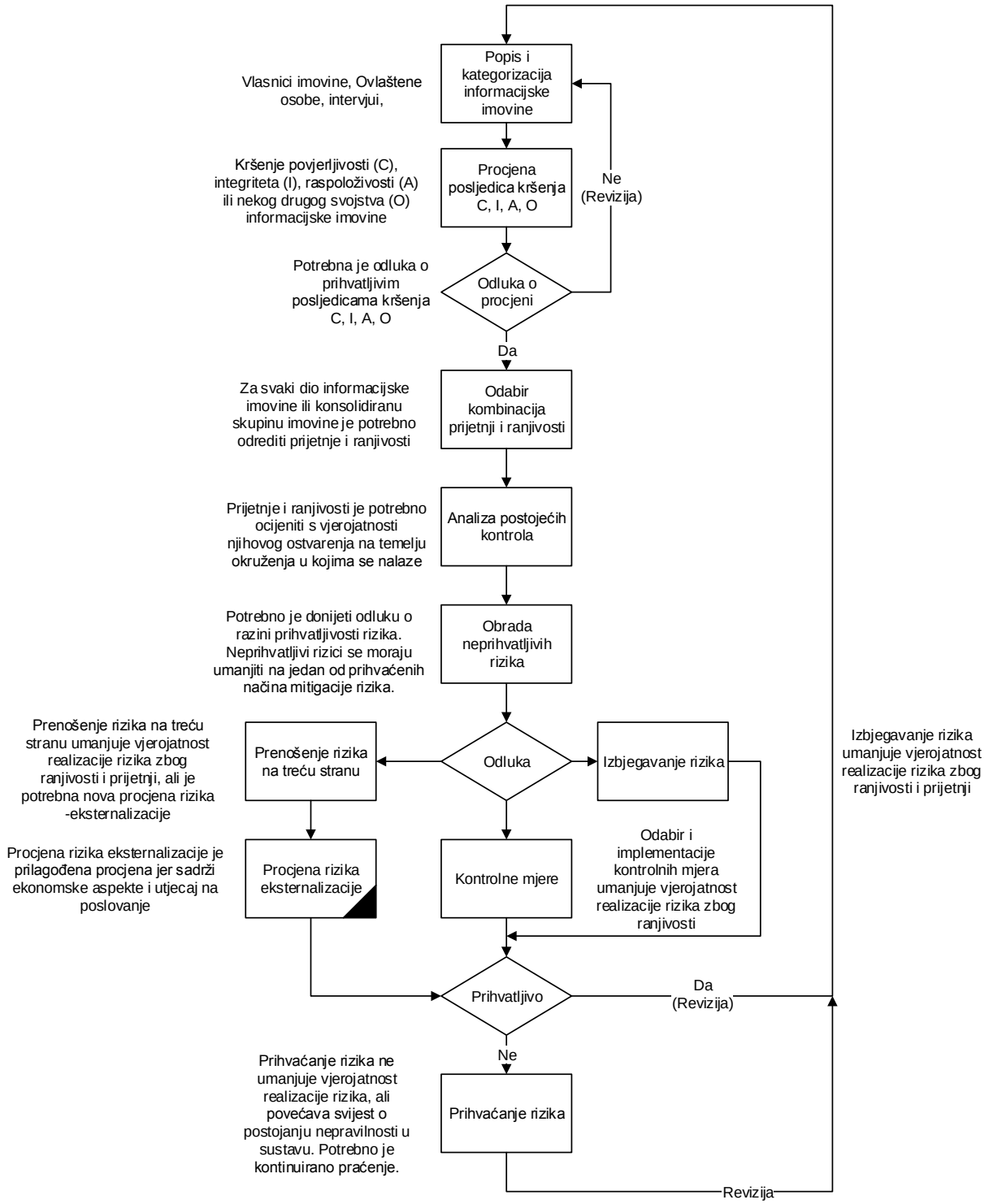
Za određivanje i analizu sigurnosnog rizika poželjno je kreirati matricu. Razine sigurnosnog rizika najjednostavnije je odrediti na temelju podataka i tablica koje su proizašle iz dva prethodna koraka:

analize vjerojatnosti realizacije i analize potencijalnih gubitaka. Na temelju ovih podataka moguće je kreirati matricu rizika (Tablica 5-12) koja će opisivati različite razine sigurnosnog rizika prisutne u sustavu.

Tablica 5-12. Matrica i skala sigurnosnog rizika

Matrica rizika		Razina prijetnje	**0**			**1**			**2**		
		Razine ranjivosti	**0**	**1**	**2**	**0**	**1**	**2**	**0**	**1**	**2**
Ocjena posljedice	Bez vrijednosti ili zanemarivo	**0**	0	1	2	1	2	3	2	3	4
	Niska vrijednost	**1**	1	2	3	2	3	4	3	4	5
	Srednja vrijednost	**2**	2	3	4	3	4	5	4	5	6
	Visoka vrijednost	**3**	3	4	5	4	5	6	5	6	7
	Vrlo visoka vrijednost	**4**	4	5	6	5	6	7	6	7	8

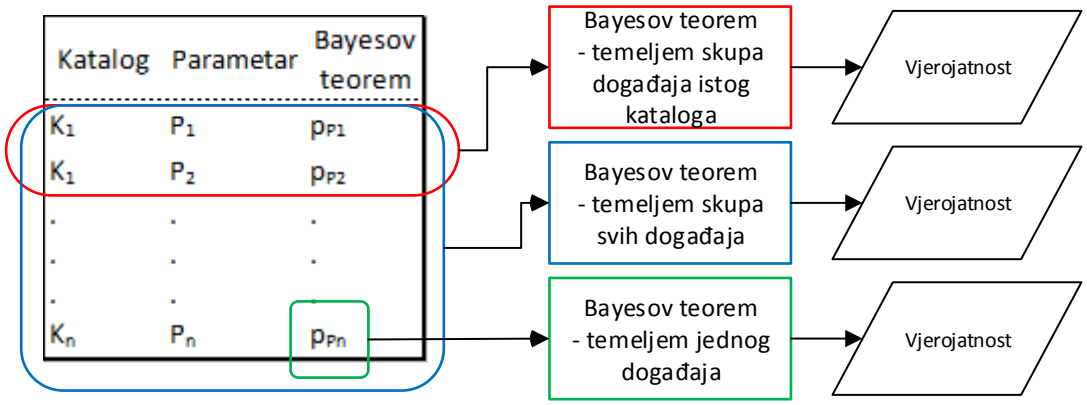
Cjelokupni proces upravljanja rizicima sadrži sve opisane aktivnosti. Načelno se proces upravljanja rizicima može uvesti na različite načine, od vrlo jednostavnog do složenog i sveobuhvatnog procesa koji uključuje široki spektar informacijske imovine. Na slici je prikazan primjer sustava upravljanja rizicima na temelju čije je metodologije osmišljena simulacija prikazana u ovome radu (Slika 5-24).



Slika 5-24. Blok dijagram metodologije upravljanja rizicima

5.8.9. Primjena modela za procjenu vjerojatnosti neželjenog događaja u praćenju parametara procjene rizika

Korištenje baza podataka s brojevima klasificiranih parametara i njihovih sudjelovanja u ukupnom broju željenih i neželjenih događaja, proširuje se mogućnostima uspostave modela u uže područje primjene. Slika 5-25 prikazuje tri načina primjene modela u bazi korištenoj u eksperimentu. Provedena su dva eksperimenta: prvi uz korištenje cijele baze podataka (dio prikazuje Tablica 5-13) s rizicima i njihovim vjerojatnostima ostvarenja i drugi uz korištenje samo jedne kategorije rizika. Korištenje jedne kategorije rizika je uključivalo praćenje parametara samo za prijetnje i ranjivosti u kategoriji sklopovlja (hardvera).



Slika 5-25. Načini korištenja modela u bazama s klasificiranim parametrima

Tablica 5-13 prikazuje primjer promatranih parametara u eksperimentu upravljanja sustavom pomoću rizika temeljenih na evidentiranim ranjivostima i prijetnjama.

Tablica 5-13. Primjer parametara praćenih u eksperimentu

Parametri događaja	**Bayes**
Temperatura u serveru 50% iznad prosječne	52,08%
Istom zapisu u bazi istovremeno pristupa 25% djelatnika više od maksimuma	45,07%
Temperatura u serveru 75% iznad prosječne	59,48%
75% više detekcija napada u jedinici vremena	54,71%
Iskorištenost pojasne brzine iznad 50% zakupljene	46,85%
Temperatura u DR serveru 25% iznad prosječne	49,04%
Produkcijska Baza podataka nema odziva	64,94%
90% manje istovremeno prijavljenih klijenata	64,98%
Putem Interneta sustavu istovremeno pristupa prosječan broj klijenata	39,11%

Parametri događaja	Bayes
Mrežni promet 90% veći od prosjeka	68,55%
75% više transakcija u jedinici vremena	55,11%
75% više aplikacijskih upita na bazu u jedinici vremena	57,44%

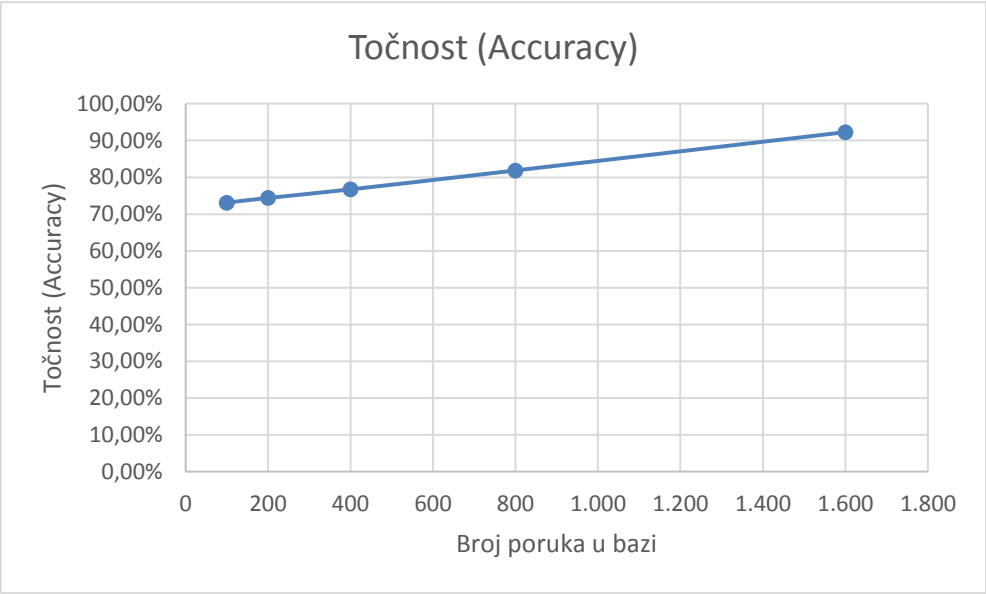
5.8.10. Izračun vjerojatnosti na temelju cijelog skupa praćenih parametara

Rizici u sljedećem eksperimentu su određeni temeljem definiranih prijetnji i ranjivosti. Subjektivnom metodom su određene vrijednosti početnih vjerojatnosti za potrebe algoritma modela. Rezultati modela su uspoređivani s odlukama eksperata iz područja upravljanja informacijskim i komunikacijskim sustavima (Tablica 5-14).

Tablica 5-14. Rezultati eksperimenta praćenja rada sustava na temelju rizika

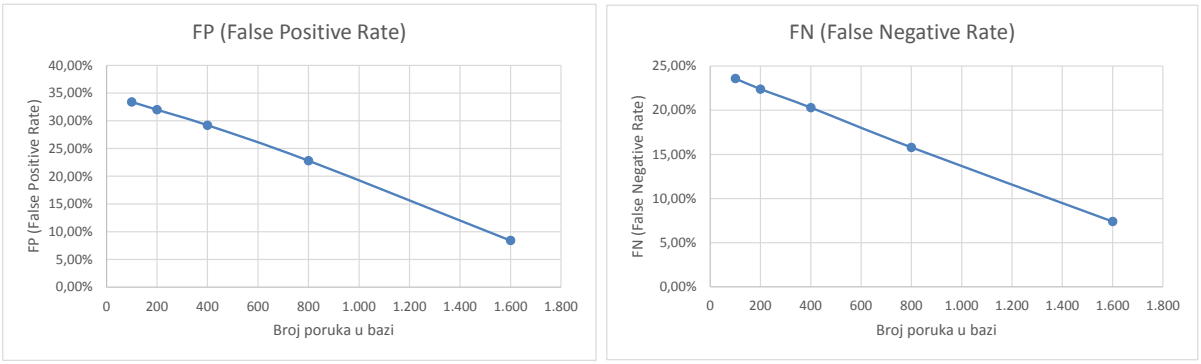
Broj poruka u bazi	Točnost (Accuracy)	TP (True Positive Rate)	FP (False Positive Rate)	TN (True Negative Rate)	FN (False Negative Rate)	Preciznost (positive predictive value)
100	64,07%	65,70%	39,20%	60,80%	34,30%	77,02%
200	64,60%	66,10%	38,40%	61,60%	33,90%	77,49%
400	66,27%	67,50%	36,20%	63,80%	32,50%	78,86%
800	70,13%	70,80%	31,20%	68,80%	29,20%	81,94%
1600	77,93%	77,10%	20,40%	79,60%	22,90%	88,32%

Slika 5-26 prikazuje točnost eksperimenta. Pokazatelji točnosti su lošiji od rezultata iz prethodnih eksperimenata. Razlog je subjektivnost i nedostatak stvarnih klasificiranih podataka.



Slika 5-26. Točnost kroz eksperimente praćenja sustava na temelju rizika (100-1600 uzoraka)

Pogrešno predviđeni pozitivni i negativni uzorci u ovisnosti o broju klasificiranih podataka prikazani su na sljedećim slikama (Slika 5-27).



Slika 5-27. Pogrešno predviđeni pozitivni i negativni uzorci (FPR i FNR) u eksperimentu praćenja sustava na temelju rizika (100-1600 uzoraka)

Sukladno rezultatima pogrešno predviđenih pozitivnih i negativnih uzoraka, pokazatelj preciznosti odluka iznosi 88% za najveći broj uzoraka od 1600.

5.8.11. Simulacija praćenja parametara unutar samo jedne kategorije resursa

Odluke temeljem procjene vjerojatnosti događaja nastavno praćenim parametrima unutar jedne kategorije (Tablica 5-15) su dobivene odabirom kategorije sklopovlja. Eksperiment je proveden na identičan način kao i prethodni.

Tablica 5-15. Kategorizirani rizici u eksperimentu

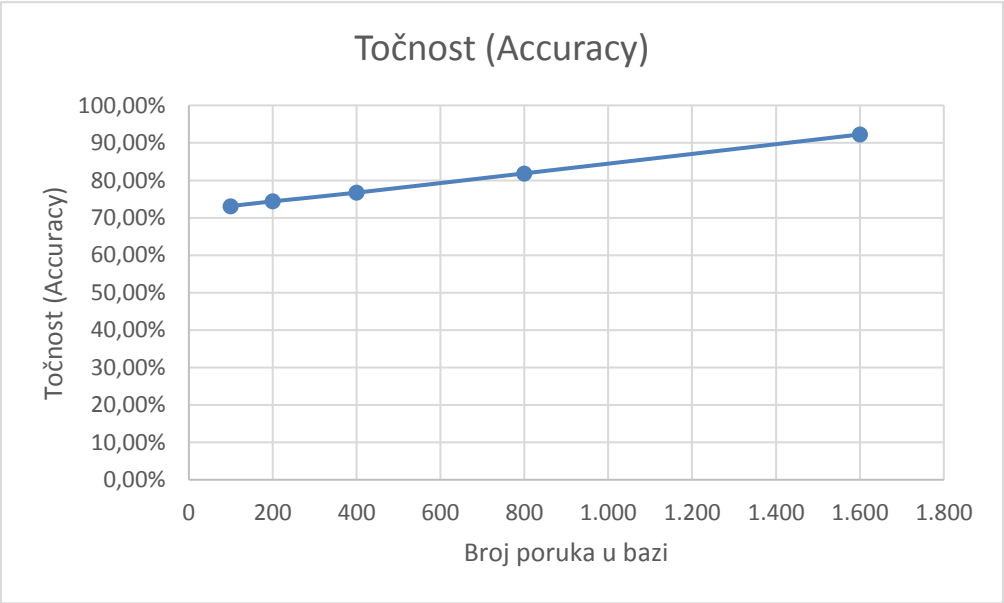
Kategorija	Nepovoljni	Povoljni	Vjerojatnost	Odluka
Obrada	2785	15286	29,83%	OK
Sklopovlje	1119	6815	40,18%	OK
Podaci	1726	9166	29,68%	OK

Tablica 5-16 prikazuje pokazatelje ispravnosti odluka u eksperimentu praćenja stanja informacijskog sustava korištenjem baze znanja koja sadrži samo jednu kategoriju resursa (hardver).

Tablica 5-16. Rezultati simulacije praćenja parametara unutar samo jedne kategorije resursa

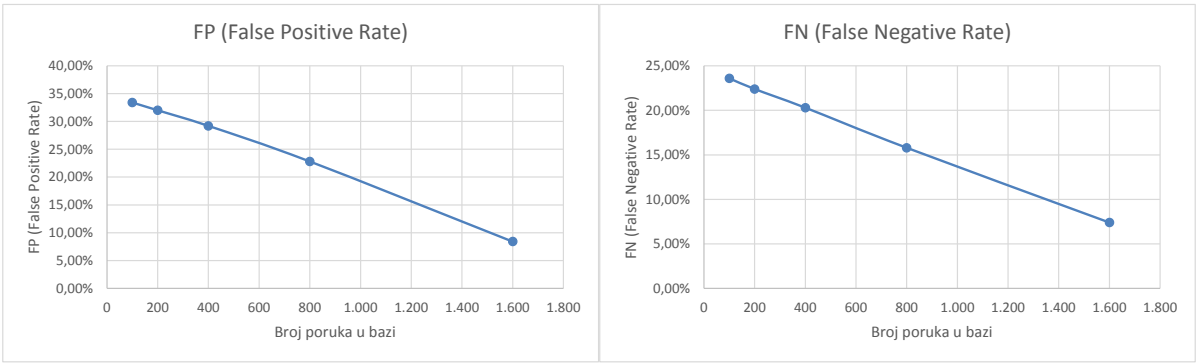
Broj poruka u bazi	Točnost (Accuracy)	TP (True Positive Rate)	FP (False Positive Rate)	TN (True Negative Rate)	FN (False Negative Rate)	Preciznost (positive predictive value)
100	73,13%	76,40%	33,40%	66,60%	23,60%	82,06%
200	74,40%	77,60%	32,00%	68,00%	22,40%	82,91%
400	76,73%	79,70%	29,20%	70,80%	20,30%	84,52%
800	81,87%	84,20%	22,80%	77,20%	15,80%	88,08%
1600	92,27%	92,60%	8,40%	91,60%	7,40%	95,66%

Slike u nastavku prikazuju rezultate iz tablice (Tablica 5-16) u ovisnosti o broju podataka u bazi znanja (Slika 5-28). Eksperiment je proveden uz korištenje jednakog broja podataka u bazi znanja, ali uz praćenje događaja na istoj kategoriji resursa.



Slika 5-28. Točnost kroz eksperimente unutar samo jedne kategorije resursa

Pogrešno predviđeni pozitivni i negativni uzorci su prikazani na slikama (Slika 5-29)



Slika 5-29. Pogrešno predviđeni pozitivni i negativni uzorci (FPR i FNR) u simulaciji praćenja parametara unutar samo jedne kategorije resursa

Zaključak ovog eksperimenta je najoptimalnije korištenje modela i to u ograničenom okruženju. Pokazatelj preciznosti odluka je 95%, što je do sada najbolji rezultat. Sljedeći eksperiment će pokazati rezultate scenarija mjerenja pri postavkama odabranim prema najbolje dobivenim pokazateljima točnosti.

5.9. Primjena modela za procjenu vjerojatnosti neželjenog događaja u scenariju najboljih rezultata

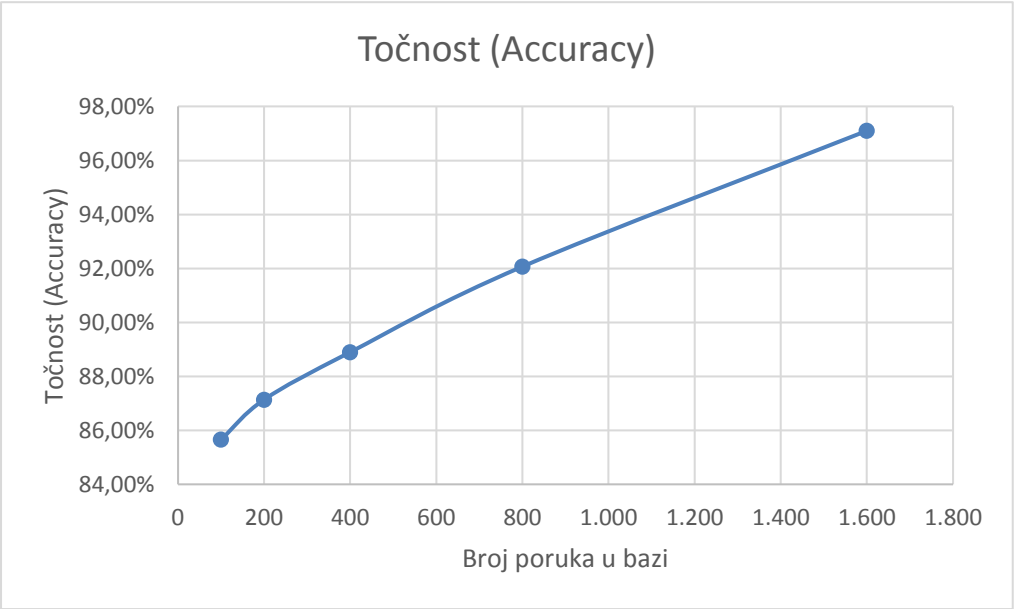
Analizom dosadašnjih rezultata zaključeno je da pozitivni statistički parametri rastu s povećanjem broja podataka u bazi znanja i općenito pokazatelji kvalitete upućuju na ispravnije rezultate prilikom korištenja modela u sustavima poznatih okruženja.

Dodatno je proveden eksperiment detekcije neželjenih razgovora na Facebook diskusijskoj grupi uz korištenje baze znanja od 100 do 1600 klasificiranih poruka. Odabir manjeg broja podataka je razlogom nedostatka dovoljnog broja klasificiranih poruka. Želja je pokazati veću važnost implementacije modela u poznato okruženje i u sustav u kojemu je jasno određen događaj (u ovom slučaju poruka na komunikaciji unutar diskusijske grupe). U tablici Tablica 5-17 prikazani su rezultati simulacije uz korištenje najboljih scenarija.

Tablica 5-17. Rezultati simulacije scenarija najboljih rezultata

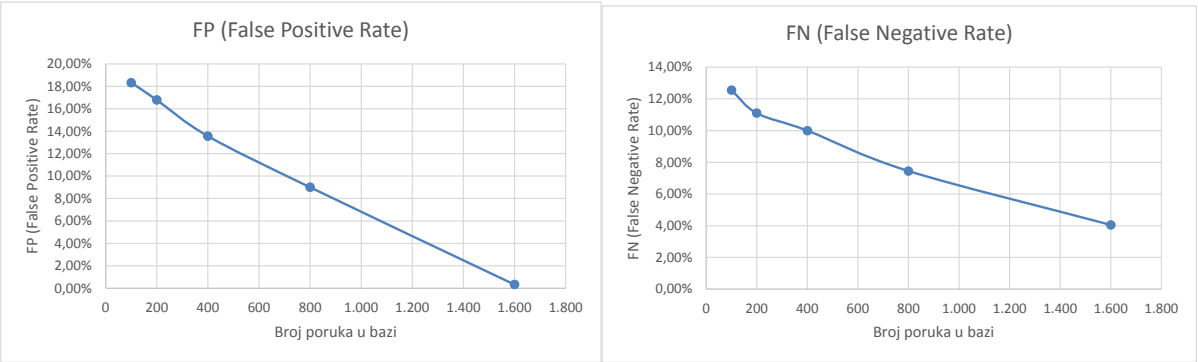
Broj poruka u bazi	Točnost (Accuracy)	TP (True Positive Rate)	FP (False Positive Rate)	TN (True Negative Rate)	FN (False Negative Rate)	Preciznost (positive predictive value)
100	85,66%	87,45%	18,33%	81,67%	12,55%	91,38%
200	87,14%	88,90%	16,78%	83,22%	11,10%	92,17%
400	88,90%	90,00%	13,56%	86,44%	10,00%	93,65%
800	92,07%	92,55%	9,00%	91,00%	7,45%	95,81%
1600	97,10%	95,95%	0,33%	99,67%	4,05%	99,84%

Rezultati ukazuju na najveću dosadašnju točnost i to u vrijednosti od preko 99% za slučaj s 1600 poruka (Slika 5-30)

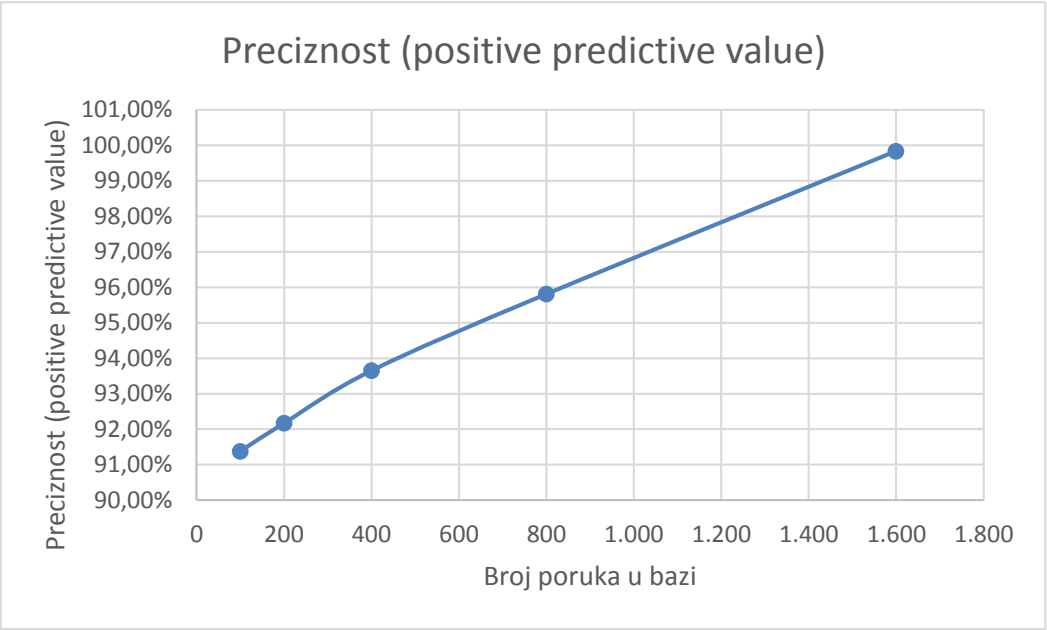


Slika 5-30. Točnost kroz eksperimente u simulaciji najboljih rezultata

Pogrešno predviđeni pozitivni i negativni uzorci ovog eksperimenta prikazani su na slikama (Slika 5-31).



Slika 5-31. Pogrešno predviđeni pozitivni i negativni uzorci (FPR i FNR) uz najbolje rezultate



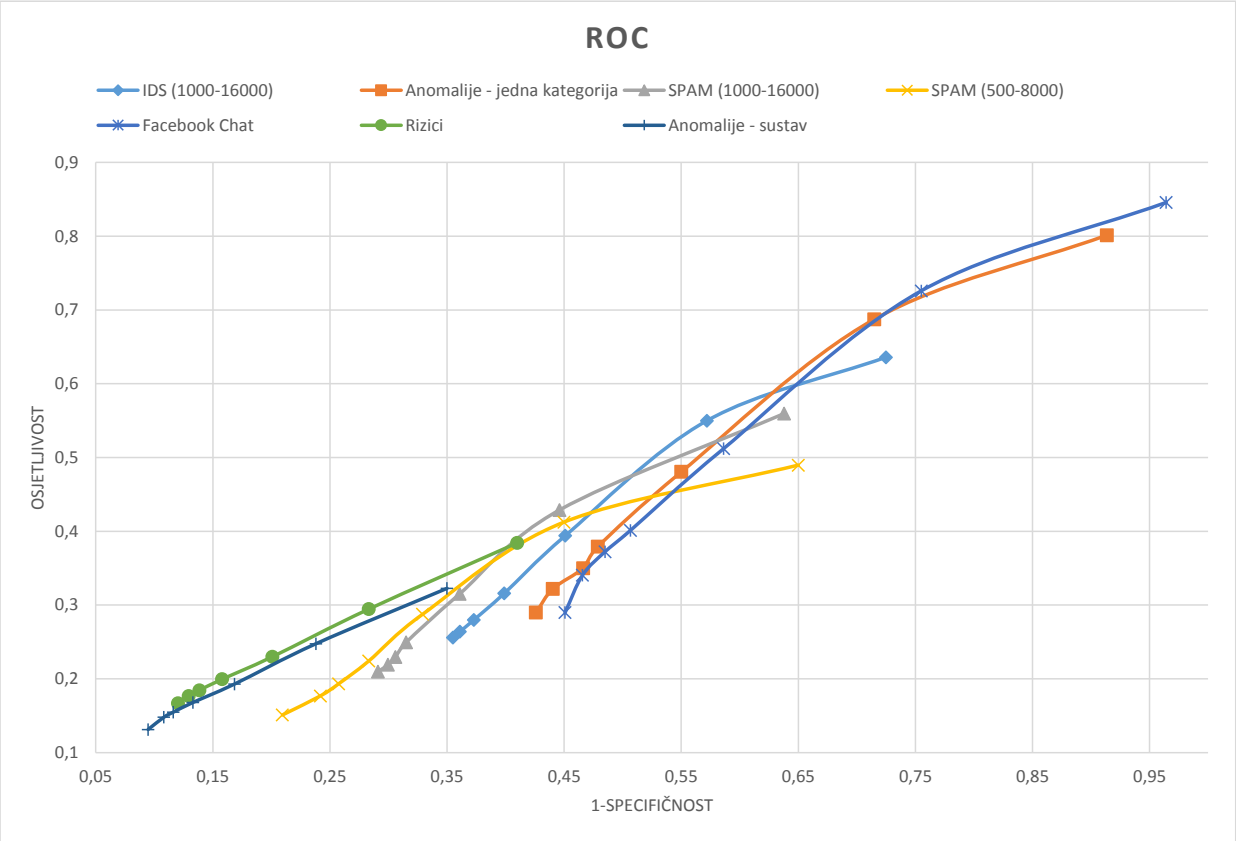
Slika 5-32. Pokazatelj preciznosti uz najbolje rezultate

Preciznost odluke je očekivano najveća (99%) u eksperimentu uz korištenje najbolje mjerenih okruženja. Pretpostavka je da je visoka preciznost modela u eksperimentu dobivena iz više razloga:

- korišteno je poznato okruženje,
- događaj je definiran dolaskom nove poruke,
- u razmjeni poruka je sudjelovao isti skup osoba,
- sadržaj poruka je bio sastavljen sintaksom na temelju koje je definirana baza znanja.

5.10. Usporedba rezultata svih eksperimenata

Slika 5-33 prikazuje usporedbu ROC krivulja koje prikazuju pokazatelje kvalitete odluke svih eksperimenata.



Slika 5-33. ROC krivulje u usporedbi svih rezultata

Na slici su vidljivi najbolji rezultati u gornjem desnom kvadrantu dijagrama. Eksperiment otkrivanja upada (anomalija) na računalnoj mreži polučio je najlošije rezultate. Konsolidirani prikaz rezultata najbolje opisuje već donesene zaključke. Model predložen u radu je moguće koristiti kao alat za podršku odlučivanju od kojega je objektivno očekivati visokokvalitetne procjene. Ograničenja modela su lošiji rezultati u nepoznatim okruženjima i pri modeliranju procesa koji se sastoji od raznovrsnih parametara. Model daje najbolje rezultate u manjem okruženju u kojemu se prate istovrsni parametri. Ovaj pristup izrade modela je sukladan već postojećim rješenjima s kojima su rezultati uspoređivani. Procjena rizika je prikazana usporedno s radom modela iz razloga sličnosti u pristupu problemima.

Na rezultatima svih eksperimenata su provedene usporedbe s rješenjima koja služe za istu svrhu i rezultati su vrednovani pomoću statističkih pokazatelja točnosti. Model nije razvijen u svrhu ugradnje u određeno područje unutar upravljanja informacijskom i komunikacijskom tehnologijom već je razrađen za općenitu upotrebu u sustavima gdje se proizvodi velika količina podataka i korisno je poznavati vjerojatnost ostvarenja neželjenih događaja. Vrednovanje se ne provodi usporedbom s referentnim modelom za sličnu ili istu upotrebu jer nisu pronađeni postojeći modeli čije su osobine i svrha istovrsni ovome modelu.

5.11. Primjer implementacije

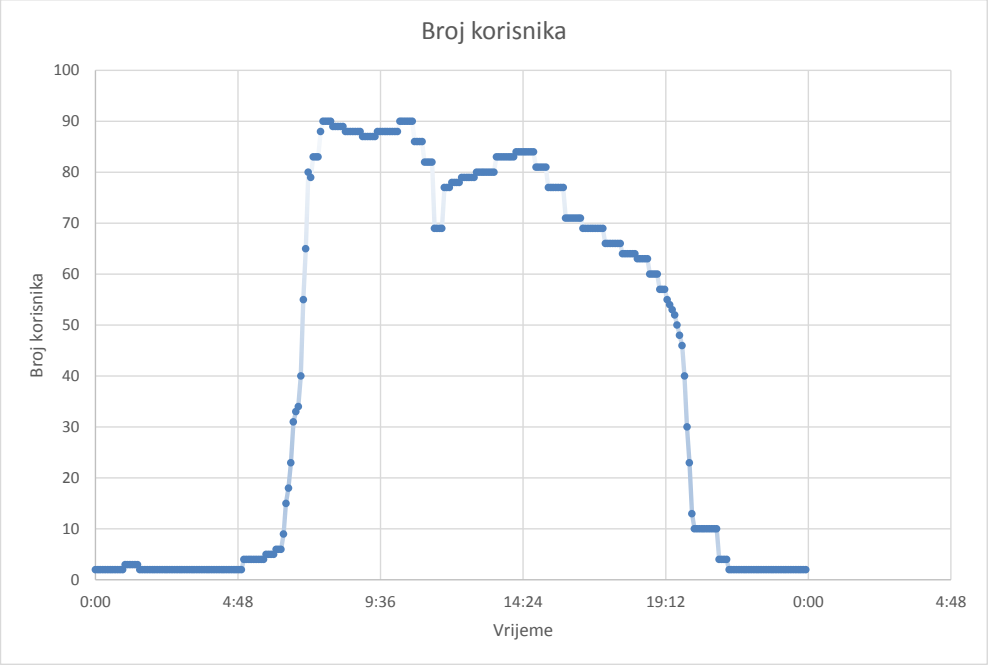
Primjer implementacije opisuje slijed aktivnosti potrebnih za ugradnju modela u realni informacijski sustav. Dodatno, opisan je algoritam rada dodatno razvijenih svojstava modela u kojima se provodi procjena rizičnosti korisnika prilikom upravljanja pristupom internetskom sadržaju.

5.11.1. Proces ugradnje modela u sustav upravljanja pristupom aplikacijskom poslužitelju

U nastavku je opisan primjer implementacije modela u sustav praćenja količine prijavljenih korisničkih računa na aplikacijskom poslužitelju i poslužitelju baze podataka. Cilj rada ovoga modela je procijeniti vjerojatnost potencijalne prijevare i curenja podataka iz poslovnog sustava kojemu pristupaju djelatnici tvrtke i vanjski korisnici putem Interneta. Model radi na principu izračuna vjerojatnosti događaja koristeći Bayesov teorem na temelju podataka o količini istovremeno prijavljenih korisnika u povijesti. Okidači za događaj su definirane razlike od prosječnih vrijednosti broja istovremeno prijavljenih korisnika u određeno doba dana. Povijest operativnih i sistemskih zapisa je duga i postoji veliki broj podataka. Prikazan je dijagram distribucije broja korisničkih računa. Prema dijagramu koji prikazuje broj korisničkih računa u ovisnosti o vremenu moguće je primijetiti devijacije u vrijednostima koje nisu točne (slučajevi pogrešnih mjerenja, „zamrznuti računi“, blokade aplikacije, itd.). Ovi slučajevi se algoritmom dojavljuju i eksperti provode odluke o ekstremnim vrijednostima.

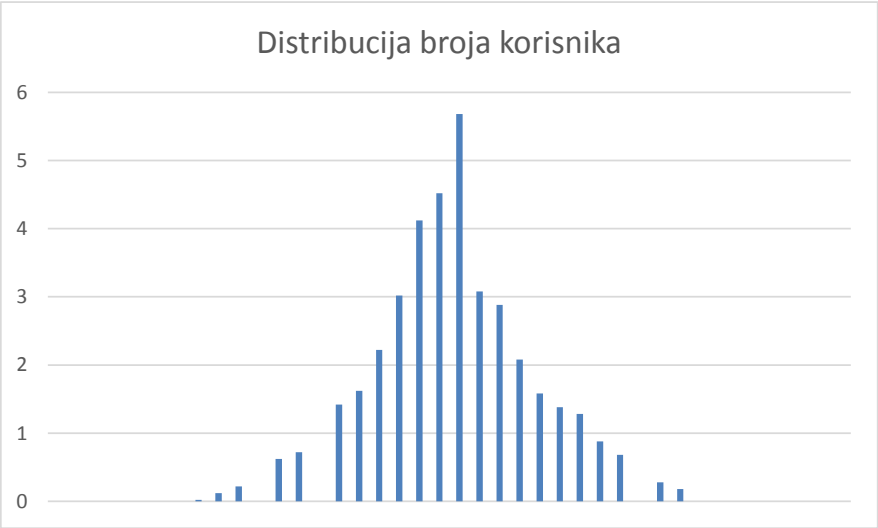
Primjer je prikazan u obliku hodograma tijeka projekta implementacije modela u postojeći sustav. Potrebno je navesti sve aktivnosti, osoblje i opremu potrebne za provođenje projekta.

Slika 5-34 prikazuje rasipanje parametara testnog primjera implementacije modela. Model može biti konfiguriran u ovisnosti o želji klijenta ili tvrtke koja ugrađuje model u svoje sustave. Navedeni primjer je zamišljen kao model procjene vjerojatnosti pogrešaka u sustavu prijavljivanja i rada korisnika na aplikacijskom poslužitelju i poslužitelju baze podataka. Model je u stanju otkrivati događaje kao što su prijevara (višestruki pristup određenim klasificiranim podacima), napadi poput distribuiranih gubitka usluge itd.



Slika 5-34. Rasipanje i distribucija parametara testnog primjera implementacije modela

Rezultati statističke analize uz korištenje odbacivanja hipoteza izvan definiranog opsega distribucije prikazani su na dijagramu (Slika 5-35). budući da događaj nije eksplicitno određen, ovdje je poželjno implementirati tehniku usporedbe aktivnosti korisničkih računa s normalnom distribucijom utvrđenom iz zapisa.



Slika 5-35. Distribucija broja istovremeno prijavljenih korisničkih računa

Hodogram implementacije opisanog primjera naveden je u koracima s pripadajućim opisom (Tablica 5-18):

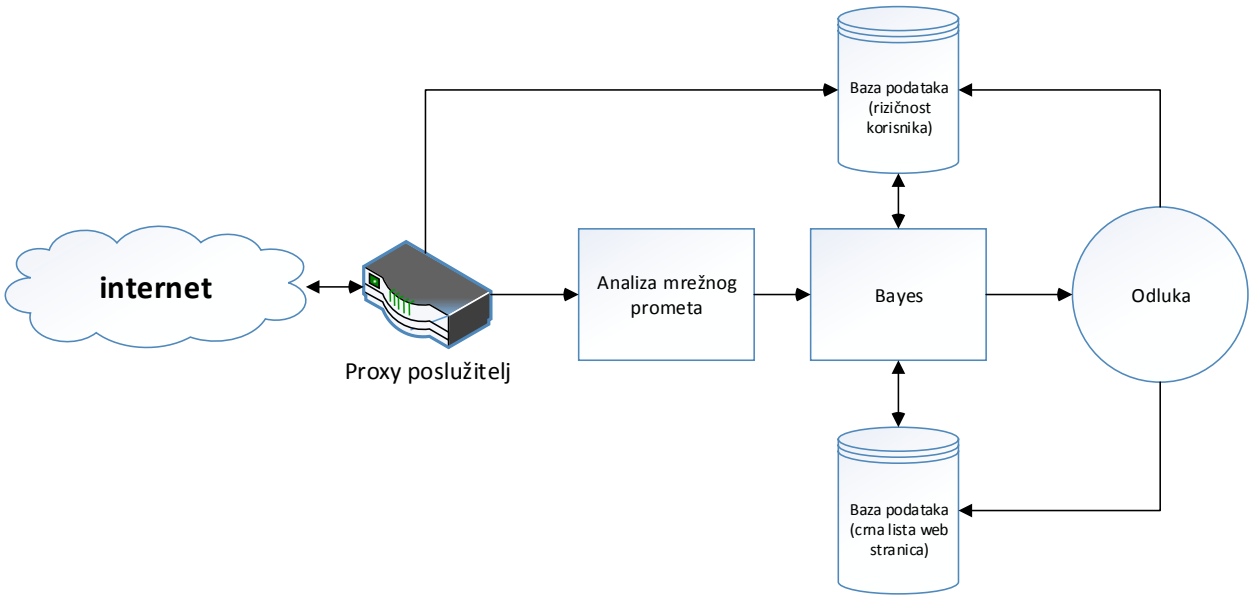
Tablica 5-18. Hodogram implementacije modela u primjeru

KORAK	OPIS
1. Utvrđivanje opsega	Opseg utvrđen u scenariju je određen praćenjem dinamike rada korisnika na aplikaciji i bazi podataka
2. Definiranje događaja i okidača	Događaj određuje okidače temeljem kojih se provodi izračuna vjerojatnosti. U navedenom primjeru to je definirana razlika broja korisnika od statistički utvrđene razine u određeno doba dana, tjedna, mjeseca, godine.
3. Parametrizacija baze podataka	Bazu podataka čine sistemski i operativni zapisi koji već postoje u arhivama administracije sustava. Korisno je poznavati ishode određenih scenarija određenih vrijednostima parametara.
4. Definiranje i postavljanje agenata	Agente mogu predstavljati postojeći alati i skripte za upravljanje bazama podataka. Način definiranja korisničkih računa na

KORAK	OPIS
	aplikativnom poslužitelju određuje i načine praćenja trenutnih vrijednosti.
5. Puštanje modela u rad u učenje	Definiranjem svih prethodnih vrijednosti model je spreman za ispitivanje, a nakon pozitivnih pokazatelja uspješnosti i za produkcijski rad.

5.11.2. Algoritam rada modela pri upravljanju pristupom internetskom sadržaju

Veliki broj ranjivosti kojima su ugroženi današnji informacijski sustavi povezani su s internetom i pristupom korisnika različitim sadržajima. Proces opisan u poglavlju 5.11.1 moguće je proširiti s svojstvom upravljanja pristupom internetskom sadržaju. Na slici (Slika 5-36) prikazan je primjer algoritma rada modela u načinu rada za upravljanje pristupom internetskom sadržaju.



Slika 5-36. Primjer korištenja modela u svrhu upravljanja pristupom internetskom sadržaju uz procjenu rizičnosti korisnika

Pored standardnog svojstva upravljanja pristupom uz pomoć crnih lista (engl. *blacklist*) dodana je i osobina modela za izračunavanje vjerojatnosti neželjenih događaja s obzirom na rizičnost

korisnika. Crne liste često nisu prihvatljive jer sadrže veliku količinu domena, a bijele liste (engl. *whitelist*) predstavljaju radikalni način kontrole i ograničenja korisnika. U modernim informacijskim sustavima s imeničkim direktorijem (engl. *active directory*) svi korisnici pristupaju različitim sadržajima nastavno definiranim pravilima. U takvim okruženjima se često nalaze i različiti sustavi za upravljanje ovlastima. Korisnici informacijskog sustava pristupaju sadržajima preko različitih sučelja, ali uz autorizaciju. Uz poznavanje povijesti prakse korisnika i povijesti njegovog korištenja internetskog sadržaja, ali i pristupa aplikacijama, diskovima i podacima moguće je izračunavati vjerojatnost neželjenog događaja i s ovog aspekta.

Sukladno provedenim eksperimentima moguće je zaključiti da model za procjenu vjerojatnosti neželjenog događaja može biti korišten kao zamjena različitih sustava za kontrolu pristupa internetskom sadržaju, ali uz izračun pomoću Bayesovog teorema na temelju rizičnosti korisnika. Ovakav način rada opisan je algoritmom u svrhu predstavljanja prilagodljivosti modela različitim okruženjima i mogućnosti proširenja prema korisničkim zahtjevima.

6. ZAKLJUČAK

Model predložen u radu izračunava vjerojatnost neželjenih događaja u informacijskom sustavu. Rad modela je ispitan nizom eksperimenata i simulacija i izračunate su vrijednosti statističkih pokazatelja ispravnosti odluka. Eksperimenti su osmišljeni kako bi pratili scenarije ispitivanja s ciljem otkrivanja najboljih kombinacija u kojima model daje najtočnije odluke.

Optimalna količina klasificiranih podataka potrebna je za izračun vjerojatnosti neželjenog događaja. Točan izračun je onaj čiji su pokazatelji valjanosti unutar opsega prihvaćenih vrijednosti. Statističkim metodama su evaluirani rezultati rada modela u stvarnim okruženjima i u simulacijama.

Načini korištenja modela su ispitani u tri različita okruženja: otkrivanje neželjenih poruka, neželjenih upada ili anomalija i za praćenje rada informacijskog sustava temeljem identificiranih rizika.

Za implementaciju modela podrazumijeva se okruženje poznatih sustava i okolnosti. Potrebno je poznavati sustav gdje je potrebno ugraditi model koji će procjenjivati vjerojatnost neželjenih događaja. Eksperimentima je dokazano je da se pri boljem poznavanju sustava i njegovih parametara dobivaju bolji rezultati i veća točnost od rezultata dobivenih pomoću alata razvijenih u istu svrhu kao i prilagođeni model u pojedinom eksperimentu.

Kvalitetno odabrani parametri su vrlo važan dio metode, jer oni opisuju događaj koji može biti neželjen ili prihvatljiv. Na ovaj način, odnosno kvalitetnom parametrizacijom se izbjegavaju i neželjeni učinci nepravilnog odlučivanja.

Definicija događaja je jedna od temeljnih aktivnosti pripreme rada modela. Eksperimentima su obuhvaćeni scenariji u kojima je događaj bio definiran unutar samog procesa i oni u kojima su događaji bili slučajne varijable. Primjerom implementacije pokazano je da su definicija događaja i okidača od ključne važnosti za projekt i rad modela.

Metodologija procjene rizika je najlakši početak uspostave upravljanja rizicima informacijskih sustava unutar kojega se metodološki upravlja svim potrebnim parametrima zahtijevanim od strane modela. Opisana metodologija upravljanja rizicima je usklađena s prihvaćenim načinima u praksi. Srodnost u načinu rada vidljiva je kroz principe provođenja aktivnosti u metodologijama

upravljanja rizicima, gdje je potrebno baviti se vjerojatnostima ostvarenja rizika, a time i prijetnji i ranjivosti.

Cijene implementacije sustava za podršku odlučivanju, upravljanja rizicima, otkrivanja i prevencije neželjenih upada, otkrivanja prijevara i raznih drugih sustava koji ne objedinjuju različita područja primjene vrlo su visoke. Također, ovi sustavi zahtijevaju sudjelovanje stručnog osoblja u radu i svakodnevnom održavanju. Predloženi model je moguće implementirati na različite načine: od pristupa u kojemu se provodi potpora odlučivanju i ukazivanju na rizike, pa do naprednih oblika modela u kojima je moguće implementirati logičke preventivne mehanizme.

Informacijski sustav je pojam koji obuhvaća sustave koji obrađuju podatke, upravljaju informacijama i može podrazumijevati široki spektar područja. Eksperimentima su obuhvaćeni sustavi u kojima je događaj jasno određen i ovisi o definiranom subjektu koji može biti okidač za analizu i procjenu, ali i sustavi u kojima se stanje parametara kontinuirano prati i nema jasne definicije događaja. U tim slučajevima korištene su statističke metode praćenja distribucije parametara i događaj može biti definirana razlika od prosječne vrijednosti. Rezultati dobiveni ovakvim pristupom su sukladni rezultatima rada modela pri analizi u prethodnim eksperimentima.

Algoritam rada koji se temelji na agentskom načinu rada u informacijskim sustavima uvelike povećava područja primjene modela. Poslovni i informatički sustavi zajedno čine skupinu koju možemo nazvati informacijski sustavi. Uporaba modela u poslovnim sustavima je prikazana u dijelu praćenja informacijskog sustava na temelju rizika sadržanih u bazi podataka. Slučajnim odabirom kombinacija parametara generirani su scenariji koje je model ocjenjivao. Primjena modela je prikladna za sustave otkrivanja rizičnog ponašanja korisnika informacijskog sustava i otkivanja prijevara. Takvi sustavi imaju jasno definirane točke u kojima su identificirani rizici koji mogu biti iskorišteni, a model je potencijalna kontrolna i preventivna mjera.

Dokazana točnost rezultata modela u smislu predloženih odluka ukazuje na mogućnosti korištenja ovakvog pristupa u svim organizacijama koje, bilo iz zakonskih ili regulatornih obveza, ali isto tako i iz obaveza koje slijede iz svijesti o informacijskoj sigurnosti imaju potrebu implementirati sustav koji upravlja informacijskom sigurnošću. Dodatna korist je mogućnost uključenosti eksperata u rad sustava. Ekspert kao osoba koja posjeduje određena saznanja i iskustva može i treba biti dio modela za procjenu vjerojatnosti neželjenih događaja. Eksperti su korišteni u ispitivanju modela i to u evaluaciji rezultata ispitivanja gdje su ocjenjivali sukladnost rezultata i svojih mišljenja o kombinacijama parametara.

Učenje je područje najvećeg rasta u upravljanju informacijskim sustavima. Funkcionalnost učenja podrazumijeva jedan široki spektar nazvan umjetna inteligencija [72]. Predloženi model u ovome radu sadrži samo manji dio cjeline umjetne inteligencije jer je učenje predloženo i realizirano samo pomoću povećanja količine ispravno klasificiranih parametara. Nizom eksperimenata su prikazani učinci dobiveni različitom količinom informacija u bazi podataka i učinci dobiveni različitim informacijama u smislu kvalitete klasifikacije. Preporuka je koristiti ispravno klasificirane informacije, odnosno događaje koji mogu biti kvantitativno ocijenjeni, ali u pozadini mora postojati metodologija procjene rizika koja rezultira odgovarajućim podacima.

Razina svijesti je segment informacijske sigurnosti koji zauzima veliki dio cjelokupnog područja djelovanja i prevencije. Procjenom rizika, odnosno procesom koji zahtjeva analizu svih prijetnji i ranjivosti i analitičku obradu parametara moguće je proširiti razinu svijesti svih osoba uključenih u upravljanje informacijskim sustavom.

Prednosti predloženog modela procjene vjerojatnosti neželjenih događaja su jednostavnost koja je čitljiva iz prikaza samog algoritma modela. Cijena implementacije modela nije visoka i ne zahtjeva nužno nabavku nove opreme. Svi eksperimenti su provedeni u mrežnom okruženju i korištenjem besplatnih alata. Pretpostavka je da se upravljanje informacijskim i komunikacijskim sustavim u današnje vrijeme provodi na moderan način, a često je to i zakonski ili regulatorno određeno. U tim slučajevima baze već sadrže velike količine klasificiranih podataka. Model je fleksibilan i kroz eksperimente je pokazano da ga je moguće ugraditi u različita okruženja. Posebno je zanimljiva mogućnost implementacije modela u sve opsege poslovnih djelatnosti koja su poduprta informacijskom i komunikacijskom tehnologijom. Načini rada su ovdje nebrojeno puta veći i model je moguće primijeniti kao alat za procjenu vjerojatnosti događaja koji su povezani sa socijalnim i srodnim aktivnostima (prijevare, curenje informacija, krađa informacija, itd.). Modularnost je osobina koja odlikuje model, što je i objašnjeno kroz niz eksperimenata i na kraju u testnom primjeru. Mogućnost sudjelovanja eksperta u svim fazama je prednost modela, ali i autonomija u radu prilikom dosezanja prihvatljive razine točnosti. Definirani su načini mjerenja učinkovitosti. Model ne opterećuje resurse i koristi postojeću infrastrukturu.

Nedostaci modela su nedostatak inicijalnog znanja (podataka) u nekim specifičnim slučajevima implementacije. Rješenje za ovaj nedostatak je ugradnja modela u manjim opsezima. Neophodno sudjelovanje eksperata u početnoj fazi kod nedostatka dovoljne količine znanja je i prednosti i mana, jer se često kod implementacija sustava zaštite očekuje potpuna autonomija u radu. Model je uspoređivan s postojećim sustavima za otkrivanje neželjenih upada upravo iz razloga što takvi

sustavi često zahtijevaju početni period učenja u kojemu nisu potpuno autonomni. Velike pogreške su izračunate u radu s malim brojem podataka ili u scenarijima koji ne odgovaraju u potpunosti preporukama i stoga su u ovome radu provedeni eksperimenti i doneseni zaključci o optimalnom korištenju modela. Model ima ograničenja u opsegu implementacije, odnosno ne preporuča se ugradnja modela u rad velikih sustava unutar kojih se provodi praćenje velike količine podataka u kratkom vremenu, odnosno u dinamične sustave. Velika količina obrađenih podataka čini sustav preciznijim i baza podataka se u takvim slučajevima može koristiti za procjene u manjim okruženjima. Preporuka je koristiti manje opsege i svakako poznata okruženja.

6.1. Opis znanstvenih doprinosa

U radu je preložen model za predviđanje neželjenog događaja u informacijskom sustavu zasnovanog na Bayesovom teoremu. Model se temelji na korištenju Bayesovog teorema i predviđen je za ugradnju u informacijske i komunikacijske sustave s upravljanjem zapisima. Pretpostavka je da se u današnjim informacijskim sustavima pohranjuju velike količine zapisa, a često je to i zakonski ili regulativno zahtijevano. Dokazano je da model ostvaruje rezultate u skladu s postojećim modelima koji služe u istu ili sličnu svrhu.

Predloženo je i korištenja agenata u raspodijeljenom okruženju. Način rada modela se temelji na komunikaciji i izračunima vjerojatnosti u stvarnom vremenu. Korištenjem agenata bi bilo moguće preventivno reagirati u slučajevima kada je izračunata vjerojatnost dosegla neku definiranu vrijednost pri kojoj je siguran neželjeni događaj. Na ovaj način bi bilo moguće ostvariti preventivne kontrole u informacijskim sustavima.

Model je ispitan u odabranim okruženjima i dobiveni rezultati su uspoređeni s referentnim alatima razvijenim za pojedine scenarije. Odabrani eksperimenti su pokazali vrlo veliku točnost izračuna modelom i mogućnost korištenja u navedenim primjerima. Eksperimentima su ispitani načini rada modela pri različitim postavkama u smislu parametrizacije. Vrednovanje rezultata je provedeno korištenjem statističkih pokazatelja točnosti i ukazani su načini rada modela u kojemu se ostvaruju najbolji rezultati.

7. LITERATURA

[1] ISO/IEC27000, Information Security Management Systems (ISMS), 2013

[2] ISO/IEC Risk Management, 2009

[3] ISO22301 Business Continuity Management System, 2012

[4] Šamec, N., Jakupović, A.: Methods and software for estimation of information system dependability, Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014

[5] Laprie, J. C.: „Dependability of Computer Systems: from Concepts to Limits", Proceedings of the Twenty-Fifth international conference on Fault-tolerant computing, Washington: IEEE Computer Society, 42 – 54

[6] Samuel Kounev: Quantitative Evaluation of Service Dependability in Shared Execution Environments, Quantitative Evaluation of Systems, Lecture Notes in Computer Science Volume 8657, 2014, pp 1-4, 20134

[7] Sommerville, I.: Software Engineering 9th edition. Boston: Addison-Wesley, 2010

[8] Avižienis, A., Laprie, J. C, Randell, B.: „Fundamental Concepts of Dependability", University of Newcastle, 2001
www.cert.org/research/isw/isw2000/papers/56.pdf,

[9] Tervo, H., Saarelainen, M.-M., Ahonen, J.J., Sihvonen, H.: The Impact of Decision-Making on Information System Dependability, Software Engineering Advances, ICSEA '08, 2008

[10] Kenneth Miller: InformationWeek Analytics, 2010 Data Center Operational Trends, 2010

[11] McKendrick, J. (2012) „Enterprise Data and the Cost of Downtime, 2012 IOUG Database Availability Survey", 2012
http://www.oracle.com/us/products/database/2012-ioug-db-survey-l695554.pdf

[12] Schroeder, B., Gibson, G. A.: „A large-scale study of failures in high-performance computing systems", Proceedings of the International Conference on Dependable Systems and Networks. Washington: IEEE Computer Society, 249 – 258, 2006

[13] Richardson, R.: „The 12th Annual Computer Crime and Security Survey", 2007, http://gocsi.com/sites/default/files/uploads/2007_CSI_Survey_full-color_no%20marks.indd_.pdf,

[14] Shiping Chen, Nepal, S., Pandey, S.: A unified monitoring framework for distributed information system management, Computing Technology and Information Management (ICCM), 8th International Conference, 2012

[15] Zhang Sheng Pan, Jin Liang Shi, Yan Sun, Bin Bin Wei: Writing and analyzing logs in a distributed information system, US 20130290519 A1, International Business Machines Corporation, 2013

[16] Cleland, J., Dargie, H.: Guidelines for the diagnosis and treatment of chronic heart failure: executive summary (update 2005): The Task Force for the Diagnosis and Treatment of Chronic Heart Failure of the European Society of Cardiology. European Heart Journal 26, 1115 – 1140, 2005

[17] J.J. Castro-Scheza, R. Miguela, V. Herreraa, J.A. Albusac: Indeks-Based Knowledge Acquisition Using Dynamic Analysis, Applied Soft Computing, Volume 13, Issue 1, Pages 509–526, 2013

[18] Bradley, J. H., Paul, R., Seeman, E.: Analyzing the structure of expert knowledge. Information and Management, 43:77-91, 2006

[19] Petz B.: „Osnovne statističke metode za nematematičare“, Naklada Slap, 2007

[20] Vercellis C.: „Business intelligence: Dana mining and optimization for decision making“, Wiley, 2009

[21] Panian Ž., Klepac G.: „Poslovna inteligencija“, Masmedia, 2003

[22] M. Wooldrige: Intelligent Agents, In G. Weiss, editor, Multi-agent systems (second edition), page 3 – 50, MIT Press, 2013

[23] Wooldridge, M.: An Introduction to MultiAgent Systems, John Wiley & Sons, Second edition, 2009

[24] Russell S., Norvig P.: Artificial Intelligence, A Modern Aproach, Third Edition, Pearson Education Inc., New Jersey, SAD, 2010

[25] H. Gardner and L. Hall.: “Multiple Intelligences After Twenty Years.” Education. No. 617, 2003

[26] P. Russel. S.T. and Norvig: Artifficial intelligence: A modern approach (SE). Englewod Cliffs, New Jersey,: Prentice Hall, 2002

[27] M. Kononenko. I. and Kukar: Machine learning and data mining: Introduction to principles and algorithms, Chichester, UK: Honvood Publishing, 2007

[28] J. Hulle. V., Marc M. and Larsen: “Machine learning for signal processing,” Neurocomputing. Vol. 72. no. 3, 2008

[29] Y. Chen. B. Yang and A Abraham: "Flexible neural trees ensemble for stock indeks modeling", Neurocomputing, vol. 70. pp. 697-703. Oct., 2006

[30] A. E. Kliandani., A. J. Kim And A. W. Lo: "Consumer credit-risk models via machine-learning algorithms", Journal of Banking & Finance, vol. 34. no. 11, pp. 2767-2787. Nov, 2010

[31] D. Chen: "A localization verification scheme for finding text in images and video frames based on contrast independent features and machine learning methods", Signal Processing: Image Communication, vol. 19. no. 3. pp. 205-217, 2004

[32] J. W. Shin, J. H. Chang and N. S. Kim: "Voice activity detection based on statistical models and machine learning approaches." Computer Speech & Language. Vol. 24. no. 3. pp. 515-530. Jul., 2010

[33] Y. Li.: "Support vector machine based multi-view face detection and recognition," Image and Vision Computing, Vol. 22. no. 5. pp. 413-427, May. 2004

[34] C. Y. Tsai and C. C. Chiu: „A purchase-based market segmentation methodology", Expert Systems with Applications, Vol. 27. no. 2. pp. 265-276. Aug. 2004

[35] J. Dias and J. Vemiunt: "Latent class modeling of website users' search patterns: Implications for online market segmentation." Journal of Retailing and Consumer Services, vol. 14. no. 6. pp. 359-368, 2007

[36] T. S. Guzella and W. M. Caminhas: „A review of machine learning approaches to Spam filtering", Expert Systems with Applications, Vol. 36. no. 7. pp. 10206-10222. Sep. 2009

[37] Y. Li. Q. Yang, and R. Jiao: "Image compression scheme based on curvelet transform and support vector machine", Expert Systems with Applications. Vol. 37. no. 4. pp. 3063-3069, 2010

[38] W. P. Kuo. E. Y. Kim. J. Trimarchi. T. K. Jenssen, S. A. Vinterbo, L. Ohmo-Machado: A primer on gene expression and microarrays for machine learning researchers, Journal of biomedical infonnatics, Vol. 37. no. 4. pp. 293-303, 2004

[39] B. D. Argali. S. Chernova. M. Veloso. And B. Browning: "A survey of robot learning from demonstration", Robotics and Autonomous Systems, vol. 57. no. 5, pp. 469-483, 2009

[40] Tom Mitchell: Machine Learning, McGraw Hill, 1997

[41] E. Alpaydin: Introduction to machine learning, Second edition, MIT Press, 2010

[42] C. M. Bishop: Pattern recognition and machine learning, Springer, 2006

[43] Witten I. H., Eibe F., and Mark A. Hall: Data Mining: Practical Machine Learning Tools and Techniques Third_Edition, Morgan Kaufmann, 2011

[44] Hrvoje Očevčić: Kvalitativno kodiranje vremensko prostornih nizova podataka, diplomski rad, Elektrotehnički fakultet Osijek, 2002

[45] Lynn: Smart Business Intelligence Solutions with Microsoft SQL Server 2008, Microsoft Press, 2009

[46] Vercellis, Carlo: Business Intelligence: Data Mining and Optimization for Decision Making, John Wiley & Sons, 2009

[47] Stephen Marsland: Machine Learning: An Algorithmic Perspective, Second Edition, 2014

[48] Journal of the American Statistical Association, Volume 109, Issue 507, 2014

[49] Japkowicz, N., Shah, M.: Evaluating learning algorithms: A classification perspective, Cambridge University Press, New York, 2011.

[50] http://en.wikipedia.org/wiki/Receiver_operating_characteristic

[51] T. Fawcett: "An introduction to ROC analysis", Pattern Recognition Letters, vol. 27, pp. 861-874, 2006

[52] Léon Bottou: From machine learning to machine reasoning, Machine Learning, Volume 94, Issue 2, pp 133-149, 2014

[53] Paul Graham: A Plan for Spam, 2002

[54] Asmaa Shaker Ashoor, Sharad Gore: Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), Advances in Network Security and Applications Communications in Computer and Information Science Volume 196, pp 497-501, 2011

[55] Steven Sturges, Marc Norton: Speed and memory optimization of intrusion detection system (IDS) and intrusion prevention system (IPS) rule processing, US8474043 B2, 2013

[56] Secure Computing Corporation, Intrusion Prevention Systems (IPS), Part one: Deciphering the inline Intrusion Prevention hype, and working toward a real-world, proactive security solution, 2003

[57] NSS Group, Intrusion Prevention Systems (IPS), 2004

[58] Hung-Jen Liaoa, Chun-Hung Richard Lina, Ying-Chih Lina, Kuang-Yuan Tung: Evolution of IDS, Journal of Network and Computer Applications, Volume 36, Issue 1, Pages 16–24, 2013

[59] Network Intrusion Prevention Systems, http://www.networkintrusion.co.uk/inline.htm, 2005

[60] Host Intrusion Prevention Systems, http/www.networkintnision.co.uk/hios.htm, 2005

[61] Stefan Creemers, Erik Demeulemeester, Stijn Van de Vonder: A new approach for quantitative risk analysis, Annals of Operations Research, 2014

[62] Nan Feng, Minqiang Li: An information systems security risk assessment model under uncertain environment, Applied Soft Computing, Volume 11, Issue 7, Pages 4332–4340, 2011

[63] Meng Meng: The research and application of the risk evaluation and management of information security based on AHP method and PDCA method, Information Management, Innovation Management and Industrial Engineering (ICIII), 6th International Conference, 2013

[64] J. M. Bernardo. A. F. M. Smith: Bayesian Theory, Wiley, ISBN 0-471-12104-5, 1996

[65] Shilpi Gupta, Roopal Mamtora: IntIntrusion Detection System Using Wireshark, National Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 11, November, 2012

[66] Renalda Kushe, Adrian Shehu: Intrusion Detection With Snort, Academic Journal of Science, 2013

[67] Mrutyunjaya Panda, Manas Ranjan Patra: Network Intrusion Detection Using Naive Bayes, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.12, 2007

[68] Viviana Molano, Carlos Cobos, Martha Mendoza, Enrique Herrera-Viedma, Milos Manic Viviana Molano, Carlos Cobos, Martha Mendoza, Enrique Herrera-Viedma, Milos Manic: Feature Selection Based on Sampling and C4.5 Algorithm to Improve the Quality of Text Classification Using Naïve Bayes, Human-Inspired Computing and Its Applications, Lecture Notes in Computer Science Volume 8856, pp 80-91, 2014

[69] Charu C. Aggarwal, ChengXiang Zhai: Mining Text Data, Springer Science & Business Media, 2012

[70] Senol Isci, Haluk Dogan, Cengizhan Oztur, Hasan H. Otu: Bayesian network prior: network analysis of biological data using external knowledge, Oxford JournalsScience & Mathematics Bioinformatics Volume 30, Issue 6Pp. 860-867, 2013

[71] Max Henrion: Practical Issues in Constructing a Bayes' Belief Network, Artificial Intelligence (cs.AI), 2013

[72] Rodney W. Johnson: Independence and Bayesian Updating Methods, Artificial Intelligence (cs.AI), 2013

[73] Judea Pearl: Bayesian networks, Department of Statistics Papers, Department of Statistics, UCLA, 2011

[74] V. Cherkassky and Y. Ma. „Another look at statistical learning theory and regularization“ Neural networks: the official journal of the International Neural Network Society, vol. 22, no. 7. pp. 958-69. Sep. 2009

[75] Kevin Mitnick, William L. Simon: The Art of Deception, 2003

[76] E. Dubrova: Fault-Tolerant Design, DOI: 10.1007/978-1-4614-2113-9_2, Springer Science+Business Media, New York, 2013

8. SAŽETAK

Upravljanje sigurnošću informacijskih sustava je vrlo važan segment upravljanja tvrtkama u cijelosti. Količina podataka koja se svakodnevno obrađuje, a i pohranjuje se povećava i često istovremeno postaje i prednost i nedostatak. Takvi podaci često služe samo za forenzičke analize. Cilj ovoga rada je iskoristiti podatke koji se pohranjuju u informacijskim sustavima izgradnjom modela za izračun vjerojatnosti budućeg događaja. Događaj je prema tezi rada često određen parametrima iz okruženja koji svojim intenzitetom mogu utjecati na ishod događaja i razinu njegovog utjecaja na informacijski sustav. Korišten je Bayesov teorem pomoću kojega je moguće izračunati vjerojatnost ostvarenja događaja na temelju vjerojatnosti praćenih parametara.

U radu su prikazani rezultati eksperimenata u kojima su ispitivani načini rada modela unutar različitih okruženja. Cilj je pronaći optimalan način rada modela i definirati uvjete koji trebaju biti ispunjeni za postizanje željenih rezultata. Rezultati su predstavljeni kroz ispravne prijedloge odluka na temelju kojih je moguće poduzimati korektivne i preventivne aktivnosti.

Evaluacija rezultata eksperimenata je također provođena na različite načine. Rezultati simulacija čije je rezultate moguće usporediti s pripadajućim sustavom ili alatom su evaluirani usporedbom s referentnim rezultatima. Evaluacije su provođene i usporedbom s mišljenjem eksperata iz područja upravljanja informacijskim sustavima. Svi rezultati su na jednak način ocijenjeni pomoću pokazatelja točnosti.

Model predstavljen u radu je moguće koristiti u opisanim okruženjima, ali i kao modul u većim ekspertnim sustavima gdje je potrebno nadzirati određene sustave kroz praćenje parametara iz okruženja. Agentski način rada je prednost jer omogućava upravljanje sustavima u stvarnom vremenu.

Najveća prednost modela je mogućnost primjene u različitim okruženjima što ne znači nužno unutar upravljanja informacijskim sustavima nego i poslovnim i socijalnim osobinama sustava koji su pogonjeni informacijskom i komunikacijskom tehnologijom.

Ključne riječi: Upravljanje informacijskim sustavima, Bayesov teorem, uvjetna vjerojatnost, događaj, odlučivanje, agenti

9. ABSTRACT

Security management of information systems is a very important part of the company management in entirety. The amount of data to be processed and stored every day is increasing and often at the same time becomes an advantage and a disadvantage. Data are used either only for forensic analysis or not used at all. The aim of this paper is to use data stored in information systems to propose a model for calculating the probability of future events. The event regarding the thesis of the paper is often determined by the parameters of the environment whose intensity can affect the outcome of the event and its impact on information systems. The Bayes' Theorem is used by which it is possible to calculate the probability of realization of events based on probability of monitored parameters.

The paper presents the results of experiments in which they studied modes of models within different environments. The goal is to find the optimal way of working and define conditions that must be met to achieve the desired results. Results are presented through proper draft decisions on the basis of which it is possible to take corrective and preventive actions.

Evaluation of results is also performed in different ways. The results of simulations whose results can be compared with the corresponding system or tools are evaluated by comparison with reference results. Evaluations are conducted also through comparison with the opinion of experts in the field of management information systems. All results are equally evaluated using accuracy indicators.

The model presented in this paper can be used in the described environments, as well as a separate module in larger systems where it is necessary to monitor certain systems through monitoring the parameters of the environment. Agent mode is advantageous because it allows managing systems in real time.

The biggest advantage of the model is the possibility of application in different environments but not necessarily within the management of information systems but also business and social characteristics of systems that are driven by information and communication technology.

Key words: Information systems management, Bayes theorem, conditional probability, event, decision, agents

10. ŽIVOTOPIS

Hrvoje Očevčić rođen je 2. kolovoza 1977 godine u Vinkovcima gdje živi i radi. Nakon srednje tehničke škole, elektrotehničkog smjera nastavlja obrazovanje na Elektrotehničkom fakultetu u Osijeku, smjer elektronika i automatizacija. Dobitnik je Rektorove nagrade za diplomski rad izrađen pod mentorstvom prof.dr.sc. Franje Jovića i naziva „Kvalitativno kodiranje vremensko-prostornih nizova podataka“.

Nakon diplomiranja zapošljava se u tvrtki Dilj d.d. u Vinkovcima gdje radi kao inženjer na održavanju automatiziranih postrojenja. Nakon akvizicije tvrtke u Nexe Grupu, radi kao sistemski inženjer na implementaciji i održavanju informacijskih sustava u sklopu Nexe grupe.

Zapošljava se u Slavonskoj banci d.d. Osijek koja je u međuvremenu pripojena većem bankarskom sustavu Hypo Alpe-Adria-Bank d.d. gdje radi prvo kao voditelj sigurnosti informacijskih sustava, a zatim kao viši unutarnji revizor informacijskih sustava.

Na Elektrotehničkom fakultetu u Osijeku radi od 2004. godine kao vanjski suradnik na kolegijima: Električna mjerenja, Informacija i informacijski sustavi, Informacijski sustavi i kodovi i Teorija informacija. Izabran je u nastavno znanje Predavača na Elektrotehničkom fakultetu u Osijeku.

Tijekom poslijediplomskog studija objavio je šest znanstvenih radova na međunarodnim konferencijama s područja mikroelektronike, VoIP komunikacije i sigurnosti informacijskih sustava. Poslijediplomski studij završava 2011 obranom rada naziva „Optimizacija VOIP komunikacije na temelju subjektivnog i objektivnog određivanja kvalitete usluge“ pod mentorstvom prof.dr.sc. Drage Žagara. Tijekom daljnjeg istraživanja i doktorskog studija objavljuje i članke u časopisima: Tehnički vjesnik i Automatika.

Predavač je na više stručnih međunarodnih konferencija na temu sigurnosti, upravljanja i revizije informacijskih i komunikacijskih sustava.