

Sadržaj

Popis kratica	V
SAŽETAK.....	VI
ABSTRACT	VII
1 UVOD	11
1.1 Predmet i objekt istraživanja	13
1.2 Postavljanje problema	15
1.3 Glavna i pomoćne hipoteze	16
1.4 Ciljevi istraživanja.....	17
1.5 Etički aspekti istraživanja i korisnici rezultata istraživanja	19
1.6 Istraživačka ograničenja	19
1.7 Metode istraživanja	21
1.8 Referentna literatura	27
2 ANALIZA POSTOJEĆIH ISTRAŽIVANJA U DOMENI RIZIKA ZRAKOPLOVNIH INFORMACIJSKIH SUSTAVA I ZAKONSKI OKVIRI	28
2.1 Analiza rizika i sigurno dizajniranje softvera	29
2.1.1 Analiza rizika	30
2.1.2 Analiza prijetnji.....	32
2.1.3 Procjena arhitektonske ranjivosti	33
2.1.4 Analiza otpornosti na napad	33
2.1.5 Analiza aktivnosti.....	34
2.1.6 Određivanje utjecaja na rizik.....	36
2.1.7 Načela sigurnosti softvera	39
2.1.8 Sigurnosna svojstva.....	43
2.1.9 Pouzdanost i sigurnost softvera.....	44
2.1.10 Otpornost i tolerancija na napade.....	48
2.1.11 Sigurno kodiranje i testiranje	50
2.2 ATM – Air Traffic Management.....	51
2.2.1 ATM Bosne i Hercegovine	51
2.2.2 Sigurnosne mjere za kritične cyber ICT infrastrukture.....	57
2.2.3 Podjela komponenata-servisa prema važnosti za pružanje usluga u zračnoj plovidbi...	58
2.2.4 Cyber prijetnje.....	59
2.2.5 Ljudske prijetnje.....	61
2.2.6 Održavanje razine povjerljivosti, integriteta i dostupnosti podataka	62

2.2.7	Arhiviranje i čuvanje radnog softvera uređaja	63
2.3	Procjena rizika i ATM sustavi.....	64
2.3.1	Metoda informacijskog napada	64
2.3.2	Sredstva prijetnje / Izvori prijetnje.....	65
2.3.3	ICT sigurnosne kontrole.....	66
2.3.4	Kontrola sustava putem Check lista	67
2.3.5	Klasične metodologije procjene rizika ICT sustava.....	69
3	IT STANDARDI (ISO STANDARDI) U INFORMACIJSKO KOMUNIKACIJSKIM SUSTAVIMA.....	71
3.1	Definiranje veze između informacije, zaštite podataka i standardizacije	71
3.2	Sustav menadžmenta sigurnosti informacija.....	73
3.3	Međunarodni standardi u sigurnosno-informacijskim sustavima	76
3.4	Povijest i razvoj standarda ISO 27001	81
3.5	Pregled ISO 27001 standarda.....	82
3.5.1	Izjava o primjenljivosti (SoA).....	84
3.5.2	Model „Plan-Do-Check-Act“	88
3.6	ISMS u okviru standarda ISO 27001	90
3.7	Koraci prema učinkovitom ISMS-u implementacijom ISO 27001.....	95
3.8	Uloga i značaj standarda ISO 27001	97
4	UMJETNA INTELIGENCIJA U REGULIRANJU ZRAČNOG PROMETA.....	100
4.1	Umjetna inteligencija i zrakoplovni promet.....	102
4.2	Implementacija umjetne inteligencije u reguliranje zračnog prometa	106
4.2.1	Dosadašnja implementacija Umjetne inteligencije u ATC	106
4.2.2	Cyber sigurnost AI sustava kontrole zračnog prometa	108
4.3	Korištenje umjetnih neuronskih mreža u domeni cyber sigurnosti i moguća primjena u zrakoplovstvu	110
4.4	Moguća područja primjene neuronskih mreža u zrakoplovstvu	111
4.4.1.	Primjena u kontroli zračne plovidbe	111
4.4.2.	Primjena na zračnim lukama	112
4.5	Eventualni problemi pri uvođenju tehnologije za obradu podataka.....	112
4.6	Korištenje neuronskih mreža u oblasti cyber sigurnosti	114
4.6.1	Primjena umjetnih neuronskih mreža u sustavima za otkrivanje upada	116
4.6.2	Osposobljavanje neuronske mreže za oponašanje vatrozida.....	118
4.6.3	Nedostaci postojećih rješenja	119

4.7	Ovisnost uvođenja neuronskih mreža i cyber sigurnosti u zrakoplovstvu	119
4.7.1.	Sigurnosne prijetnje korištenja neuronskih mreža u kontroli zračne plovidbe i u zračnim lukama	120
5	MODEL I EFEKTI.....	122
5.1	Određivanje rizika prije uvođenja standarda.....	133
5.2	Određivanje i Procjena rizika nakon uvođenja standarda	148
5.3	Određivanje i Procjena rizika nakon uvođenja standarda i vanrednih upravljačkih kontrola 167	
5.4	Efekti usporedbe modela.....	170
6	ZAKLJUČAK	173
7	LITERATURA.....	174
8	Popis slika	178
9	Popis tablica	179