ODSJEK ZA SIGURNOSNE I MIROVNE STUDIJE

UPRAVLJANJE INFORMACIJAMA I ZAŠTITA PODATAKA U SISTEMU SIGURNOSTI BOSNE I HERCEGOVINE

-magistarski rad-

Kandidat:

Malagić Nihad

Broj indexa: 761/II-SPS

Mentor:

prof. dr. Bajramović Zlatan

Sarajevo, decembar 2022. godina

SKRAĆENICE

EU- Europska unija

NATO- eng. North Athlantic Treaty Organisation- bos. Sjevernoatlantski savez

OSCE- eng. Organization for Security and Co-operation in Europe- bos. Organizacija za europsku sigurnost i suradnju

ISO- eng.- International Organization for Standardization- bos. Međunarodna organizacija za standardizaciju

OS BiH- Oružane snage Bosne i Hercegovine

OSA- Obavještajno-sigurnosna agencija

SIPA- eng. State Investigation and Protection Agency- bos. Državna agencija za istrage i zaštitu

GP BiH- Granična policija Bosne i Hercegovine

DKPT- Direkcija za koordinaciju policijskih tijela

MUP- Ministarstvo unutrašnjih poslova

SADRŽAJ

1. UVOD

Različiti akteri iz oblasti sigurnosti, koji mogu biti predstavljeni kroz globalne, regionalne, međudržavne i državne organizacije i institucije, koji u svojim aktivnostima i radu nastoje kroz različite sfere društvenog ili profesionalnog djelovanja, obezbjediti sigurnost koja se odnosi na efikasno upravljanje i zaštitu svoje infastrukture i samih informacija i podataka, a sve s ciljem podizanje sigurnosnog ambijenta na jedan viši nivo, i sigurnosti ali i stabilnosti sistema. Različite nestabilnosti koje prate ljudsku civilizaciju dovele se do različitih tranformacija u poimanju sigurnosti informacija. Period 20. stoljeća obilježen je sa mnogo ratova, dva svjetska rata i periodom takozvanog Hladnog rata, ovaj period se odrazio i na ono što obrađujemo u ovome radu. Transformacija i modernizacija svih društvenih sfera dovele su do potrebe za što bržim prilagođavanjem različitim situacijama, te savladavanjem prepreka i uspostavljanjem efikasnih i vrhunski obučenih aktera u oblasti upravljanja informacija, zaštite informaciono-komunikacionih sistema i zaštite podataka u tim sistemima.

Trendovi na globalnom nivou doveli su do promjene percipiranja sigurnosti, od sigurnost državne strukture i granice do okretanju sigurnosnog pitanja ka pojedincu, tako bi možda najlakše i najjednostavnije mogli predstaviti promjenu sigurnosne paradigme. Tokom Hladnog rata i stvaranja blokovske podjele svijeta, međunarodne organizacije vezane za sigurnosni sektor, te pristup istim se mogao smatrat, u isto vrijeme i političkim pitanjem, odnosno uvjerenjima nekog naroda i/ili lidera, ali i vojnim pitanjem, odnosno pogodnosti zaštite i sigurnosti. Kroz sve ove krize kroz koje je prolazio svijet, jedna od konstanti je bila kvalitetno upravljanje i zaštita informacija iz sistema sigurnosti jedne orgnizacije i u krajnjem slučaju države.

Kada govorimo o Bosni i Hercegovini, trenutnom stanju države općenito, ali i u aspektu sigurnosti, svjesni smo djelovanja i aktivnosti kako pojedinaca i političkih subjekata, tako i vandržavnih aktera u kontekstu ukrožavanja sigurnosti. Samim tim Bosna i Hercegovina se društveno i politički nalazi na raskrsnici, nastojanje da naša država otvaranjem prema Zapadu koji predstavlja sinonim za ekonomsku stabilnost, razvoj i napredak, ili prema Istoku koji nema tako popularnu reputaciju, osigura bolji kvalitet života građana. Bosna i Hercegovina koja kroz svoju blisku prošlost pamti agresivno narušavanje

teritorijalnog integriteta i suvereniteta od strane susjednih država, mora se opredijeliti i trasirati svoj put ili ka NATO paktu ili ka traženju alternativa. Tema koja sa sobom nosi sigurnost, bilo to kroz kontekst upravljanje i zaštite informacija i podataka, uvijek je aktuelna i aktuelnost ove tematike u Bosni i Hercegovini, ali i državama nastalim iz raspada Jugoslavije, je uvijek prisutna iz razloga što veoma često dolazi do pokušaja narušavanja integriteta državnih institucija, pogotovo onih koje se odnose na oblast sigurnsoti.

Napadi na suverenitet i integritet Bosne i Hercegovine dolaze od visokih zvaničnika susjednih zemalja ili od njihovih partnera u svijetu, desničarskih organizacija, ali i iz akademskih krugova, te iz tog razloga potreba za promjenama ustava, stvaranje i jačanje institucija na državnom nivou, jačanje pravosudnih institucija i sigurnosnih agencija, unapređenje, prilagođavanje i modernizacija sigurnosnog sistema, usvajanje politika i strategija, su neki od elemenata za stvaranje moderne i stabilne Bosne i Hercegovine.

2. TEORIJSKO-METODOLOŠKI OKVIR

2.1 *Problem istraživanja*

Kada govorimo o informacijama i upravljanju informacijama, moramo spomenuti kontekst na koji se ti pojmovi odnose. Informacije i upravljanje informacijima se najćešće odnose na sektor sigurnosti, u ovom radu ćemo obrađivati općenito sistem sigurnosti u Bosni i Hercegovini, upravljanje informacijama u sistemu sigurnosti Bosne i Hercegovine, rad polcijskih agencija po ovom pitanju, pogled NATO-a na ovu temu te pitanja cyber sigurnosti i standardizacije. U samom radu će biti spomenut i definisani relevantni pojmovi koje obuhvata i na koji se odnosi ova tematika, radi boljeg razumijevanja samog rada.

Problem ovog istraživanja će predstavljati: ***Efikasnije upravljanje informacijama i kvalitetnija zaštita podataka kao potreba za podizanje sveokupne stabilnosti i sigurnosti države Bosne i Hercegovine i njenjih građana.***

2.2 *Predmet istraživanja*

Predmet istraživanja bi predstavljao:

Upravljanje informacijama u sistemu sigurnosti Bosne i Hercegovine

Kako je navedeno u dijelu koji se bavio Problemom istraživanja, u ovom dijelu koji se odnosi na Predmet istraživanja bit će predstavljeni akteri koji imaju učešće u ovom predmetu a to su institucije i agencije koje čine sigurnosni sistem Bosne i Hercegovine, kao i međunarodni akteri. Također kroz Predmet istraživanja će bi predstavljeno da li je trenutni sistem efikasan, i da li i u kolikoj mjeri postoji mogućnost unapređenja kroz saradnju sa međunarodnim partnerima.

Opći tipski model istraživanja koji se sastoji od: prirodnih i društvenih uslova, subjekata, interesa i ciljeva, djelovanja tih društvenih subjekata, metode, način i sredstva djelovanja, skup rezultata i određenih posljedica tog djelovanja.

I. Uslovi: Društveni uslovi po ovom pitanju predstavljaju narušen sigurnosni ambijent u Bosni i Hercegovini i regionu.

II. Subjekti: Institucije BiH i njeni predstavnici, policijske agencije, međunarodne organizacije i stanovništvo Bosne i Hercegovine.
III. Interesi i ciljevi: Unapređnje sektora sigurnosti, modernizacija i stavaranje sigurnijeg ambijenta.
IV. Aktivnosti: Usvajanje politika, strategija, zakona, podzakonskih akata, smjernica u kontekstu upravljanja informacijama.
V. Metode i sredstva: Predstavljaju utrošena sredstava na unaprijđenje i modernizaciju, te obuku kadra.
VI. Efekti: Efekti se mogu povezati sa svim prethodno navedenim stavkama, odnosno dostignuća na terenu, ali i instutcionalno u smjeru željenih interesa.

.

Vremensko određenje predmeta istraživanja

Djelovanja i aktivnosti od samih držanih institucija i agnecija, te mađunarodnih aktera, a koje su provedene od 1995. godine pa do 2022. godine.

Prostorno određenje predmeta istraživanja

Prostorno određenje predmeta istraživanja bi bio teritorij Bosne i Hercegovine, te odnos na međunarodnom planu prema BiH u kontekstu sigurnosti.

Disciplinarno određenje predmeta istraživanja

Predmet istraživanja bi okrakterisali kao interdisciplinaran, iz razloga što odvija u okviru sigurnosnih i mirovnih studija, međunarodnih odnosa i politika.

2.3 *Ciljevi istraživanja*

Kada govorimo o cilju ovog istraživanja potrebno je prepoznati aktivnosti i djelovanja svih učesnika ka ostvarivanju nekog cilja koji je dat u samom istraživačkom radu. *Upravljanje informacijama i zaštita podataka u sistemu sigurnooti Bosne i Hercegovine* kao predmet istraživanja i posmatranja sigurnosti Bosne i Hercegovine je potrebno promatrati u geopolitičkom i geostrateškom kontekstu, kao i okvirima

međunarodne dimenzije sigurnosti. Segment cilja istraživanja možemo promatrati kroz naučni ili društveni cilj istraživanja. Naučni ciljevi se odnose na „sticanje naučnog saznanja određenog obima i nivoa“ dok je društveni cilj „usmjeren na dobrobit ljudi“. (Termiz, 2009:220)

2.3.1 Naučni ciljevi istraživanja

Obrazlaganje uključenosti međunarodnih organa u ovo pitanje, ali i ulogu i rad samih državnih institucija Bosne i Hercegovine će predstavljati određene segmente ovog rada. Također će biti predstavljen tranzicijski period i promjena političkog sistema i sam uticaj ovih događaja na pitanje koje obrađujemo. Kroz pristup određenim platformama koje imaju zadatak za poboljšanje infrastuktrure na određeni način pripreme i obuče za zadatke i norme koje nastoje ispuniti kako bi dovelo do lakšeg prilagođavanja kriznim situacijama. Kroz naučni cilj nastojimo da predstavimo relevantne podatke koji bi se odnosili na sistem sigurnosti Bosne i Hercegovine, nakon toga bi sticanjem saznanja mogli sa nekon naučnog aspekta promatrati ovu granu sigurnosti.

Prikaz ovog rada i ove tematike bi se odnosio na benefite, odnosno pozitivne i negativne elemente koji bi se odrazili na stanje društva nakon poboljšanja ili zadržavanja trenutnog stanja. Odraz bi se odnosio na sam sistem sigurnosti, ali i svakodnevni život pojedinaca, korporacija državnog i međudržavnog karaktera. Sam region Jugoistočne Europe je izvor nestabilnosti i kriza, te je to i razlog više zašto bi svaka država trebala imati efiksan način upravljanja i zaštite informacija iz sektora sigurnosti. Ovaj dio rada bi trebao predstaviti prezentaciju korijena tih konflikata i nerazumijevanja.

2.3.2 Društveni ciljevi istraživanja

U ovom radu društveni cilj bi predstavljao prezenaciju svih relevantnih faktora koji bi se odnosili na upravljanje informacijama u sigurnosnom sistemu Bosne i Hercegovine, te kako bi unaprijeđenje dovelo

do sigurnijem ambijentu na državnom, regionalnom i međunarodnom nivou. Pitanje pred kojim će se naći BiH u budućem periodu će biti opredjeljenje o učešću u međunarodnim sistemima sigurnosti što kroz vid članice, partnera ili neutralnog posmatrača. Siguran ambijent i stabilna država postaju interes za investitore, koorporacije, te i razvoj svih industrijskih grana.

2.4 *Generalna hipoteza*

Generalna hipoteza bi glasila: „Država Bosna i Hercegovina koja teži ka članstvu u EU i NATO-u mora da posjeduje efikasan način upravljanja i zaštite informacija i podataka u sistemu sigurnosti.“

2.4.1 Posebne hipoteze

Posebna hipoteza 1: Kvalitet upravljanja informacijama i zaštite podataka u sistemu sigurnosti Bosne i Hercegovine treba poboljšati na način saradnje sa međunarodnim agencijama i sigurnosnim organizacijama.

Posebna hipoteza 2: U sistemu sigurnosti Bosne i Hercegovine nema potreba za poboljašnju upravljanja informacijama i zaštite podataka, odnosno sadašnje stanje je zadovoljavajuće.

Posebna hipoteza 3: Sigurnosni sistem Bosne i Hercegovine je zbog unutardržavne retrogradne politike i djelovanja vandržavnih aktera postao ranjiv i zahtijeva reformu ili dogradnju.

Posebna hipoteza 4: Pristupom Sjevernoatlantskom savezu, upravljanje informacijama u sistemu sigurnosti Bosne i Hercegovine smanjila bi se mogućnost ataka na informacije i doprinjelo smanjenje tenzija, i ambicija na ugrožavanje suvereniteta, intigriteta, političke nezavisnosti i sigurnosti sveobuhvatno.

Posebna hipoteza 5: Pristupom NATO savezu svi građani i kompanije postaju oslobođeni određene neizvjesnosti po pitanju vlastitih informacija i podataka, te mogu aktivnije učestvovati u riješavanju stvarnih problema i osmišljati budućnost u sigurnijem ambijentu.

2.4.2 Indikatori

„Faktički, indikatori su neposredovano ili posredovano, pokazatelji stavova hipoteze.“ (Termiz, 2003:182)

Indikator 1: Potreba za poboljšanjem komunikacije između sigurnosnih agencija unutar države, te sa međunarodnim organizacijama i agencijama.

Indikator 2: Blokade institucija i ne pokazivanje želje za izmjenama ustava po svim pitanjima, pa i pitanjima sigurnosti građana.

Indikator 3: Aktivnije ućešće svih relevantnih aktera za uspostavljanje funkcionalnog političkog sistema u Bosni i Hercegovini.

Indikator 4: Političkim predstavnicima unutar Bosne i Hercegovine, ali i u susjednim državama odgovara ambijent neizvjesnosti iz razloga ostvarivanja vlastitih političkih interesa i ciljeva.

Indikatori 5: Pristup Bosne i Hercegovine u NATO paktu bi predstavljao opasnost i sigurnosni rizik za cijeli savez.

2.5 *Metode i načini istraživanja*

„Način istraživanja, kao poseban dio projekta istraživanja – nacrta naučne zamisli, po osnovnom sadržaju, smatra se dijelom naučnog dokumenta. Zaista on sadrži osnovne bitne odluke o tome kako ćemo istraživati prethodno određen predmet istraživanja, kako ćemo istraživanjem ostvariti naučne i društvene ciljeve i kako ćemo provjeriti hipoteze, te upotpuniti naučni fond.“ (Termiz, 2003: 183)

2.5.1 Vrste i tip istraživanja

Istraživanja mogu biti teorijska i ili empirijska, ovaj rad će predstavljati kombinaciju te dvije vrste istraživanja, ali će zastupljeni biti empirijski vid istraživanja iz razloga prisutnosti i aktivnosti aktera. Teorijski dio ovog istraživanja će se odnositi na sam sigurnosni sistem Bosne i Hercegovine, te saradnje sa drugim organizacijam i agencijama iz oblasti sigurnosti. Emprijsko istraživanje bi se odnosilo na stanje na terenu, aktivnosti i djelovanja od strane sudionika, te predstavljanje rezultata na terenu po ovome pitanju.

2.6 *Teorijsko-metodološki pravac*

Radi objektivnog predstavljanja ove teme potrebna je velika doza neutralonsti tokom obrade podataka koji su relevanti u ovom kontekstu. U ovom radu neće biti poseban akcenat na jedan teorijski-metodološki pravac te iz toga razloga navodima da se odnosi na integralno-sintetički.

2.7 *Opštenaučne metode*

Rad će biti zasnovan na period od nezavisnosti Bosne i Hercegovine, trenutne situacije i budućnosti po ovom pitanju.

Koristit će se sljedeće opštenaučne metode:

Hipotetičko deduktivna metoda: „U osnovi hipotetičko - deduktivne metode je opažanje – čulno i nečulno...Ona nema svoje posebne tehnike i instrumente već se oslanja na već postojeće standarde istraćivačko - operativnog metoda ali i spada u red najsloženijih metoda.“ (Termiz, 2003: 80).

Statistički metod: Dio ovog rada će svakako sačinjavati mišljenja građana sakupljenih tokom ispitivanja, anketa... prethodnih godina i tumačenje istih u kontekstu sigurnosti, odnosno uticaju “stranaca“ i razlike u tim periodima i danas. U ovom dijelu je neophodna i informatičko-statistička metoda kroz obradu podataka, zatim prebrojavanje i sistematizaciju.

Opštenaučna metoda modelovanja: Podrazumijeva zamišljanje, imitiranje i konstrukciju novih modela, promjene sadašnjih modela i zamišljanje njihovih mogućih budućih stanja. Neki od ovih načina će svakako biti uključene u izradu ovog rada radi pronalaska mogućih alternativa.

2.8 *Metode analize sadržaja i ispitivanja*

Kao jedna od osnovinih metoda analize sadržaja u ovom radu će se ogledati kroz analizu zvaničnih dokumenata od institucija Bosne i Hercegovine, međunarodnih organizacija i svih ostalih relevantnih subjekata. Za ovaj rad je planirano da se hronološki prikaže dokumentacija i usvajanjae zakona i pravilnika koji se odnose na način poboljšanja, ali i saradnje sa drugim agencijama po pitanju sigurnosti u državi.

2.9 *Izvori podataka*

Izvori podataka koji će biti korišteni za izradu ovog rada pored stručne literature bit će i publikacije, sporazumi, članci, pravilnici, zakoni i podzakonski akti; u suštini bit će korištena sva relevantna literatura po pitanju upravljanja informacijama i zaštiti podataka u sistemu sigurnosti Bosne i Hercegovine.

2.10 *Naučna i društvena opravdanost*

2.10.1 Naučna opravdanost istraživanja

Poimanje i definisanje sigurnosti u akademski krugovima koji se bave tim pitanjima je poprilično raznolika, no sama dinamika društvenog života i procesi koji se događaju na globalnom nivou svaki put postavljaju novu prepreku za poimanje sigurnosti. Kada posmatramo procese tokom 20. stoljeća možemo

uvidjeti transformaciju sigurnosti od sigurnosti države i njenog suvereniteta ka sigurnosti pojedinca, u sadašnjem vremenu i trenutnoj situaciji možemo iskazati da je pojedinac najviše ugrožen od strane globalnih procesa kao što su globalno zagrijavanje, aktuelne pandemije, cyber napadi itd. Kroz sve nedaće kroz koje prolazi društvo i sistemi sigurnosti u tom kontekstu, postavlja se pitanje sigurnosti i načinu upravljanja informacijama u istom. Veći dio ovoga rada će se odnositi na sistem sigurnosti u Bosni i Hercegovini i na upravljanje informacijama u istom. Općenito pitanje upravljanja informacija ima puno širu sliku i potrebu da se stavi u historijski kontekst i tranziciju kroz različite periode društva kao što su razne krize, ratovi, promjene političkih sistema i drugi.

2.10.2 Društvena opravdanost istraživanja

Tematika upravljanja informacijama u sitemu sigurnosti nije toliko zastupljena u naučnim krugovima koji se bave pitanjem i problemima sigurnosti. Ovaj rad će predstavljati polazni osnov za upoznavanje i bolje razumijevanje pojma upravljanja informacijama, zaštite podataka i u samom sistemu sigurnosti Bosne i Hercegovine. Također će biti predstavljen nivo saradnje sa međunarodnim organizacijama i agencijama u kontekstu same teme.

2.11 *Kategorijalno pojmovni aparat*

U ovom dijelu rada ćemo predstaviti pojmove koji su važni za razumijevanje same tematike rada, bitno je napomenuti da u ovom dijelu neće biti definisani svi pojmovi, te će ostali pojmovi biti predstavljeni i definisani u samom radu.

Informacija- lat. (informare- dati oblik, oblikovati, predočiti) uputa, obavijest, obavještenje, saopćenje o toku radova ili o nečijoj djelatnosti; podatak o nečemu **(**Klaić, 2004:588). NATO glosariji (2013:2-I-4) nam daje sljedeću definiciju, prema tome informaciju čine "Neobrađeni podaci svih opisa koji se mogu koristiti u proizvodnji obavještajnih podataka". Csandi (2018:144) također navodi i životni ciklus informacije, „Životni ciklus informacija obuhvata faze planiranja, prikupljanja, stvaranja ili generisanja

informacija; njihovu organizaciju, pronalaženje, korištenje, dostupnost i prijenos; te skladištenje i zaštita; i, konačno, njihovu dispoziciju".

Upravljanje informacijama- pojam upravljanja informacijama u literaturi na engleskom jeziku predstavlja *information management* ili menadžment informacija. Upravljanje informacijama se odnosi na niz mjera i aktivnosti koje imaju za cilj neometan, efikasan i siguran protok informacija unutar organizacija i između organizacija. Upravljanje informacijama također čine politike, strategije, smjernice i standardi kako bi se obezbjedila sigurnost u komunikaciji i razmjeni informacija, te procesi i procedure skladištenja i arhiviranja informacija.

Zaštita podataka- predstavlja proceduralnu preventivnu aktivnost institucija, kompanija ili agencija u svrhu zaštite ličnih ili tajnih podataka. Prema zakonu o zaštititi ličnih podataka (2006), lični podaci se odnose na "bilo koju informaciju koja se odnosi na fizičko lice koje je identificirano ili se može utvrditi identitet lica". Zakon o zaštiti tajnih podataka (2009), ovu vrstu podataka definiše na sljedeći način: „tajni podatak je činjenica ili sredstvo koje se odnosi na javnu sigurnost, odbranu, vanjske poslove ili obavještajnu i sigurnosnu djelatnost Bosne i Hercegovine, koji je potrebno, u skladu s odredbama Zakona, zaštititi od neovlaštenih osoba i koji je ovlaštena osoba označila oznakom tajnosti".

Sigurnost- „stepen zaštićenosti ljudi od različitih oblika ugrožavanja, zaštitu materijalnih i kulturnih dobara, zaštitu društva i njihovih vrijednosti" (Beridan, 2001:348-349). Dok autor Abazović za sigurnost navodi da je to "stanje u kome je obezbjeđen uravnotežen psihički, duhovni, materijalni i društveni opstanak pojedinca, društvenih grupa sa drugim pojedincima, društvenim grupama i prirodom". Teško je pronaći jedinstvenu definiciju koja bi obuhvatila sve faktore i aktere u definisanju pojma sigurnost. Autor Abazović (2002:250) za definisanje sigurnosti od međunarodnih organizacija navodi sljedeće: "U svom radu se oslanjaju na međunarodne standarde po kojima je sigumost shvaćena kao društveno stanje u kojem je svakom građaninu zajamčen njegov fizički integritet, opstanak, odgoj i obrazovanje, odgovarajući životni standard, pravna sigurnost, mirovinska sigurnost u starosti itd."

Sistem sigurnosti je cjeloviti mehanizam (nosioci i njihove djelatnosti) koji ostvaruje nacionalnu sigurnost putem prevencije i otklanjanja ugrožavanja temeljnih vrijednosti društva, u skladu ustavno i međunarodno priznatim standardima razvijenih demokracija i međunarodnih organizacija. (Kržalić, Purišević, Alispahić, 2020 :64)

2.12 *Naučna i druga saznanja o predmetu istraživanja*

2.12.1 Polazna saznanja o predmetu istraživanja

U ovom radu će biti predstavljeni dostupni podatci od stranje institucija i agencija BiH, odnosno sporazumi, pravilnici, zakoni i podzakonski akti. Biti će prikazani i koraci koji su urađeni od strane institucija, a koji predstavljaju i reforme sigurnosnog i odbrambenog sistema i politike. Bosna i Hercegovina kao država koja već u velikoj mjeri ima saradnju sa Sjeveroatlantskim savezom nastoji to upotpuniti punopravnim članstvom. Poltička situacija i mogućnost blokiranja i ugrožavanja bilo kojih pozitivnih procesa po pitanju sigurnosti, usporava i otežava, i samim građanima BiH, te domaćim i stranim kompanijama, ali i međunarodnim organizacijama. Prenos nadležnosti se često predstavlja kao glavni kamen spoticanja, ali ako težimo ka tome da Bosna i Hercegovina bude moderna i funkcionalna država potrebana su izmjene i dopune ustava, te dogovor svih etničkih i nacionalnih grupa unutar Bosne i Hercegovine.

2.12.2 Fundamentalna pitanja u vezi sa predmetom istraživanja

Ugrožavanja društva i građana Bosne i Hercegovine, ali i svijeta u 21. stoljeću dolaze iz mnogo različitih pravaca. Terorizam kao sigurnosna prijetnja koja je "otvorila" ovo stoljeće napadom na Sjedinjene Američke Države 11. Septembra 2001. godine i dan danas predstavlja opasnost. Migracije kojima se suočava BiH nisu problem samo jedne države već cijelog svijeta, migracije koje su izazvane uništavanjem ekosistema i globalnim zagrijavanjem se tek očekuju. Cyber sigurnost kao neka poprilično nova sfera ugrožavanja u Bosni i Heregovini poprilična je nepoznaniza za građane, a koja predstavlja jedno jako važno pitanje vezano za ovu temu. Ovo su samo od nekih pitanja i problema na koje država BiH ne može samostalno odgovoriti.

- Kako do sigurnijeg ambijenta u Bosni i Hercegovini.
- Zagovaranje neutralonsti i zadržavanje statusa quo ili zajednički odgovor na ugrožavanje sigurnosti.

- Bosna i Hercegovina bi na pitanja ugrožavanja bilo kojeg vida sigurnosti trebala djelovati kolektivno sa partnerima.

2.13 *Koncept mogućih odgovora*

Država Bosna i Hercegovina kao država koja i nakon 30 godina od početka oružane agresije nastoji da stabilizuje svoj sistem sigurnosti i hijerarhiju unutar tog sistema, često nailazi na opasnosti i prijetnje kako iz untardržavnih političkih aktera tako i od susjednih država. Potreba za unaprijeđenjem i poboljšanjem sistema sigurnosti i upravljanja informacijama unutar istog, u ovom ambijentu nije moguća bez saradnje sa međunarodnim agencijam i organizacijama, te i sa organizacijama i agencijama partnerskih i prijateljskih država. Konstantna obuka kadrova i tehnološka modernizacija su jedan od faktora koji može doprinijeti sigurnijem ambijentu po pitanju sigurnsoti informacija i podataka.

U svijetu kakav je danas samostalnost ne donosi ništa dobro, samostalnosti slijedi izolovanost iz društvenih procesa te potom donosi i zaostalost u društvenim zbivanjima. Bosna i Hercegovina kao mala država u okruženju koju sačinjavaju NATO članice ne bi smjela da ima alternativu po tom pitanju i trebala bi težiti ka zajedničkom rješavanju problema.

Svakako bi BiH trebala biti dio pozitivnih društvenih tokova izolovanost ne donosi ništa dobro. Kolektivnost se često u prethodnom periodu dovodila u pitanje, a uzrok tome su krize uzrokovane pandemijom i trenutnom agresijom Rusije nad Ukrajinom. Faktori u sistemu sigurnosti Bosne i Hercegovine posjeduju veliki broj sprovedenih aktivnosti sa partnerima po pitanju stvaranja sigurnijeg ambijenta. Svakako većina građana u BiH teži ka ostvarivanju ravnopravnosti, uživanju punih prava i sloboda i što moguće većoj afirmaciji u najnaprednijim državama svijeta. Smatramo da Bosna i Hercegova treba da teži kolektivnosti po pitanju odbrane i sigurnosti, te da njenji građani teže ka uživanju sigurnom okruženju, lišenom bilo kojeg oblika neizvjesnosti.

3. SISTEM SIGURNOSTI I SIGURNOSNA POLITIKA BOSNE I HERCEGOVINE

Kada govorimo o sferi sigurnosti moramo posjedovati znanja koja se odnose na terminologiju koja se upotrebljava. Ukoliko odlučimo rasložnjavati pojmove iz naslova moramo definisati i obrazložiti sljedeće pojmove: sistem, sigurnost i sistem sigurnosti. Prema Klaiću (2004:1234) riječ sistem se odnosi na sustav, poredak, uvjetovan planskim, pravilinim rasporedajem dijelova u određenoj vezi. Prethodnom definicijom sistema smo uvidjeli da ona predstavlja poprilično jednostavno, bez tereta koji se odnose na narušavanje tog sistema. Mi ćemo u ovom radu također obrađivati prijetnje i opasnosti koje se odnose na sisteme iz sfere sigurnosti.

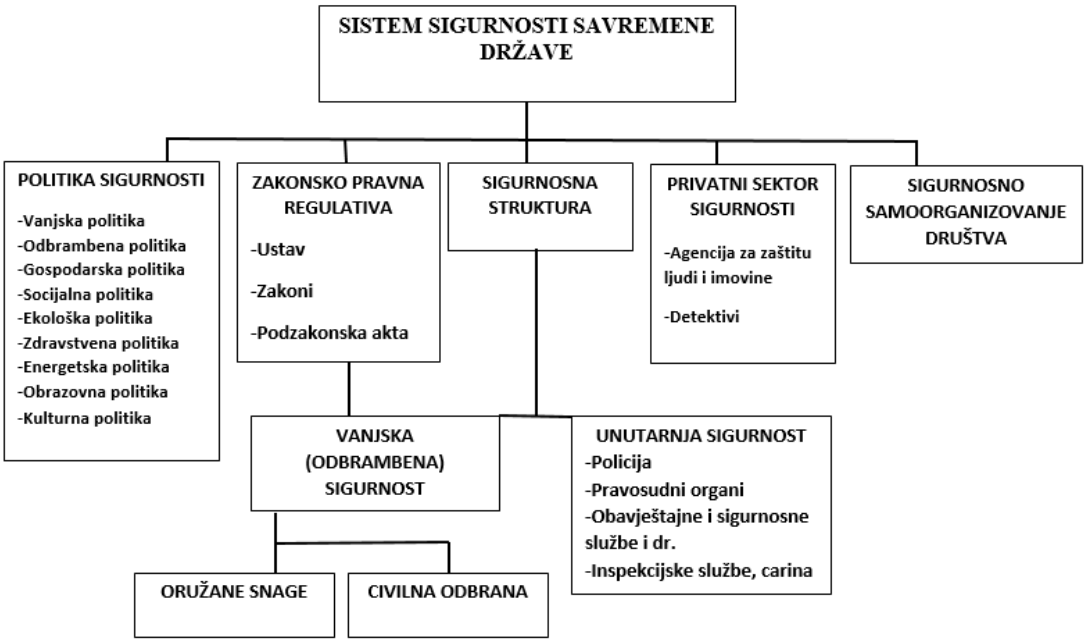
Za pojam sigurnosti autor Beridan (2001:348:349) navodi da se odnosi „stepen zaštićenosti ljudi od različitih oblika ugrožavanja, zaštitu materijalnih i kulturnih dobara, zaštitu društva i njihovih vrijednosti“. Dok autor Abazović (2012:27) za pojam sigurnosti navodi da je to „stanje u kome je obezbjeđen uravnotežen psihički, duhovni, materijalni i društveni opstanak pojedinca, društvenih grupa sa drugim pojedincima, društvenim grupama i prirodom.“

Priručnik za Rad policije u zajednici u Bosni i Hercegovini (2010:15) prepoznaje dvije vrste sigurnosti a to su objektivna i subjektivna sigurnost. Te za njih navode sljedeće:

• Stepen objektivne sigurnosti se oslikava u statističkim podacima koji navode konkretno činjenično stanje koje je ustanovila policija. Naprimjer, u mostarskom kvartu X u 2009. godini prijavljeno je pet lica zbog fizičkog nasilja.

• Stepen subjektivne sigurnosti, odnosno osjećaja sigurnosti se izražava ličnim osjećajem lica, koji je vezan za sigurnosnu situaciju u njihovom okruženju. Radi se o pitanju da li ta lica nemaju, imaju malo, mnogo ili veoma mnogo straha od toga da postanu žrtve nekog kriminalnog djela ili neke nesreće. Naprimjer, prema podacima provedene ankete, u dobojskom kvartu Y mnoga lica osjećaju strah kada navečer poslije 22 sata izađu van kuće, iako statistika navodi da se radi o natprosječno sigurnom kvartu.“

Potreba za navođenjem podjele sigurnosti iz gore navedenog priručnika se ogleda u tome što je samo shvatanje sigurnosti kroz objektiv policije mnogo bliži i opipljiviji građanima, zbog svakodnevne komunikacije i aktivnosti.



Slika br. 1 –Sistem sigurnosti savremene države (Cikotić, 2013)

U gore navedenoj ilustraciji su nam prikazani elementi sistema sigurnosti savremene države, sistem se sastoji od pet glavnih elemenata, a to su: politika sigurnosti, zakonsko pravna regulativa, sigurnosna struktura, privatni sektor sigurnosti i sigurnosno samoorganizovanje drušva. Pod politikama sigurnosti su pobrojane: vanjska politika, odbrambena politika, gospodarska politika, socijalna politika, ekološka politika, zdravstvena politika, energetska politika, obrazovna politika i kulturna politika. Zakonsko pravna regulativa se odnosi na Ustav, zakone i podzakonke akte. Zakonsko pravna regulativa je povezana sa sigurnosnom strukturom koju sačinjavaju odbrambena sigurnost i unutarnja sigurnost, odbrambena sigurnost se dalje dijeli na oružane snage i civilnu odbranu, dok se unutarnja sigurnost odnosi na policiju, pravosudne organe, obavještajne i sigurnosne službe i dr; inspekcijske službe i carine. Sledeći dio se odnosi na privatni sektor sigurnosti koji sačinjavaju agencije za zaštitu ljudi i imovine i detektivi. Posljedni dio ove ilustracije se odnosi na sigurnosno samoorganizovanje društva.

3.1 *Sigurnosna politika Bosne i Hercegovine*

Kada govorimo o sistemu sigurnosti Bosne i Herceovine u kontekstu današnjice, možemo reći da se poduzimaju koraci da ide u korak sa državama parterima i saveznicima, ali nažalost postoji politički teret koji nastoji da sve procese maksimalno uspori, da saradnje onemogući ili svede na minimalan nivo. Sigurnosna politika Bosne i Hercegovine (u daljem tekstu Sigurnosna politika) se temelji na dokumentu iz 2006. godine, glavni dijelovi tog dokumenta se odnose na: principe sigurnosne politike, stanje sigurnosti, elemente sigurnosne politike te ciljeve i provođenje sigurnosne politike. Definisanje samog pojma sigurnosne politike dao nam je autor Abazović (2012:34), te on navodi: sigurnosna politika treba dati odgovore na pitanja zaštite interesa i prioriteta građana, konkretnog društva i države u cjelini od vanjskih i unutrašnjih prijetnji bilo koje vrste predvidjeti političke, ekonomske i vojne mjere u tom smislu. Iz prethodno navedenog teksta možemo uvidjeti da sigurnosna politika obuhvata cjelinu društva i državne strukture, te da treba da prepoznaje i nudi odgovore na ugrožavanje s vana ili iznutra neke države i njenih građana.

U dokument Sigurnosne politike Bosne i Hercegovine (2006:1) u uvodu se konstatuje sljedeće:

Sigurnosna politika Bosne i Hercegovine *je dokument koji definiše dugoročnu i koherentnu strategiju, koja daje okvir i smjernice za izgradnju sistema, strukture i svih mehanizama neophodnih za efikasno djelovanje sektora sigurnosti. Sigurnosnu politiku razrađuje izvršna vlast Bosne i Hercegovine koja ima sposobnost da koordinira primjenu obavještajnosigurnosnih, vojnih, ekonomskih, diplomatskih, tehnoloških, informacijskih i ostalih resursa radi postizanja sigurnosnih ciljeva.*

U dokumentu, definisanjem sigurnosne politike nam se daje vremenski okvir za koji je ona namjenjena, te način i smjerovi djelovanja. Također nam se navodi način izrade sigurnosne politike i način postizanja ciljeva, oblasti kojima je definisana koordinacija su i unutardržavne prirode, ali i pokrivaju oblast vanjske politike.

3.1.1 Principi Sigurnosne politike Bosne i Hercegovine

Sigurnosna politika Bosne i Hercegovine se temelji na sljedećim principima:

- Princip pravne uređenosti,
- Princip nedjeljivosti sigurnosti,
- Princip sveobuhvatnosti u zaštiti vitalnih vrijednosti,
- Princip miroljubivosti i partnerstva,
- Princip transparentnosti, i
- Princip otvorenosti za promjene.

Princip pravne uređenosti kao što sam naziv govori zahtijeva poštivanje ustava i zakonskih normi: „Sigurnosna politika, kao specifično područje društvenog djelovanja, zasnovana je na ustavnim i zakonskim odredbama i normama međunarodnog prava, kao i na pravima i obavezama koje proističu iz međunarodnih dokumenata koje je Bosna i Hercegovina prihvatila u ovoj oblasti. To podrazumijeva da pravna uređenost sigurnosnog koncepta mora biti primjerena objektivnim potrebama i postavljenim sigurnosnim ciljevima nesmetanog razvoja demokratskog društva“ (Sigurnosna politika Bosne i Hercegovine, 2006:2). Princip pravne uređenosti je ujedno i norma za dostizanje što savremenijeg uređenja, u kojima bi građani mogli uživati u svim svojim pravima i slobodama. Ovaj princip je također važan i za samu temu ovog rada, preciznije iz oblsti zaštite podataka i zabrane zloupotrebe podataka, sektor koji se bavi zaštitiom podataka u određenom sistemu sigurnosti zahtijeva potrebu da to sve odvija u granicama po kojima je to zakonima regulisano.

Princip nedjeljivosti u sigurnosti „u savremenom svijetu ukazuje da nivo sigurnosti u okruženju i šire nužno utiče na sigurnost u Bosni i Hercegovini, i obratno. Ovakvi interaktivni odnosi u oblasti sigurnosti u svijetu obavezuju sve države, pa time i BiH, da preuzme odgovornost u održavanju unutrašnje i vanjske sigurnosti i da u granicama svojih kapaciteta, kroz saradnju i partnerstvo sa drugim subjektima međunarodnih odnosa, aktivno doprinosi ukupnoj sigurnosti“ (Sigurnosna politika Bosne i Hercegovine, 2006:2). Ovaj princip se odnosi na određene prijetnje i opasnosti u širem okruženju, te da postoji potreba i odgovornost za efikasnom unutardržavnom strukturom.

Princip sveobuhvatnosti u zaštiti vitalnih vrijednosti je u određenoj vezi sa prethodnim principom, iz razloga prepoznavanja prijetnji i opasnosti na međunacionalnom nivou i potreba saradnje u rješavanju istih. U Sigurnosnoj politici (2006:2) se za ovaj princip navodi sljedeće: „Uzimajući u obzir kompleksnost i međuzavisnost savremenih rizika i prijetnji, Bosna i Hercegovina će osigurati koordinaciju aktivnosti postojećih, a gdje je potrebno ustanoviti i odgovarajuće nove mehanizme unutar sistema sigurnosti, s ciljem pružanja sveobuhvatne i aktivne zaštite njenih društvenih vrijednosti i interesa". Ovaj princip još prije 16 godina prepoznaje potrebu uspostave novih mehanizama unutar sistema sigurnosti, danas bi se tu mehanizmi vjerovatno odnosili na kibernetičku sigurnost i migracije.

Sigurnosna politika (2006:2) navodi i Princip miroljubivosti i partnerstva, ovaj princip zavodovoljava sve pacifističke i liberalne norme i u njemu se navodi: " Bosna i Hercegovina je čvrsto uvjerena u mogućnost rješavanja svih otvorenih pitanja političkim i pravnim sredstvima. Nema teritorijalnih pretenzija prema susjednim i drugim državama, niti susjedne i druge države doživljava kao neprijateljske i kao moguću prijetnju svom teritorijalnom integritetu i suverenitetu. Zbog toga je od posebnog značaja dalje razvijanje dobrosusjedskih odnosa zasnovanih na principima jednakosti i saradnje."

Princip koji se odnosi na kontrolu i nadzor, te ispunjavanje demokratskih normi je Princip transparentnosti. U Sigurnosnoj politici (2006:2-3) su jasno definisane institucije koje vrše nadzor i za ovaj princip je navedeno sljedeće: „S ciljem ostvarivanja demokratske kontrole u oblasti sigurnosti, osigurat će se odgovarajuća transparentnost aktivnosti nadležnih državnih institucija, u skladu sa standardima koji se primjenjuju u razvijenim demokratskim državama. To podrazumijeva jedinstveno upravljanje i kreiranje daljeg razvoja sigurnosnog sistema i aktivno ostvarivanje nadzorne funkcije od strane Parlamentarne skupštine, Predsjedništva i Vijeća ministara BiH nad zakonitošću rada institucija koje čine taj sistem".

Posljedni princip prepoznaje dinamičnost sigurnosnog ambijenta, te se za Princip otvorenosti za promjene navodi sljedeće: „Kako je sigurnosni kontekst po sebi dinamičan, Sigurnosna politika će biti otvorena za doradu, kreiranje i prilagođavanje. Na ovo obavezuju moguće nagle i iznenadne prijetnje stanju sigurnosti u zemlji, regionu i svijetu." (Sigurnosna politika Bosne i Hercegovine, 2006:3)

3.1.2 Stanje sigurnosti u Sigurnosnoj politici Bosne i Hercegovine

Ovaj dio Sigurnosne politike je podijeljen na tri dijela, prvi dio se odnosi na sigurnosno okruženje u kojem su predstavljenje neke osnovne geografske i političke karakteristike Bosne i Hercegovine, drugi dio se odnosi na sigurnosne izazove i rizike i treći dio se odnosi na procjenu sigurnosnih kretanja u Bosni i Hercegovini i regionu. Prema ovome možemo zaključiti da određenje stanja sigurnosti se vrši prema tri elementa a to su: okruženje, izazove-rizike i procejnu sigurnosnih kretanja.

3.1.3 Sigurnosno okruženje, izazovi i rizici

Geografske i društveno-političke karakteristike Bosne i Hercegovine u Sigurnosnoj politici (2006:3) su predstavljenje na sljedeći način: „Bosna i Hercegovina je smještena u jugoistočnoj Evropi i preko njene teritorije vode najkraći komunikacijski pravci koji povezuju prostor Podunavlja sa srednjim Jadranom. Veličinom, nivoom društvenog proizvoda, položaja, komunikacijskim značajem, te po osnovu raspolaganja strategijskim sirovinama i resursima Bosna i Hercegovina ima ograničen uticaj u savremenom svijetu. Međutim, ona je i dalje faktor uticaja na stabilnost jugoistočne Evrope i Evrope u cjelini, zbog čega će njena unutrašnja i vanjska dinamika razvoja biti predmet evropske i šire međunarodne pažnje i u narednom periodu“. U ovom dijelu su navedene samo osnovne karakteristike, dok u dijelu koji se odnosi na društveno-političke karakteristike daje značaj i navodi da je Bosna i Hercegovina “faktor uticaja na stabilnost“ jugoistočne Evrope i Evrope kao cjeline. U daljem dijelu ovog poglavlja pored navođenja karakteristika procesa globalizacije identificiraju se i izazovi i prijetnje po mir, kao najizraženiji izazovi navode se: „međunarodni terorizam, organizovani kriminal, proliferacija biološkog, hemijskog i nuklearnog oružja, nelegalna trgovina raznim tehnologijama i narkoticima, ljudima i dr.“ (Sigurnosna politika Bosne i Hercegovine, 2006:3). Interesantno je kako u tom periodu nisu identificirani cyber napadi kao prijetnja ili izazov, možda iz razloga što ne izazivanju direktnu patnju ili stradanje, ili su ipak navedeni pod skraćenicom “i dr.“ što bi značilo i drugi.

Pod izazovima i prijetnjama u sigurnosnom okruženju u ovom dijelu se još navode: „Neujednačen razvoj zemalja, neriješeni problemi zdravlja,

a naročito visok stepen siromaštva i druge negativne pojave u svijetu, u sve većoj mjeri postaju globalni izazovi“ (Sigurnosna politika Bosne i Hercegovine, 2006:3). Također se navode i lokalni sukobi i njihova mogućnost eskalacije, ispoljavanje nacionalnih, vjerskih, kulturnih identiteta koja nose retrogradna obilježja. Kao izazov se također navodi i proces povratka izbjeglih i raseljenih lica iz Bosne i Hercegovine i susjednih zemalja, ovaj dio u BiH je regulisan Ustavom Bosne i Hercegovine i to u članu 2. tački 5. gdje se navodi:

Sve izbjeglice i rasejena lica imaju pravo da se slobodno vrate u svoje domove. Oni imaju pravo, u skladu sa Aneksom 7[1] *Opšteg okvirnog sporazuma, da im se vrati imovina koje su bili lišeni za vrijeme neprijateljstava od 1991. i da dobiju kompenzaciju za svu takvu imovinu, koja im ne može biti vraćena. Sve obaveze ili izjave u vezisa takvom imovinom, koje su date pod prisilom ništavne su.* (Ibrahimagić, Seizović, Arnautović, 2010:17)

Također strane potpisnice su se obavezale stvaranju uslova za miran i normalan povratak. Demokratski progres se navodi kao razlog smanjenja tenzija u regionu, isto tako se navodi težanja ka europskim i euroatlantskim integracijama. Završni dio koji se odnosi na sigurnosno okruženje navodi da praktično ne postoji nemogućnost neke buduće agresije od susjednih zemalja na Bosnu i Hercegovinu,

„Mogućnost da će Bosna i Hercegovina u nekoj bližoj budućnosti biti suočena s agresijom izvana, praktično i ne postoji. Ukoliko bi došlo do radikalnih promjena, koje bi rezultirale osnovnim prijetnjama po suverenitet i teritorijalni integritet Bosne i Hercegovine, novim izazovima bi se odgovorilo odgovarajućim mjerama i aktivnostima usmjerenim na odbranu, koja bi se zasnivala na sistemu kolektivne odbrane i na potpunoj saradnji sa prijateljskim i savezničkim zemljama“ (Sigurnosna politika Bosne i Hercegovine, 2006:4).

Opće geografske, društvene, političke i sigurnosne karakteristike i težnje su opisane u sigurnosnom okruženju dokumentu Sigurnosne politike Bosne i Hercegovine. Postoji potreba donošenja nove

[1] Aneks 7 - Sporazum o izbjeglicama i prognanicima, gdje se u članu 1. navodi: „Sve izbjeglice i prognanici imaju pravo slobodno se vratiti u svoje domove. Imaju pravo na povrat imovine koje su lišeni tijekom neprijateljstava od 1991. godine i na naknadu imovine koja se ne može vratiti“. Opći okvirni sporazum za mir u Bosni i Hercegovini, 53. str.

sigurnosne politike iza razloga prolazska znatnog vremenskog perioda, te i novih oblika ugrožavanja koji treba navesti u novom dokumentu.

U ovom dijelu sigurnosni izazovi i rizici su podijeljeni u tri dijela u odnosu na obim i strukturu koju zahvaćaju. Prvi dio se odnosi na globalne izazove i rizike koji po svojim karakteristikama zahvataju cijelu Zemlju, drugi dio se odnosi na kontekst regionalnih izazova i rizika, i posljednji se odnose na unutardržavne izazove i rizike.

Za globalne izazove se navodi sljedeće: „razlika u nivou ekonomskog i društvenog razvoja, razlika između bogatog i siromašnog dijela svijeta, međunarodnog terorizama sa svim oblicima ispoljavanja,stalnog ugrožavanja životne sredine (kao posljedica industrijskog i tehnološkog razv oja), nekontrolisane proizvodnje i prodaje naoružanja, uključujući i oružje za masovno uništavanje (nuklearno i biološko naoružanje), intenziviranja prisilnih migracija, koje su posljedica oružanih sukoba, kao i sukoba i diskriminacije na rasnoj osnovi, etničkoj netoleranciji ili su proizvod političkih pritisaka u autokratskim i nedemokratskim režimima. Tu su i izazovi povezani s različitim oblicima organizovanog kriminala, koji potiču trajnu socijalnu i političku nestabilnost u pojedinim državama regiona, što je praćeno općim siromaštvom i širenjem raznih bolesti koje ugrožavaju cijele populacije.” (Sigurnosna politika Bosne i Hercegovine, 2006:4). Svakako i ova oblast zahtijeva određenu dopunu, svaki problem koji u nekom vremenu predstavlja problem neke zajednice ili države u savremenom svijetu u kratkom roku može postati globalni problem. Ekstremističke i terorističke grupe pored migracija kao načina širenja svojih ideja i stavova, danas imaju dostupne savremene tehnologije za komuniciranje sa svojim pratiocima i saučesnicima. Pandemija Covid-19 virusa je pokazla da savremeni svijet nije imun na takve pošasti koje su odnosile žrtve stoljećima unazad. Globalno zagrijavanje kao fenomen koji se različito manifestira u svim krajevima svijeta donosi i nama poprilično novij pojam a to su ekološki migranti, to su osobe koje su primorane napustiti svoje mjesto stanovanja zbog narušenog ekološkog ambijenta. Svakako svi ovi izazovi zahtijevaju zajedničko djelovanje u kapacitetu pod kojim je to moguće.

U dijelu koji se odnosi na regionalne izazove Bosna i Hercegovina je pozicionirana u Jugoistočnoj Europi. Ovaj region zbog svoje nerazivejnosti ima elemente koji bi mogli predstavljati određene izazove i opasnosti, no prevshodno se ovaj region u ovom dokumentu gleda kao trenzitna ruta zbog svog

geografskog položaja. U sigurnosnoj politici ze za regionalne izazove i rizike vežu elementi globalnih izazova i rizika što je u savremenoj svijetu i razumljivo. Sigurnosna politika (2006:4) za regionalne izazove navodi sljedeće: ”Po geostrateškom položaju, region jugoistočne Evrope se nalazi na važnim putevima između Evrope i Azije, posebno značajnim sa stanovišta trgovinske razmjene. To su istovremeno i putevi za ilegalnu trgovinu naoružanjem, narkoticima, bijelim robljem, a mogu biti korišteni i za tranzit terorističkih grupa i sredstava za izvođenje terorističkih akcija. Region je u posljednjoj deceniji 20. vijeka bio poprište različitih sukoba, koji su ostavili određene ekonomske, psihološke, socijalne i druge posljedice. U ovom području su još prisutna nastojanja za secesijom, autonomijom i nezavisnošću određenih etničkih grupa, što, uz relativno visoku koncentraciju vojnih kapaciteta, dodatno usložnjava ukupno sigurnosno stanje”. Također se kao sigurnosni izazov i prijetnja spominje separatizam, u cjelini od usvajanja ovog dokumenta ništa se znatno nije promjenilo u regionu Jugoistočne Europe, jedino veći akcenat je stavljen na migrante i migrantske rute koje predstavljaju više društveni izazov za države, iz razloga što upravo migranti ovaj region gledaju kao tranzitno područje a ne kao cilj gdje se žele zadržati.

Unutrašnji izazovi se u Odbrambenoj politici Bosne i Hercegovine (2008:4, u Lisica, Bajramović, 2021:221-222) definiše kao: Unutrašnji izazovi su: zaostali politički i društveni animoziteti, nepotpuna implementacija Općeg okvirnog sporazuma za mir u BiH, problemi političke i ekonomske tranzicije, problem zaštite granica; problem viška naoružanja i municije i ilegalnog oružja, kontaminacija teritorije minama i neeksplodiranim ubojnim sredstvima i prirodne i druge katastrofe i nesreće. Politički ciljevi Bosne i Hercegovine u oblasti odbrane su da se podrži ostvarivanje „općesigurnosnih državnih ciljeva definiranih dokumentom Sigurnosna politika Bosne i Hercegovine i prioriteta vanjske politike Bosne i Hercegovine.“. Slično kao u prethodnom tekstu u Sigurnosnoj politici se smatra da su unutrašnji izazovi produkt političkih faktora koji izazivaju i ostale vrste nestabilnosti. Te su identificirani između ostalog ”zaostali politički i društveni animoziteti, nepopuna implemnetacija Daytonskog mirovnog sporazuma, nedovoljna sredstva za realizaciju održivog povratka, problemi političke tranzicije, problemi tranzicije ka tržišnoj ekonomiji, nedovoljna zaštićenost granica, visoka stopa nezaposlenosti i sve što ona nosi, naoružanje i municija koja se drži u neadekavtnim skladištima, i nelagalno držanje kod pojedinaca, veliki broj nagaznih mina i razni ekološki izazovi. (Sigurnosna politika Bosne i Hercegovine, 2006:5)

3.1.4 Procjena sigurnosnih kretanja u BiH i okruženju

Procjena sigurnosnih kretanja u BiH i okruženju predstavlja završni dio Stanja u sigurnosnoj politici Bosne i Hercegovine, u ovom dijelu se vrši identifikacija izazova i rizika, na globalnom nivou je naveden Irak, dok na nivo Balkana je navedeno Kosovo, uzimajući u vidu da je dokument sigurnosne politike usvojen 2006., a Kosovo proglasilo nezavisnost 2008. godine, predstavlja još jedan razlog za usvajanje nove Sigurnosne politike BiH. I u ovom dijelu se navodi težnja ka Euroatlantskim integracijiama, kao potrebu za smanjenje rizika od konflikta, te se identificiraju određeni problemi kao što su ekonomski i socijalni. Terorizam se izravno predstavlja kao jedan od najvećih prijetnji po stabilnost Bosne i Hercegovine i regiona.

Potreba za boljom saradnjom između policijskih agencija unutar države, ali i sa međunarodnim agencijama je prepoznata i u ovom dokumentu, te se za to navodi sljedeće: ”U tim namjerama treba posmatrati i neophodnost jače povezanosti službi sigurnosti u Bosni i Hercegovini, uključujući i graničnu, ali i jaču saradnju sa međunarodnim policijskim organizacijama, posebno Interpolom, te policijama pojedinih zemalja iz okruženja i šire, kako bi se preventivno djelovalo na onemogućavanje izvođenja terorističkih akata u BiH ili korištenje njene teritorije za tranzit.” (Sigurnosna politika Bosne i Hercegovine, 2006:6)

Potreba za boljim nadzorom i kontrolom granica je predstavjena u ovom dokumentu, također je definisana potreba za boljom saradnjom i u ovoj oblasti zaštite od ilegalnih migracija i krijumčarenja. Još jednom se potvrđuje interes za borbu protiv terorizma, te se on veže i sa svim ostalim oblicima kriminala kao što su: ” organizovanog, uglavnom prekograničnog, kriminala, počev od finansijskog (pranje i falsifikovanje novca, korupcija), trgovine drogom i oružjem, preko trgovine ljudima i ljudskim organima do organizovane prostitucije” (Sigurnosna politika Bosne i Hercegovine, 2006:6). U završnom dijelu se navode mogućnosti od nuklearne opasnosti i narušavanja sigurnosti u BiH od strane istog, te da Bosna i Hercegovina može biti ruta za transport nuklearnih materija.

3.1.5 Elementi i ciljevi sigurnosne politike

Imamo sedam elemenata sigurnosne politike, to su:

- Vanjska politika;
- Unutrašnja politika;
- Odbrambena politika;
- Socijalna politika;
- Finansijska politika;
- Demokratizacija i ljudska prava i
- Zaštita čovjekove okoline.

Djelovanje i pravci vanjska politike u Sigurnosnoj politici (2006:7) definisani su kao: "Vanjska politika BiH usmjerena je ka očuvanju i unapređenju trajnog mira, sigurnosti i stabilnog demokratskog i sveukupnog državnog razvoja. U međunarodnim odnosima, aktivnosti BiH zasnivaju se na principima koji su sadržani u Povelji UNa, Završnom aktu iz Helsinkija i ostalim dokumentima Organizacije za sigurnost i saradnju u Evropi, te na općeprihvaćenim principima međunarodnog prava." Također je navedeno i puno poštivanje deklaracija Europske unije i korištenje mehanizama EU, te poštivanje i drugih deklaracija kojih je Bosna i Hercegovina potpisnik a koji se odnose na vanjsku politiku.

Opredjeljenja po pitanju unutrašnje politike su navedena na sljedeći način: " Unutrašnja politika Bosne i Hercegovine ima za cilj da doprinosi stabilnosti i sigurnosti kroz zaštitu ustavnog uređenja, razvitak demokratskog političkog sistema, jednakopravnosti naroda i građana i poštivanju ljudskih prava i osnovnih sloboda, održavanju trajnog mira, kao i drugih, Ustavom utvrđenih, vrijednosti. U cilju zaštite ustavnog poretka, izvršena je reorganizacija i dogradnja ustavnopravnog i sigurnosnog sistema" (Sigurnosna politika Bosne i Hercegovine, 2006:8). U sigurnosnoj politici su predstavljeni oblici ugrožavanja unutrašnje sigurnosti i opredjeljenja za borbu protiv istih.

Odbrambena politika kao i što sam naziv kaže, odnosi si na odbrambene kapacitete neke države u ovom slučaju Bosne i Hercegovine, te predstavlja važan dio prethodno navedenih politika. U sigrunosoj politici su navedeni sljedeći prinvipi odbrambene politike:

- ”demokratskoj, civilnoj kontroli vojske, uz parlamentarni nadzor;
- transparentnosti aktivnosti u oblasti odbrane, uključujući planiranje i budžetiranje odbrane;
- uravnoteženosti snaga i mogućnosti unutar Bosne i Hercegovine, podregija i jugoistočne Evrope;
- modernizaciji snaga, uključujući razvoj interoperabilnosti Oružanih snaga Bosne i Hercegovine s NATOom;
- integraciji u evroatlantske kolektivne sigurnosne strukture;
- saradnji u oblasti kontrole naoružanja i mjerama izgradnje sigurnosti i povjerenja, uključujući učešće u sigurnosnim strukturama i protokolima jugoistočne Evrope;
- izgradnji sistema odbrane, zasnovanog na navedenim principima, čime će Bosna i Hercegovina realizovati ciljeve odbrambenih reformi na putu od individualne ka kolektivnoj sigurnosti.” (Sigurnosna politika Bosne i Hercegovine, 2006:10)

Socijalna politika je isto tako regulisana Sigurnosnom politikom Bosne i Hercegovine (2006:12-13), te je za nju navedeno sljedeće: ”Bosna i Hercegovina će omogućiti potpunu pokrivenost osnovnom zdravstvenom zaštitom na cijeloj teritoriji, posebno imajući u vidu ugrožene kategorije: povratnike, raseljena lica, djecu i Rome i omogućiti pokretljivost tih prava unutar zemlje. Kontrola sigurnosti hrane i vode, kao javno zdravstveno pitanje, bit će provođena i praćena u skladu s evropskim standardima. Trgovina lijekovima i narkoticima, uključujući uvoz, proizvodnju i promet, bit će regulisana državnim zakonima, i osigurat će stroge mehanizme kontrole njihovog provođenja, uz osnivanje državne Agencije za lijekove.” Bosna i Hercegovina će i u socijalnoj politici slijediti Evropsku socijalnu povelju i Povelju o socijalnoj zaštiti, također se navodi i donošenje socijalne strategije u skladu sa socijalnom politikom.

Povezanost sigurnosnog sektora se ekonomski sektorom u savremenom svijetu je neminovna, iz tog razloga sigurnosna politika obrađuje i dio koji se odnosi na finansijsku politiku. U ovom dijelu su navedni

rezultati koji su postignuti u ekonomskom smislu koji se odnosi na obnovu infrastrukture, te je iznesena potreba ja jačanjem i vraćanjem povjerenja u domaći bankarski sistem. Potrebe za saradnjom sa susjednim državama i državama regiona su jedna od mjera za jačanje ekonomskog sektora. Također se navodi potreba za ekonomski reformama i ekonomskoj sigurnosti Bosne i Hercegovine.

Politika demokratizacije i ljudskih prava regulisana je ustavom i međunarodinim instrumentima, a u Sigurnosnoj politici (2006:14) se navodi: "Bosna i Hercegovina je prihvatila osnovne međunarodne instrumente koji regulišu zaštitu ljudskih prava i sloboda, od kojih je većina uključena u Ustav Bosne i Hercegovine kao standard za zaštitu ljudskih prava i sloboda. Na osnovu međunarodnih standarda, Bosna i Hercegovina ima obavezu da implementira odgovarajuće mjere s ciljem podizanja standarda zaštite osnovnih ljudskih prava i sloboda, među kojima je jedan od osnovnih principa pravo na ličnu slobodu i sigurnost." Mogućnost političke participacije i uživanja svih građanskih prava i sloboda su dolike savremenih demokratskih društava, iz priloženog vidimo da BiH teži ka tome. Svakako postoji potreba za efikasnijim strukturama koji štite građane od različitih obilka ugrožavanja, ali također se navodi i potreba za reformom pravosudnog sistema.

I posljednja politika koja se odnosi na zaštitu čovjekove okoline, ekološki segment čini jako važan dio sistema sigurnosti, jer izravno može negativno uticati na čovjeka ili grupu ljudi. U sigurnosnoj politici (2006:16) po pitanju ovog pojma navodi sljedeće: "Zaštita čovjekove okoline odnosi se na poslove zaštite vodnih resursa, zraka, zemljišta i biljnog materijala. Zagađivanje okoline globalni je problem, a njena zaštita globalni zadatak, zbog čega zemlje koje se ne ubrajaju u bogate, s pravom računaju i na podršku međunarodne zajednice. Pitanje zaštite flore i faune, zraka i vode, postaje jedno od urgentnih pitanja s kojima se danas suočava čovječanstvo, a time i prvorazredno političko i sigurnosno pitanje". Ovo pitanje u dobija sve više na važnosti kako na globalnom nivou tako i na državnom. Ovaj dokument predviđa pobaljšanja usaglašavanje domaćih zakona za zakonima EU. Problem isto tako predstavlja odlaganje otpada svih vrsta, te vidi potrebu za jačanje institucija i sektora zadušenih za ovu problematiku.

Ovaj dokument predviđa ispunjavanje sljedećih pretpostavki:

- ”uspostavljanje i razvoj institucija sistema sigurnosti koje će biti sposobne da odgovore na sve rizike i prijetnje osnovnim vrijednostima i interesima Bosne i Hercegovine;
- aktivno učešće u izgradnji kolektivne sigurnosti na regionalnom i globalnom planu putem pristupanja međunarodnim sigurnosnim konvencijama, evropskim i evroatlantskim strukturama;
- oporavak i razvoj privrednog potencijala, čime će se dugoročno obezbijediti resursi i sredstva za efikasno suprotstavljanje sigurnosnim rizicima i prijetnjama.” (Sigurnosna politika Bosne i Hercegovine, 2006:17)

Jačanje kapaciteta za nadzor i kontrolu granica, saradnja policijskih agencija na unutardržavnom i međunarodnom nivou, saradnja sa susjednim državama i državama regiona, pristupanje EU i NATO-u su neki od ciljeva pobrojani u Sigurnosnoj politici. Dok kao krajni cilj u Sigurnosnoj politici (2006:18) se navodi ”Bosna i Hercegovina u bliskoj budućnosti dostigne nivo samoodrživog mira i društvene stabilnosti koji će omogućiti povlačenje misije međunarodnih snaga iz Bosne i Hercegovine, te dalji svestrani prosperitet zemlje.”

3.1.6 Provođenje sigurnosne politike

U ovom dijelu se navode nadležnosti zakonodavnih i izvršnih organa u provođenju sigurnosne politike, te navodi da Predsjedništvo BiH usvaja Sigurnosnu politiku, te da sve što je u domenu sigurnosne politike informiše Parlamentarnu skupštinu BiH. Skupštine na svim nivoima predstavljaju instutcionalni i politički nivo oblikovanja i provođenja sigurnosne politike, ili nekih dijelova u skladu sa ovlaštenjima. Važnost parlamenata u sprovođenju sigurnosne politike se ogleda u sljedećem ” Navedeni parlamenti određuju zakonske okvire i dugoročne smjernice razvoja Sigurnosne politike, te osiguravaju materijalne pretpostavke za njeno provođenje. Poseban značaj za njeno provođenje ima ostvarivanje i razvijanje parlamentarne kontrole nad funkcionisanjem i radom svih elemenata sigurnosnog sekto ra na svim nivoima. U mjeri u kojoj je potrebno,

Parlamentarna skupština BiH i entitetski parlamenti formiraju stručna tijela, putem kojih se vrši procjena stanja u oblasti sigurnosti" (Sigurnosna politika Bosne i Hercegovine, 2006:18). Također Vijeće ministara BiH i vlade entiteta kao predstavnici izvršne vlasti imaju nadelžnosti u sporvođenju sigurnosne politike, ili nekih dijelova.

Važnost saradnje i efikasnost sistema je navedena u završnom dijelu koji se odnosi na Provođenje sigurnosne politike:

Organi izvršne vlasti svih nivoa će, unapređujući međusobnu saradnju, doprinositi institucionalnom razvoju i harmonizaciji struktura, funkcija i napora izvršne vlasti od značaja za sigurnost i stabilnost BiH. Na ovaj način će se postići efikasnije korištenje raspoloživih resursa i podići nivo sigurnosti. Od posebnog značaja je preuzimanje odgovornosti za vlastiti razvoj i stabilnost, kroz uvažavanje prihvaćenih evropskih standarda i kroz razvijanje partnerskog odnosa s prisutnim predstavnicima i institucijama međunarodne zajednice. (Sigurnosna politika Bosne i Hercegovine, 2006:18)

4. UPRAVLJANJE INFORMACIJAMA I ZAŠTITA PODATAKA U SISTEMU SIGURNOSTI BOSNE I HERCEGOVINE

4.1 *Upravljanje informacijama i zaštita podataka u sistemu sigurnosti Bosne i Hercegovine*

Kada govorimo općenito o pojmu upravljanja informacijama, ovaj pojam sačinjavaju poprilično interdisciplinarnu primjenu. Upravljanje informacijama u sektoru informacionih tehnologija popularno nazvanog IT sektor ima različito značenje od onoga koji se koristi u informativno-marketinškom sektoru, ili onoga koji je za naš rad od velike važnosti sektor sigurnosti. IT sektor iz dana u dan ima sve više uticaja na život običnog čovjeka, kroz svakodnevne aktivnosti čovjek se susreće sa proizvodima i servisima iz tog sektora, te sam nije svjestan obima koji IT sektor reguliše, od bankarskih, obrazovnih i medicinskih i mnogih drugih oblasti.

Kada govorimo o informativno-marketinškom sektoru prevashodno mislimo na sredstva javnog informisanja, ali i za taj marketinški sektor za kojeg su isto tako informacije i upravljanje informacijama jako važno. Za razliku od IT sektora, informativni sektor kroz višednevno i svakodnevno komuniciranje i informisanje građana ima i više utjecaja na svakodnevni život istih. Kada govorimo o zajedničkim elementima IT i informativno-marketinškog sektora to su informacije, upravljanje informacijama i uticaj na svakodnevni život građana. Razlike između ova dva sektora bi se mogle predstaviti kroz krizne odnosno vanredne situacije, kada IT sektor dođe pod određene napade i ili za neki vremenski period ne funkcionišu servisi koji su u njegovom domenu, građani to odma osjete. informativno-marketinški sektor ima mogućnost da građane uvede, koliko je to moguće, u kriznu situaciju, i svakodnevnim izvještajima informiše, neinformiše ili dezinformiše o stvarnim događajima na terenu.

Kada govorimo o upravljanju informacijama u sistemu sigurnosti, to možemo predstaviti na nivo sutrukture jedne institucije ili agencije naprimjer Ministartsva odbrane ili Obavještajno-sigurnosne agencije Bosne i Hercegovine (u daljem tekstu OSA BiH), ili na nivou neke grupe institucija koje imaju neki oblik saradnje ili zajedničkih aktivnosti, na bilo kojem bolju društvenih zbivanja. Kada govorimo o upravljanju i zaštiti podataka na oba prethodna nivoa oni su regulisane politikama, strategijama, standardima, smjernicama, zakonima, podzakonskim aktima i pravilnicima.

Kada govorimo o upravljanju informacijama to bi predstavljalo kombinaciju i institucija iz sfera sigurnosti jedne države, informativnog sektora i IT sektora. Trenutna dešavanja na polju sigurnosti informacija i podataka zahtijevaju sve veću uključenost i "snagu" IT sektora koja se ogleda na savremenosti tehnologija koje se koriste i obučenosti i obrazovanosti kadara koje ih koristi. Jedna od definicija sigurnosti informacija glasi:

Sigurnost informacija osigurava povjerljivost, dostupnost i integritet informacija. Informaciona sigurnost podrazumijeva primjenu i upravljanje odgovarajućim kontrolama koje podrazumijevaju razmatranje širokog spektra prijetnji, s ciljem osiguravanja održivog poslovnog uspjeha i kontinuiteta, te minimiziranja posljedica incidenata informacione sigurnosti. (International standard ISO/IEC 2700, 2016:15)

Danas glavni rizik po upravljanje informacija i sigurnosti podataka upravo dolazi iz pravca IT sektora, odnosno cyber prostora, te iz toga proizilazi potreba za tijesnom saradnjom faktora iz sistema sigurnosti jedne država sa IT sektorom, koji je u mnogim državama postao važan element u tom sistemu.

4.1.1 Definisanje pojma informacija

Razmjenivanje podataka i informacija su sastavni dio svake komunikacije, s tim da stavljanje određnog podataka ili više njih u kontekst dobijamo informaciju. Autor Mecanović (1991:15) informaciju smatra i robom koju potrošać nastoji svakodnevno konzumirati :" Informacija za pojedinca predstavlja način spoznaje o nizu pojava, događaja, saznanja i sl., koji su u domeni njegovog interesa, odnosno potrošačke potrebe, koja se opet može zadovoljavati konstantnim praćenjem novih pojava, događaja, saznanja o različitim predmetima i sl. Prema tome, informacija kao roba u pravilu spada u proizvod dnevne potrošnje koju kupac konzumira dnevno, tražeći sutra novi set informacija. " Iz prethodno navednog možemo zaključiti da same informacije možemo podijeliti na one koje su namjenje i interesantne široj populaciji za svakodnevno "konzumiranje", te služe kao svojevrsni instrument, ali i one koje se odnose na komunikaciju i funkcionisanje elemenata nekog sistema. Dok u konteksu Međunarodnih standarda koje se bave ovim poljem informacija se definiše u puno širem smislu, tako da oni navode:

Informacija je imovina koja je, kao i druga važna poslovna imovina, neophodna za poslovanje organizacije i shodno tome mora biti na odgovarajući način zaštićena. Informacije se mogu pohraniti u mnogim oblicima, uključujući: digitalni oblik (npr. datoteke pohranjene na elektronskim ili optičkim medijima), materijalni oblik (npr. na papiru), kao i nepredstavljene informacije u obliku znanja zaposlenih. Informacije se mogu prenositi na različite načine uključujući: kurirsku, elektronsku ili verbalnu komunikaciju. Bez obzira na oblik informacije ili način na koji se informacije prenose, uvijek im je potrebna odgovarajuća zaštita. (International standard ISO/IEC 2700, 2016:15)

4.2 *Upravljanje informacijama u sistemu sigurnosti Bosne i Hercegovine*

Kada govorimo o upravljanju inofrmacijama u nekom sistemu sigurnosti, prvo pitanje koje se postavlje se odnosi na efiksnost tog sistem, odnosono sigurnost samih informacija u tom sistemu. U Bosni i Hercegovini informaciona sigurnost regulisana je *Politikom upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period od 2017. do 2022. godine* (u daljem tekstu Politika). U ovome dokumentu se navodi na se informaciona sigurnost tretira po standardu ISO/IEC 27001[2], te da se ovaj dokument odnosi i na oblast tajnih podataka.

Ova politika u članu 1. koji se odnosi na Opće o informacionoj sigurnosti, stavka 1.1. Pojam informacione sigurnosti navodi sljedeće: ”Naime, informaciona sigurnost se odnosi na zaštitu informacija bez obzira na medij na kome se čuva i prijenosi. Sistemom informacione sigurnosti obuhvataju se fizička lica, procesi, organizacija i tehnologija. Taj sistem se sastoji od uravnoteženog skupa sigurnosnih mjera, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacionih sistema, koordiniranog uvođenja formalnih procedura, kao što su procjene rizika, certificiranje uređaja i akreditacije tehničkih sistema za primjenu u određenim segmentima poslovnih procesa u Institucijama. Uravnoteženost i koordinacija mjera i postupaka treba da se postiže organizacijom i upravljanjem sistemom informacione sigurnosti.”

[2] ISO/IEC 27001- Međunarodni standard koji se odnosi na Upravljanje sigurnošću informacija.

Ova Politika također reguliše i predstavlja mehanizme zaštite i sprječavanja te ih dijeli na tri osnovna nivoa:

- **fizička sigurnost**, pod kojom se smatra sigurnost računarske opreme i podataka,
- **lična sigurnost**, koja podrazumijeva zaštitu korisnika i povjerljivih informacija o korisniku,
- **sigurnost institucije**, koja proizilazi iz prva dva nivoa. (Politika upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017-2022. godine, 2017)

Iz gore navedenog možemo uvidjeti da su zaštita računarske opreme i podataka i zaštita samog korisnika i njegovih ličnih podataka u bliskoj korelaciji sa sigurnošću same institucije. Ako uzmemo u obzir da su oprema i podaci, kao i sam korisnik, odnosno uposlenik i jegovi lični podaci vezani za institucije ili agencije iz sektora sigurnost, postoji potreba za podizanjem opreza i kontrole na viši nivo.

4.2.1 Definisanje sigurnosnih zahtjeva

Kada govorimo o definisanju sigurnosnih zahtjeva koji se odnose na upravljanje infomacijama od sigurnosnog značaja ova Politika nam navodi tri kategorije:

- Procjena rizika, uzimajući u obzir poslovnu strategiju institucije i njezine ciljeve. Na ovaj način se identificiraju prijetnje imovini institucije, njezina ranjivost i određuje vjerovatnost pojave prijetnji, kao i njihov utjecaj na instituciju ukoliko se te prijetnje realiziraju;
- Ustavne, zakonske i ugovorne obaveze koje institucija mora zadovoljiti;
- Skup ciljeva, načela i poslovnih zahtjeva institucije. (Politika upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017-2022. godine, 2017)

Prva kategorija koja se odnosi na procjenu rizika u ovom kontekstu, upravljanja i sigurnosti informacija je od važnosti za sve institucije na svim nivoima, ali iz našeg rada prevashodno smo koncentrisani na instiucije sigurnosti. Ministarstvo sigurnosti i Ministarstvo odbrane kao institucije od izuzetnog sigurnosnog značaja na državnom nivou, imaju potrebu za izuzetno detaljnim procjenama rizika. Ustavnim, zakonskim, podzakonskim aktima i pravilinicima regulisani su odnosi unutar držanih, entitetskih i kantonalnih ministarstava i državnih agencija.

Politika upavljanja informacijskoj sigurnošću (2017) nam navodi i aktivnosti koje postižu dobre rezultate po pitanju upravljanja informacijama, a to su:

- sigurnosna politika;
- podjela odgovornosti informacione sigurnosti;
- svijest o informacionoj sigurnosti, edukacija i trening;
- ispravno procesiranje podataka u aplikacijama;
- upravljanje ranjivostima;
- upravljanje poslovnim kontinuitetom;
- upravljanje sigurnosnim incidentima i poboljšanjima sistema. (Politika upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017-2022. godine, 2017)

4.2.2 Procjena rizika i izbor odgovarajućih kontrola

Kada govorimo o procjeni rizika postoji potreba za prethodnom definicijom samo pojma:

Rizik se definira kao učestalost i intenzitet štetnih posljedica ili očekivanih gubitaka po zdravlje, život i socijalni status ljudi, imovinu i druga dobra, te životne uvjete i okoliš, koje su rezultat interakcije između opasnosti[3] i prijetnji prouzročenih prirodnim pojavama, nenamjernim ili namjernim ljudskim djelovanjem u uvjetima ranjivosti objekata ugrožavanja (Lisica, Bajramović, 2021:66).

A za sam pojam procjena rizika isti autori navode sljedeće ”*Procjena rizika podrazumijeva identifikaciju i analizu njegovih elemenata i njihove međusobne interakcije*” (Lisica, Bajramović, 2021:66). Definisanjem pojma procjene rizika uvdijeli smo potrebu za pronalaženjem faktora koji su sastavni dio same procjene, te njihovog međusobnog uticaja za moguće štetno djelovnje po sistem ili strukturu sigurnosti unutar neke države. Politika upravljanja informacionom sigurnošću (2017) nam za izbor odgovarajućih kontrola navodi sljedeće: ”Kako bi se rizik sveo na prihvatljiv nivo, nakon identificiranja sigurnosnih zahtjeva i izrade procjene rizika, potrebno je izabrati i implementirati adekvatne kontrole. Izbor kontrola zavisi o instituciji, odnosno prihvatljivosti rizika i načinu upravljanja rizikom, ali i o

[3]Po svojoj definiciji, opasnost je nešto širi pojam od prijetnje. Ono što razlikuje prijetnje od opasnosti je postojanje zle namjere. Zlonamjerno djelovanje nekog protivnika karakteristično za prijetnje, nužno ne postoji kod opasnosti. Opasnosti su uglavnom rezultat nenamjernog djelovanja ljudi ili mogu biti prouzročene prirodnim nepogodama izvan ljudske kontrole. One ne uključuju direktnu namjeru protivnika prema određenom cilju. (Lisica, Bajramović, 2021:55)

državnim i međunarodnim zakonskim pravima i obavezama". Kao što je navedeno izbor kontrola zavisi od institucija i od prihvatljivosti rizika[4], tako da bi institucije iz oblsiti sigurnosti provodili određene sigurnosne provjere i kontrole. Kada su u pitanju institucije iz sektora sigurnosti one u praksi predstavljaju *sigurnosne rizike,* a njih definišemo kao:

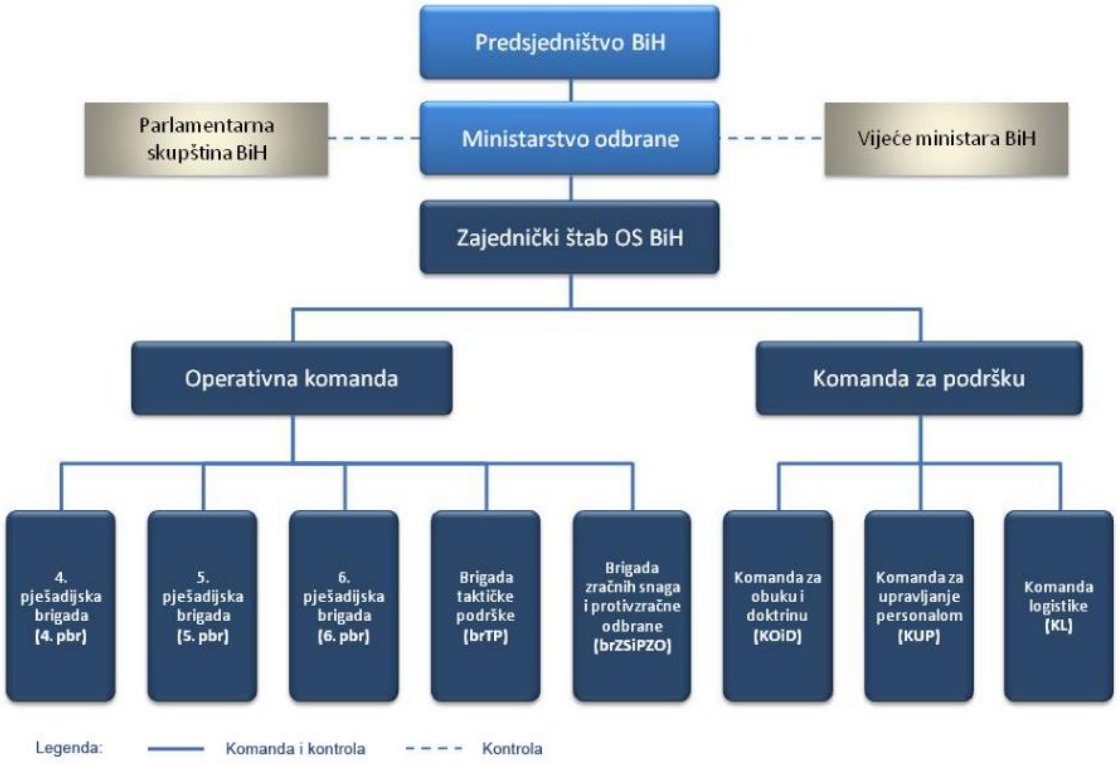
Sigurnosni rizici su specifična vrsta rizika koji su procijenjeni i ugrađeni u sigurnosne i obrambene planove, strategiju obrane i strategiju nacionalne sigurnosti, te sigurnosnu politiku zemlje. Njihov izvor je u opasnostima i prijetnjama proizišlih iz ljudskog djelovanja, čiji nosioci posjeduju sposobnost da namjerno ili nenamjerno izazovu štetu kojom se ugrožavaju ljudi, imovina, informacije i društvo u cjelini, u mjeri koja predstavlja sigurnosni izazov. (Lisica, Bajramović, 2021:67)

4.3 *Upravljanje informacijama u Ministarstvu odbrane Bosne i Hercegovine*

Kada govorimo o Ministarstvu odbrane Bosne i Hercegovine, struktura i uređenje ovog ministarstva se temelji na dokumentu iz 2005. godine, a koje nosi naziv Zakon o odbrani Bosne i Hercegovine. Kada govoriomo za period od proglašenja nezavisnosti u BiH je djelovalo Ministarstvo odbrane Repubilke Bosne i Hercegovine. Pored tadašnjeg republičkog ministarstva postojala su još dva ministartsva odbrane i to Republike Srpske i Hrvatska zajednica Herceg-Bosna. Spajanjem Armije Republike Bosne i Hercegovine i Hrvatskog vijeća obrane nastaje Vojska Federacije Bosne i Hercegovine. Zakonom o odbrani iz 2005. godine nastaje jedinstvena vojna formacija na području cijele teritorije Bosne i Hercegovine, a to su Oružane snage Bosne i Hercegovine.

[4] U širem smislu značenja, svi rizici se mogu smatrati sigurnosnima, ako se sigurnost promatra kao stanje, odnosno kao odsustvo izvora rizika – opasnosti, prijetnji i izazova. Sigurnosni rizici utječu na oblikovanje nacionalnih interesa i sigurnosnih ciljeva kroz njihovu interakciju sa temeljnim društvenim vrijednostima.14 Oni su specifični i po tome što se njihovom identifikacijom, procjenom i suzbijanjem bavi sektor sigurnosti. (Lisica, Bajramović, 2021:67)

4.3.1 Struktura Ministarstva odbrane Bosne i Hercegovine



Slika 2.- Struktura Ministarstva odbrane Bosne i Hercegovine

(izvor: www.mod.gov.ba)

Kada govorimo o strukturi Ministarstva odbrane i gore navedene ilustracije možemo vidjeti da vrhovnu komandu posjeduje institucija Predsjedništva Bosne i Hercegovine, kontrolu nad Ministarstvom odbrane vrše Parlamentarna skupština i Vijeće ministara Bosne i Hercegovine. Ministarstvo odbrane je direktno nadređeno Zajedničkom štabu Oružanih snaga Bosne i Hercegovine, dok je on nadređen Operativnoj komandi i Komandi za podršku. Opertivna komanda je nadređena brigadama i provodi politike Zajedničkog štaba, dok je Komanda za podršku nadređena: Komandi za obuku i doktrinu, Komandi za upravljanje personalom i Komandi logistike.

4.3.2 Sektori unutar Ministarstva odbrane Bosne i Hercegovine

U Ministartsvu odbrane je sljedeća sektorska podjela: Generalni inspektorat, Sektor za politiku i planove, Sektor za međunarodnu saradnju, Sektor za obavještajno-sigurnosne poslove, Sektor za komandu, kontrolu i komunikacije, kompjutere i upravljanje informacijama, Sektor za upravljanje personalom, Sektor za nabavku i logistiku i Sektor za finansije i budžet.

Za ovaj rad su nama važni Sektor za obavještajno-sigurnosne poslove i Sektor za komandu, kontrolu i komunikacije, kompjutere i upravljanje informacijama. Nadležnosti Sektora za obavještajno-sigurnosne poslove su: ”Sektor za obavještajno-sigurnosne poslove vrši poslove i odgovoran je za uspostavljenje i upravljanje obavještajno-sigurnosnog sistema, uključujući prikupljanje i obradu vojno obavještajnih podataka za Ministarstvo odbrane, Zajednički štab, Operativnu komandu i druge strukture odbrane kao, po potrebi, i za pružanje ulaznih podataka i informacija inostranog vojnog obavještavanja civilnim obavještajnim agencijama BiH”. (Ministarstvo odbrane Bosne i Hercegovine (n.d.). Izvor: www.mod.gov.ba)

Kada govorimo o Sektoru za komandu, kontrolu i komunikacije, kompjutere i upravljanje informacijama, on djeluje u okviru sljedećih nadležnosti: ” Sektor za komandu, kontrolu, komunikacije, kompjutere i upravljanje informacijama vrši poslove u vezi sa uspostavljanjem interoperabilnog komunikacijskog sistema, te upravljanje informacijama i kompjuterskom tehnologijom koja se odnosi na komunikacije i upravljanje informacijama u cijelom odbrambenom sistemu BiH”. (Ministarstvo odbrane Bosne i Hercegovine (n.d.). Izvor: www.mod.gov.ba)

4.3.3 Zakon o odbrani Bosne i Hercegovine

Kada govorimo iz domena upravljanja informacijama i zaštite podataka iz Zakona o odbrani BiH (2005), u odjeljku A. koji se odnosi na nadležnosti Bosne i Hercegovine, članu 9. (Vojnoobavještajni poslovi) se navodi sljedeće nama od važnosti:

1) Planiranje, kontrola i obavljanje svih vojnoobavještajnih poslova spada u nadležnost Bosne i Hercegovine. Vojno obavještavanje je rod Oružanih snaga koji prikuplja, obrađuje i distribuira informacije u vezi s Oružanim snagama, s ciljem podrške vojnih misija Oružanih snaga.
2) Osim dužnosti propisanih u stavu (1) ovog člana, vojnoobavještajni rod Oružanih snaga pružit će pomoć Obavještajno-sigurnosnoj agenciji Bosne i Hercegovine u prikupljanju strateških vojnih podataka i vršenju protuobavještajnih aktivnosti.
3) Prikupljanje strateških vojnih podataka i obavljanje protuobavještajnih aktivnosti iz stava (2) ovog čana, koje zahtijeva posebne istražne aktivnosti i upotrebu tehničkih sredstava za nadgledanje, obavlja isključivo Obavještajno-sigurnosna agencija Bosne i Hercegovine, u skladu sa Zakonom o Obavještajnosigurnosnoj agenciji Bosne i Hercegovine („Službeni glasnik BiH“, br. 12/04 i 20/04).
4) Koordinacija između vojnoobavještajnog roda Oružanih snaga i Obavještajno-sigurnosne agencije Bosne i Hercegovine detaljnije se ureuje sporazumom koji će ministar odbrane Bosne i Hercegovine i generalni direktor Obavještajno-sigurnosne agencije Bosne i Hercegovine potpisati najkasnije 30 dana nakon stupanja na snagu ovog zakona.

Iz navedenog teksta možemo uvidjeti da Oružane snage BiH mogu u saradnji sa Obavještajno-sigurnosnom agencijom djelovati po pitanju vojnoobavještajnih poslova, odnosno nisu u domenu civilnih odnosa. Također i ministar odbrane ima nadležnost da planira i nadzire vojnoobavještajne radnje Oružanih snaga, zamjenik ministra odbrane za politika također ima odgovornost prema vojnoobavještajnim radnjama i sigurnosti. Dok u okviru Zajedničkog štaba, zamjenik načelnika ima nadležnosti u okviru vojnoopbaještajnih i kontraobavještajnih radnji. Nadležnosti Parlamentarne skupštine Bosne i Hercegovine se ogledaju u tome da donosi propise o čuvanju tajnih podataka tokom istraga i razmatranja.

4.3.4 Dostupnost informacija u Ministarstvu odbrane Bosne i Hercegovine

Ova oblast unutar Ministarstva odbrane Bosne i Hercegovine regulisana je Registrom informacija koje možete dobiti od Ministarstva odbrane Bosne i Hercegovine iz 2021. godine. Nadležnost za informsanje od dostupnosti određenih podataka i informacije je u okviru Ureda za odnose s javnošću Ministarstva

odbrane. Ovom uredbom su predstavljene tri kategorije informacija koje su izuzete od otkrivanja, a odnose se na sljedeće:

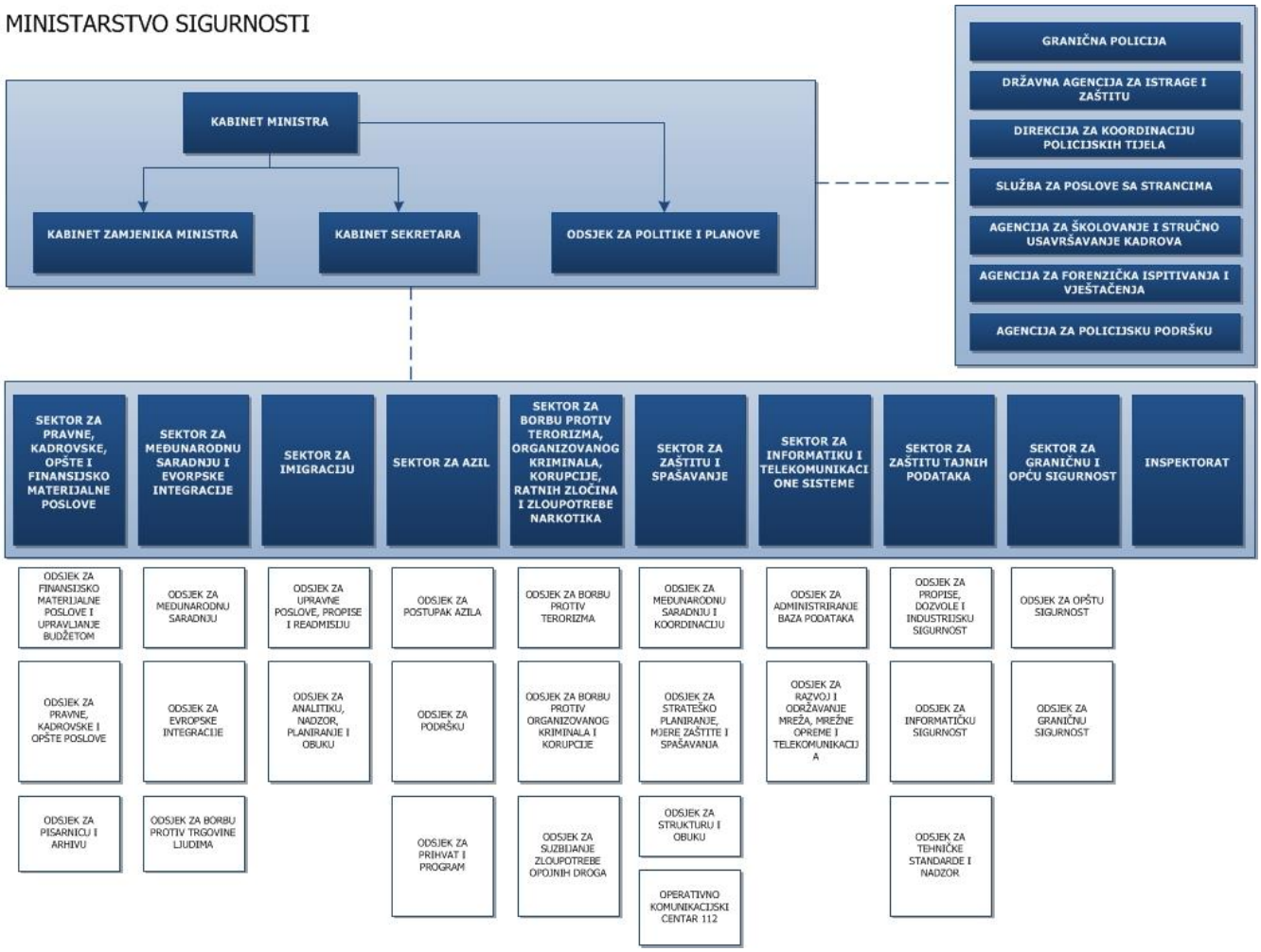
”Prva kategorija se odnosi na funkcije javnih organa. U smislu ove kategorije, izuzetak može biti utvrđen, u slučajevima:

- kada bi otkrivanje informacije izazvalo značajnu štetu po legitimne ciljeve,
- interesi odbrane i sigurnosti, kao i zaštita javne sigurnosti, sprečavanje kriminala i otkrivanje kriminala,
- zaštita postupka donošenja odluka u javnom organu (uključujući davanje mišljenja, savjeta ili preporuka, bilo da se radi o osobi zaposlenoj u javnom organu ili drugoj osobi koja radi za ili u ime javnog organa, s tim da to ne obuhvata činjenične, statističke, znanstvene ili tehničke informacije).

Druga kategorija izuzeća odnosi se na zaštitu komercijalno osjetljivih informacija treće strane, kada bi objavljivanje takve informacije moglo prouzrokovati štetu trećoj strani.

Treća kategorija izuzetaka je zaštita privatnosti druge osobe.” (Indeks Registar informacija koje možete dobiti od Ministarstva Odbrane Bosne i Hercegovine, 2021:2-3)

4.4 *Upravljanje informacijama i zaštita podataka u Ministarstvu sigurnosti Bosne i Hercegovine*



Slika br. 3.- Struktura Ministarstva sigurnosti Bosne i Hercegovine

(izvor: www.msb.gov.ba)

Kada govorimo o upravljanju informacijama i zaštiti podataka unutar Ministarstva sigurnosti BiH bitno je napomenuti i oragnizacionu strukturu samog ministarstva, te se ono sastoji od sljedećih sektora:

- Sektor za zaštitu i spašavanje,
- Sektor za pravne, kadrovske, opšte i finansijsko-materijalne poslove,
- Sektor za međunarodnu saradnju i evropske integracije,

- Sektor za imigraciju,
- Sektor za azil,
- Sektor za borbu protiv terorizma, organizovanog kriminala, korupcije, ratnih zločina i zloupotrebe narkotika,
- Sektor za informatiku i telekomunikacione sisteme,
- Sektor za zaštitu tajnih podataka,
- Sektor za opću i graničnu sigurnost, i
- Inspektorat.

Od važnosti za ovaj rad potrebno je istaknuti nadležnosti i rad dva sektora, a to su Sektor za informatiku i telekomunikacione sisteme i Sektor za zaštitu tajnih podataka.

4.4.1 Sektor za informatiku i telekomunikacione sisteme

Nadležnosti Sektora za informatiku i telekomunikacione sisteme su sljedeće, ” Sektor za informatiku i telekomunikacione sisteme vrši poslove koji se odnose na održavanje i otklanjanje kvarova na informatičkoj i mrežnoj opremi; administraciji mreže; nabavci aplikativnog softvera i njihovoj postavci na računar; standardizaciji sistemskog softvera i opreme; uvođenje i primjenu mjera zaštite podataka u informacionom sistemu; kreiranje i održavanje web stranice i mail servera; instaliranje i podešavanje potrebnih programskih rješenja na radnim stanicama korisnika; preventivno održavanje i testiranje instalirane računarske, mrežne i telekomunikacijske opreme; pronalaženje i otklanjanje kvarova na instaliranoj opremi i instalacijama; preventivno održavanje sistema za neprekidno napajanje; analizu rada softvera za baze podataka” (Ministarstvo sigurnosti BiH, n.d.izvor: www.msb.gov.ba). Iz navedenih nadležnosti vidimo da pored svakodnevnih poslova koji se odnose na održavanje informatičke opreme i telekomunikacijskih sistema, ovaj sektor ima i nadležnost koja se odnosi na uvođenje i primjenu mjera zaštite podataka u informacionom sistemu.

Ovaj sektor također posjeduje i dva odsjeka, a to su:

- Odsjek za razvoj i održavanje mreža i mrežne opreme i telekomunikacije, i

- Odsjek za razvoj i administriranje baza podataka.

Ministarstvo sigurnosti Bosne i Hercegovine (n.d.) kao nadležnosti Odsjeka za razvoj i održavanje mreža i mrežne opreme i telekomunikacija navodi sljedeće:

- uvođenje i primjena mjera zaštite podataka u informacionom sistemu, te usklađivanje dostignutog nivoa zaštite sa stalnim razvojem informacionih tehnologija;
- kreiranje i održavanje web stranice i mail servera Ministarstva, te uvođenje i primjena mjera zaštite web stranice i mail servera;
- instaliranje i održavanje telekomunikacijske, radio relejne i druge opreme za potrebe mreže policijskih organa;
- instaliranje i dopunjavanje operativnih sistema, održavanje i otklanjanje kvarova na informatičkoj i mrežnoj opremi, administriranje mreže, usmjeravanje rada na nabavci aplikativnog softvera i njihovoj postavci na računar.

Iz navedenog vidimo da je ovaj odsjek važan za tematiku kojom se ovaj rad bavi, te da same nadležnosti ovog odsjeka kao što su *uvođenje i primjena mjera zaštite podataka u informacionom sistemu, te usklađivanje dostignutog nivoa zaštite sa stalnim razvojem informacionih tehnologija* i *instaliranje i održavanje telekomunikacijske, radio relejne i druge opreme za potrebe mreže policijskih organa* imaju važnu ulogu po pitanju upravljanja informacija i zaštite podataka. Iz nadležnosti koja se odnosi na zaštitu podataka vidimo i oblast koja se odnosi na unapređenje i usklađivanje nivoa zaštite, te konstantan razvoj i prilagođavanja na ovom polju. Telekomunikacijska, radio relejna i druga oprema u sferi mreže policijskih organa je itekako važna u kontekstu upravljanja informacijama i zaštite podataka, te je u ovome dijelu rada posebno ističemo.

Odsjek za razvoj i administriranje ima sljedeće nadležnosti:

- projektovanje i izrada baza podataka, definisanje načina i strategije pravljenja sigurnosnih kopija baza podataka, te pravljenje sigurnosnih kopija, analiziranje softvera za razvoj baza podataka; i

- razrada softvera za baze podataka i njihovo postavljanje na računar, analiza rada softvera za upravljanje bazama podataka, administriranje baza podataka, dodjeljivanje korisnicima prava pristupa podacima. (Ministarstvo sigurnosti BiH, n.d. izvor: www.msb.gov.ba)

Ovaj odsjek se više odnosi na pojam zaštite podataka i njegove nadležnosti se odnose na izradu i strategiju zaštite baza podataka, te pravljenje sigurnosnih kopija i dodjeljivanje korisncima pravo pristupa istim tim bazama podataka.

4.4.2 Sektor za zaštitu tajnih podataka

Ovaj sektor posjeduje veliki broj nadležnosti te ćemo ih podijeliti na tri oblasti, prva oblast će se odnostiti na samu državu Bosnu i Hercegovini i nadležnosti na nivou unutar državne strukture:

Sektor za zaštitu tajnih podataka vrši poslove nadzora nad sigurnosnim provjerama; izdaje dozvole za pristup tajnim podacima BiH, drugih država, međunarodnih ili regionalnih organizacija u skladu sa Zakonom ili međunarodnim odnosno regionalnim ugovorom; prati stanje u oblasti određivanja i zaštite tajnih podataka i brine za usavršavanje i provođenje fizičkih, organizacionih i tehničkih standarda zaštite tajnih podataka u državnim, entitetskim i organima na drugim nivoima državne organizacije BiH, kod nosilaca javnih dužnosti, te u privrednim organizacijama koje dolaze do tajnih podataka i njima raspolažu. (Ministarstvo sigurnosti Bosne i Hercegovine (2011). izvor: www.msb.gov.ba)

Druga oblast ovog odsjeka će se odnosti na međunarodni nivo, te po tom pitanju ovaj sektor ima sljedeće nadležnosti:

Brine o izvršavanju prihvaćenih međunarodnih obaveza i međunarodnih ugovora o zaštiti tajnih podataka te s tim u vezi sarađuje sa nadležnim organima drugih država, međunarodnih ili regionalnih organizacija, brine o zaštiti tajnih podataka u državnim institucijama i organima u inostranstvu; izdaje sigurnosne potvrde za sisteme i sredstva za prijenos čuvanje i obradu tajnih podataka BiH, drugih država, međunarodnih ili regionalnih organizacija; potvrđuje ispunjavanje propisanih uslova za obradu tajnih podataka od strane pojedinih organa; izdaje uputstva za postupanje sa tajnim podacima BiH, druge države odnosno međunarodne ili regionalne organizacije, vrši nadzor nad sprovođenjem fizičkih, organizacionih

i tehničkih odluka za zaštitu tajnih podataka druge države, međunarodne ili regionalne organizacije i u skladu sa saznanjima na osnovu nadzora izdaje obavezne instrukcije za otklanjanje ustanovljenih propusta koje su organi dužni neodgodivo otkloniti. (ibid.)

Sljedeća oblast se odnosi na savjetodavnu ulogu ovoga odsjeka, te sama uspostava i kontrola registara iz ove oblasti:

Razmjenjuje podatke s državnim sigurnosnim organima drugih država, međunarodnim organizacijama; priprema prijedloge propisa potrebnih za provođenje zakona; daje mišljenje o usaglašenosti općih akata o određivanju, zaštiti i pristupu tajnim podacima sa zakonom; koordinira djelovanje organa nadležnih za sigurnosnu provjeru; predlaže postupke za djelotvorniju zaštitu tajnih podataka; vrši nadzor nad kriptozaštitom tajnih podataka i izdaje certifikate za korišćenje sistema kriptozaštite u organima BiH; uspostavlja i vodi nacionalni centralni registar u kojem se vodi službena evidencija o izdatim dozvolama za sve osobe koje imaju pravo pristupa tajnim podacima povjerljivo, tajno i vrlo tajno. (ibid.)

I posljednja oblast, koja je povezana sa drugom oblasti po redu a koja se odnosi na međunarodna pitanja, ova oblast se odnosi na saradnju sa međunarodnim sigurnosnim organizacijama, te se navodi sljedeće:

Na osnovu sporazuma o saradnji BiH sa Sjeveroatlanskom ugovornom organizacijom (NATO) uspostavlja i vodi NATO centralni registar u Ministarstvu sigurnosti i pod-registar u vojnoj misiji BiH pri NATO u Briselu u kojima se čuvaju i procesuiraju klasifikovani podaci NATO-a; na osnovu sporazuma između Bosne i Hercegovine i Evropske unije o sigurnosnim procedurama za razmjenu klasifikovanih informacija uspostavlja i vodi pod-registar EU; uspostavlja i vodi pod-registar Minstarstva sigurnosti za čuvanje i procesuiranje tajnih podataka Ministarstva; obavlja poslove prijema i dostavljanja tajnih podataka na teritoriji BiH i drugih država; utvrđuje Pravilnik o edukaciji o pitanju sigurnosti tajnih podataka i obavlja druge zadatke koji su određeni Zakonom i propisima donesenim na osnovu njega. (ibid.)

Odsjeci unutar Sektora za zaštitu tajnih podataka su sljedeći:

- Odsjek za propise, dozvole i industrijsku sigurnost,
- Odsjek za informatičku sigurnost, i
- Odsjek za tehničke standarde i nadzor.

Svaki odsjek unutar sektora posjeduje svoje nadležnosti koje će biti navedene u sljedećem dijelu rada. Odsjek za propise, dozvole i industrijsku sigurnost posjeduje sljedeće nadležnosti: ”Odsjek sarađuje sa drugim odsjecima u Sektoru, prati stanje u oblasti određivanja i zaštite tajnih podataka i brine za usavršavanje i provođenje fizičkih, organizacionih i tehničkih standarda zaštite tajnih podataka u državnim, entiteskim organima i organima na drugim nivoima državne organizacije BiH, kod nosilaca javnih dužnosti, te u privrednim organizcijama koje dolaze do tajnih podataka i njima raspolažu, učestvuje u izradi mjesečnih planova rada Odsjeka.” (ibid.)

Odsjek za informatičku sigurnost nadležan je za: ” Odsjek sarađuje sa drugim odsjecima u Sektoru, prati stanje u oblasti određivanja i zaštite tajnih podataka i brine za usavršavanje i provođenje fizičkih, organizacionih i tehničkih standarda zaštite tajnih podataka u dijelu informatičke sigurnosti u državnim, entitetskim i organima na drugim nivoima državne organizcije BiH, učestvuje u izradi nacrta planova rada” (ibid.). Razlike između nadležnost prva dva odsjeka se odnose na to da Odsjek za propise, dozvole i industrijsku sigurnost se odnosi na unutardržavne organe, nosioce javnih dužnosti i prevredne organizacije, dok Odsjek za informatičku sigurnost se odnosi na informatičku sigurnost na nivou državnih, entitetskih i drugih organa na nivou države.

Odsjek za tehničke standarde i nadzor posjeduje sljedeće nadležnosti: ”prati stanje u oblasti tehničke žaštite, ugradnje i izbora sigurnosnih sistema neophodnih za zaštitu osoblja; informacija i materijalno tehničkih dobara i brine za usavršavanje fizičkih i tehničkih mjera zaštite u državnim; entitetskim i organima na drugim nivoima u BiH, te u privrednim organizacijama koje imaju pristupa tajnim podacima i povjerljivim informacijama i njima raspolažu; planira i rukovodi mjerama fizičke i tehničke zaštite; sudjeluje u izradi pravila i standardnih operativnih procedura; izrađuje i usavršava sigurnosne standarde za sigurnosne sisteme koji se primjenjuju u zaštiti tajnih podataka; rukovodi i planira sigurnosne mjere koje se poduzimaju u kriznim sigurnosnim situacijama; vrši nadzor i kontrolu ugradjenih sigurnosnih sistema i mjera sigurnosne zaštite, te nadzor nad sigurnosnim provjerama.” (ibid.)

Sva tri odsjeka sarađuju sa ostalim odsjecima unutar sektora i svoje aktivnosti vrše na osnovu zakona i podzakonski akata i pravilnika, neki od njih su sljedeći: Pravilnik o programu edukacije iz oblasti zaštite tajnih podataka, Zakon o zaštiti tajnih podataka, Pravilnik o unutrašnjem nadzoru nad provođenjem Zakona o zaštiti tajnih podataka i propisa donijetih na osnovu zakona, Pravilnik o listi funkcionera koji imaju pristup tajnim podacima stepena "interno"i "povjerljivo" bez sigurnosne provjere i dozvole,

Sporazum izmedu Bosne i Hercegovine i Evropske unije o sigurnosnim procedurama za razmjenu povjerljivih informacija, Sporazum između Bosne i Hercegovine i Sjeveroatlantske ugovorne organizacije (NATO) o sigurnosti informacija, Pravilnik o uspostavi kontrolnih sigurnosnih mjera i sistema zaštite sigurnosnih područja, te i petnaest Sporazuma o zaštiti tajnih podataka.

4.5 *Obavještajno-sigurnosna agencija Bosne i Hercegovine- OSA BiH*

Obavještajno-sigurnosna agencija BiH osnovana je 2004. Godine Zakonom o Obavještajno-sigurnosnoj agenciji Bosne i Hercegovine. Agencija je nadležna za cijeli teritoriji Bosne i Hercegovine i njeno sjedište je u Sarajevu. Rad OSA-e se temelji na sljedećim zakonima:

- Zakon o Obavještajno-sigurnosnoj agenciji Bosne i Hercegovine,
- Zakon o zaštiti tajnih podataka BiH**,**
- Zakon o strancima**,** i
- Zakon o kretanju i boravku stranaca i azilu**.**

Zakon o Obavještajno-sigurnosnoj agenciji počinje sa Općim odredbama, zatim drugo poglavlje se odnosi na dužnosti i zadatke, te se tu navodi sljedeće:

U članu 5. i 6. Zakona o Obavještajno-sigurnosnoj agenciji regulisani su zadaci ove agencije, a oni glase:

Član 5.

“Agencija je odgovorna za prikupljanje obavještajnih podataka u vezi sa prijetnjama po sigurnost Bosne i Hercegovine, kako unutar, tako i van Bosne i Hercegovine, njihovo analiziranje i prenošenje ovlaštenim dužnosnicima i tijelima navedenim u članu 6. stav 5. ovog zakona, kao i za prikupljanje, analiziranje i prenošenje obavještajnih podataka s ciljem pružanja pomoći ovlaštenim službenim osobama kako je definirano zakonima o krivičnom postupku u Bosni i Hercegovini, te ostalim nadležnim tijelima u Bosni i Hercegovini kada je to potrebno radi suzbijanja prijetnji po sigurnost Bosne i Hercegovine. U smislu ovog zakona, pod "prijetnjama po sigurnost Bosne i Hercegovine" smatrat će se prijetnje

suverenitetu, teritorijalnom integritetu, ustavnom poretku, osnovama ekonomske stabilnosti Bosne i Hercegovine, kao i prijetnje po globalnu sigurnost koje su štetne po Bosnu i Hercegovinu, uključujući:

a. terorizam, uključujući međunarodni terorizam;
b. špijunaža usmjerena protiv Bosne i Hercegovine ili štetna po sigurnost Bosne i Hercegovine na bilo koji drugi način;
c. sabotaža usmjerena protiv vitalne nacionalne infrastrukture Bosne i Hercegovine ili na drugi način usmjerena protiv Bosne i Hercegovine;
d. organizirani kriminal usmjeren protiv Bosne i Hercegovine ili štetan po sigurnost Bosne i Hercegovine na bilo koji drugi način;
e. trgovina drogama, oružjem i ljudima usmjerena protiv Bosne i Hercegovine ili štetna po sigurnost Bosne i Hercegovine na bilo koji drugi način;
f. nezakonita međunarodna proizvodnja oružja za masovno uništenje, ili njihovih komponenti, kao i materijala i uređaja koji su potrebni za njihovu proizvodnju;
g. nezakonita trgovina proizvodima i tehnologijama koje su pod međunarodnom kontrolom;
h. radnje kažnjive po međunarodnom humanitarnom pravu;
i. djela organiziranog nasilja ili zastrašivanja nacionalnih ili vjerskih grupa u Bosni i Hercegovini.

Pri izvršavanju aktivnosti navedenih u stavovima 1. i 2. ovog člana, Agencija ima pravo da koristi operativna sredstva i metode navedene u Poglavlju VIII. i Poglavlju IX. ovog zakona.

Član 6.

Agencija vrši razmjenu obavještajnih podataka i ostvaruje druge oblike saradnje s obavještajnim i sigurnosnim službama u drugim državama i drugim stranim i međunarodnim institucijama u cilju obavljanja zadataka navedenih u stavovima 1. i 2. člana 5. ovog zakona, u skladu s članom 70. i 71. ovog zakona.

Agencija koristi svoja operativna sredstva i metode u cilju pružanja zaštite institucijama i objektima Bosne i Hercegovine kao i institucijama i objektima Federacije, Republike Srpske i Distrikta Brčko Bosne i Hercegovine (u daljem tekstu: Distrikt), te diplomatskim misijama Bosne i Hercegovine u inostranstvu, kao i prilikom državnih posjeta i drugih događaja, kako to odrede predsjedavajući Vijeća

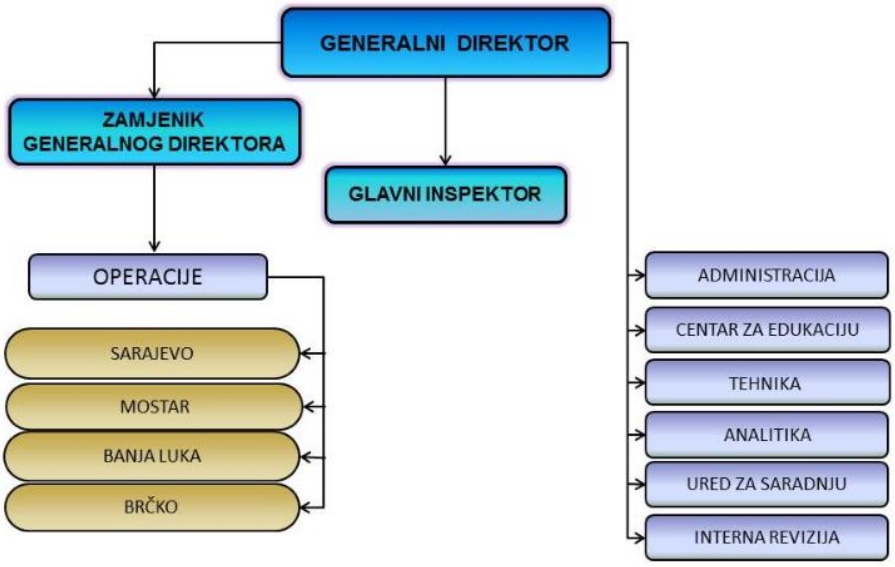
ministara (u daljem tekstu: predsjedavajući) ili generalni direktor. Agencija nije odgovorna da osigura fizičku zaštitu za gore navedene institucije i događaje.
Agencija sarađuje sa Međunarodnim krivičnim tribunalom za zločine počinjene na teritoriji bivše Jugoslavije (u daljem tekstu: Međunarodni tribunal), inter alia, tako što Tribunalu dostavlja podatke u vezi sa licima koja su odgovorna za ozbiljna kršenja međunarodnog humanitarnog prava na teritoriji bivše Jugoslavije od 1991. godine.
Agencija provodi sigurnosnu provjeru lica koja se prijave za posao u Agenciji, u cilju određivanja stepena njihove odgovornosti i povjerljivosti, kao i onih osoba koje traže državljanstvo Bosne i Hercegovine.
Kada je to potrebno radi ispunjavanja svojih dužnosti u skladu sa ovim zakonom, Agencija blagovremeno obavještava slijedeće zvaničnike i tijela o obavještajnim pitanjima kako na vlastitu inicijativu tako i na njihov zahtjev: Predsjedništvo Bosne i Hercegovine (kolektivno) (u daljem tekstu: Predsjedništvo), predsjedavajućeg Vijeća ministara, ministra vanjskih poslova, ministra sigurnosti, ministra odbrane, predsjednike, potpredsjednike i premijere Federacije i Republike Srpske, ministre unutarnjih poslova Federacije i Republike Srpske, predsjedavajućeg i zamjenike predsjedavajućeg Predstavničkog doma Parlamentarne skupštine Bosne i Hercegovine, predsjedavajućeg i zamjenike predsjedavajućeg Doma naroda Pralamentarne skupštine Bosne i Hercegovine, predsjedavajućeg i zamjenike predsjedavajućeg Narodne skupštine Republike Srpske, predsjedavajućeg i zamjenike predsjedavajućeg Predstavničkog doma Federacije, predsjedavajućeg i zamjenike predsjedavajućeg Doma naroda Federacije, kao i Sigurnosno-obavještajnu komisiju Parlamentarne skupštine Bosne i Hercegovine (u daljem tekstu: Sigurnosno-obavještajna komisija).

Informacije se dostavljaju u skladu s principom "potrebno da zna", osim ukoliko nije drugačije propisano ovim zakonom.

Agencija izrađuje i stavlja na raspolaganje javnosti godišnji izvještaj o svojim ciljevima, programima i generalnom težištu svojih aktivnosti, koji je zasnovan na informacijama koje nisu povjerljive.“

U trećem poglavlju Zakona regulisana su pitanja Vanjskog rukovođenja i nadzora nad OSA-om, te se tu navode prava i odgovornosti, te nadležnosti: Predsjedništva BiH, Vijeća ministara BiH i Predsjedavajućeg vijeća ministara BiH. Agencija posjeduje i Parlamentarni nadzor kroz Sigurnosno-obavještajnu komisiju za nadzor nad Agencijom.

U sljedećem dijelu rada će biti prikazane ilustracije koje se odnose na unutrašnju organizaciju OSA-e i poziciju OSA-e u Bosni i Hercegovine. Što se tiče unutrašnje organizacije OSA-e, ona je organizovana na sljedeći način:



Slika br. 4- Unutrašnja organizacija OSA-e

Izvor: www.osa-oba.gov.ba

Slika br. 5- Unutrašnja organizacija OSA-e

Izvor: www.osa-oba.gov.ba

Četvrtim poglavljem Zakona regulisane su prava i odgovornosti generalnog direktora i zamjenika generalnog direktora i prava i odgovornosti glavnog inspektora. Poglavljima 6. i 7. regulisani su operativni principi i međunarodna saradnja agencije. Članovima zakona 70. i 71. regulisana je međunarodnja saradnja OSA-e na sljedeći način:

Član 70.

U cilju ispunjavanja svojih dužnosti u skladu sa ovim zakonom, Agencija može, uz odobrenje predsjedavajućeg, zaključivati sporazume sa sigurnosnim i obavještajnim agencijama stranih zemalja. U cilju ispunjavanja svojih dužnosti u skladu sa ovim zakonom, Agencija također može, uz odobrenje predsjedavajućeg, nakon njegove konsultacije sa ministrom vanjskih poslova Bosne i Hercegovine, zaključivati sporazume sa institucijom strane države, ili nekom međunarodnom organizacijom države ili nekom njenom institucijom.

Predsjedavajući informira Sigurnosno-obavještajnu komisiju o postojanju takvih sporazuma. Na osnovu međunarodnih sporazuma, Agencija može sarađivati sa stranim sigurnosnim i drugim odgovarajućim službama u svrhu razmjene podataka, zajedničkog obavljanja aktivnosti koje spadaju u nadležnost rada Agencije i u cilju uspostavljanja tehničke i obrazovne saradnje.

Član 71.

Agencija može stranim obavještajnim i drugim odgovarajućim službama dostaviti podatke o građanima Bosne i Hercegovine samo na osnovu informacija da građanin predstavlja opasnost po sigurnost Bosne i Hercegovine, države primatelja traženih podataka, ili opasnost širih razmjera po regionalnu ili globalnu sigurnost.
Agencija ne može dostaviti podatke vezane za građane u skladu sa prethodnim stavom osim ukoliko nema osnovane garancije da će primalac podataka osigurati jednak nivo zaštite koju su ti podaci imali u Bosni i Hercegovini.

Osmo poglavlje reguliše način i ovlaštenja za prikupljanje podataka, član 72. Navodi sljedeće: “Agencija je ovlaštena da prikuplja, analizira, čuva i distribuira obavještajne podatke nadležnim tijelima unutar Bosne i Hercegovine na način koji je u skladu sa Ustavom Bosne i Hercegovine, ovim zakonom i drugim

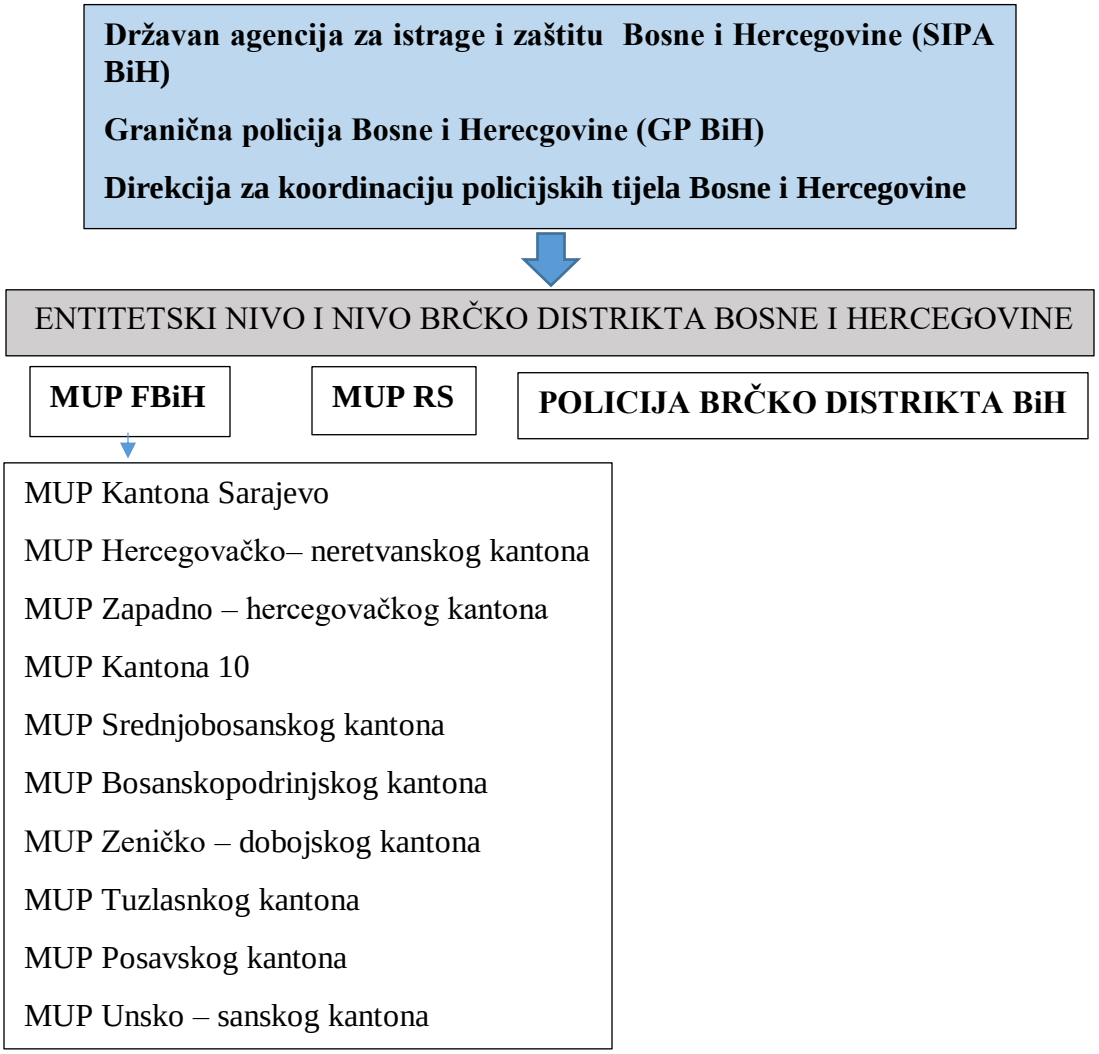
relevantnim državnim zakonima", te i član 73. istog Zakona navodi "Agencija može prikupljati samo one informacije za koje se opravdano može pretpostaviti da su potrebne za obavljanje njenih dužnosti nabrojanih u članovima 5. i 6. ovog zakona". Također u ovom poglavlju se definisani i načini na koji se mogu prikuplati podaci, ovlaštenja Agencije zaprikupljanje informacija, saradnja sa Agencijom po pitanju prikupljanja informacija, mjere tajnog prikupljanja podataka, naloge za prikupljanje informacija, te način obustave prikupljanja.

Devet poglavlje nosi naziv Upravljanje podacima, član 81. reguliše primjenu Zakona o zaštiti ličnih podataka od strane agencije, "Zakon o zaštiti ličnih podataka Bosne i Hercegovine se ne primjenjuje na lične podatke koje prikuplja i obrađuje Agencija". Također ovo poglavlje obrađuje i zabrane, zaštite obavještajnih podataka i identiteta, zatim čuvanje informacija. Nadležnosti za uspostavljanje efikasnog Sistema klasifikacije podataka je na Generalnom direktoru, te reguliše upotrebu tajnih i strogo povjerljivih dokumenata. Također reguliše i rad arhiva, prosljeđivanje informacija o ozbiljnim prijetnjama po sigurnost BiH i obavještavanje građanja o mogućem postupku prikupljanja podataka o njemu samom.

Deseto poglavlje Zakona se odnosi na finansiranje agencije, dok jedanaesto sačinjava prijelazne i završne odbredbe Zakona o sigurnosno-obavještajnoj agenciji Bosne i Hercegovine.

5. POLICIJSKE AGENCIJE I UPRAVLJANJA INFORMACIJAMA I ZAŠTITA PODATAKA U BOSNI I HERCEGOVINI

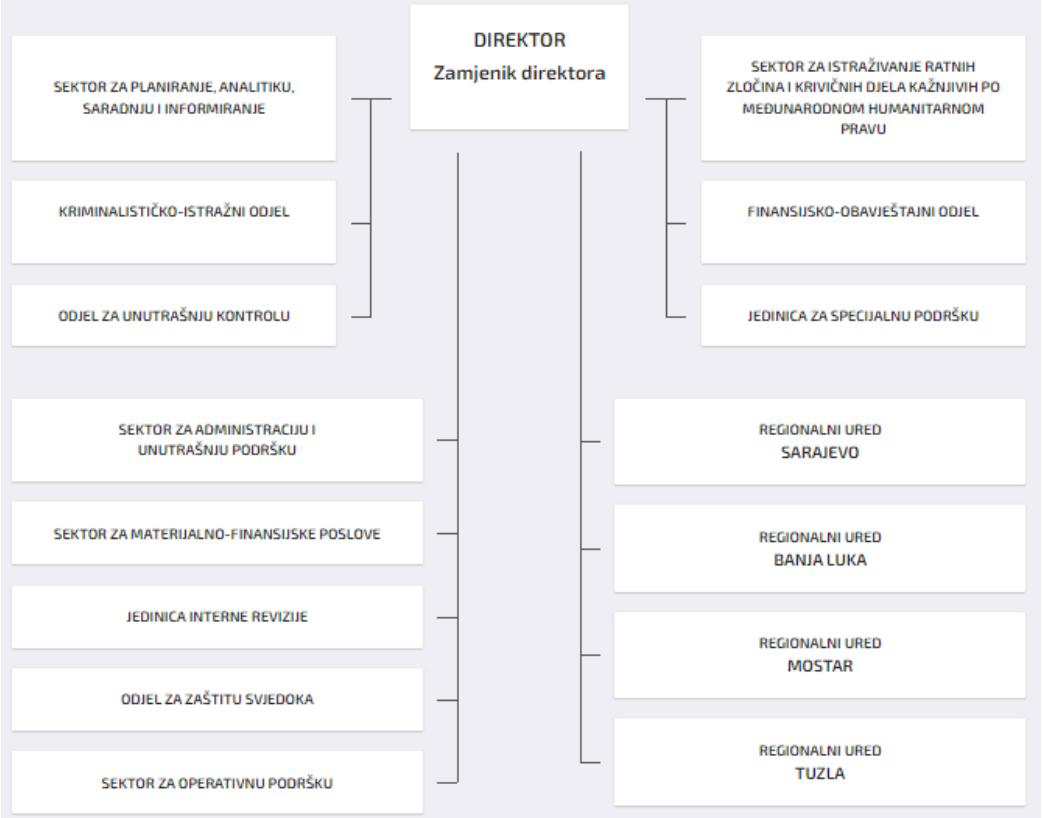
U Bosni i Hercegovini na svim nivoima djeluje šesnaest policijskih agencija, u nastavku će biti predstavljene te agencije. Za svaku od njih ćemo iznijeti sektore i odjele tih agencija koje se odnose na tematiku ovoga rada.



5.1.1 Državni nivo

Na državnom nivou djeluju tri policijske agencije, a to su Državna agencije za istrage i zaštitu- SIPA[5], Granična policija Bosne i Hercegovine i Direkcija za koordinaciju policijskih tijela.

Struktura državne agencije za istrage i zaštitu je sljedeća:



Slika 6.- Organizaciona struktura SIPA-e

izvor: www.sipa.gov.ba/bs

[5] SIPA, skr.- eng. State investigation and protection agency

Za naš rad važni su sljedeći sektori: Direktor i Zamjenik direktora, Sektor za planiranje, analitiku, saradnju i informisanje, Finansijsko-obavještajni odjel, Sektor za administraciju i unutrašnju podršku, Sektor za operativnu podršku i Odjel za unutrašnju kontrolu. Za svaki od ovih sektora ćemo navest nama relevantne podatke vezane za ovaj rad.

Direktor SIPA-e prema Zakonu o Državnoj agenciji za istrage i zaštitu (2004), u članu 8. se navode dužnosti i odgovornosti direktora:

- predstavlja SIPA-u;
- izrañuje godišnji plan rada prema smjernicama predsjedavajućeg Vijeća ministara te godišnji budžet SIPA-e i predlaže ih ministru, koji ih prosljeñuje Vijeću ministara;
- rukovodi i usmjerava obavljanje poslova iz nadležnosti SIPA-e;
- osigurava pravilno izvršavanje smjernica i naloga tužioca o radnjama policijskih službenika u vezi s krivičnim postupkom;
- osigurava saradnju s organima za provoñenje zakona te ostalim odgovarajućim tijelima u BiH;
- osigurava saradnju s organima za provoñenje zakona i ostalim nadležnim službama stranih država, kao i provoñenje ostalih meñunarodnih sporazuma o policijskoj saradnji i drugih meñunarodnih instrumenata iz nadležnosti SIPA-e.

Zamjenik direktora ispunjava određene dužnosti za vrijeme odsustva Direktora, te određene dužnosti za koje ga ovlasti sam Direktor agencije.

Sektor za planiranje i analitiku, koji je nama od važnosti za svoj djelokrug rada navodi sljedeće "Sektor za planiranje, analitiku, saradnju i informiranje izrađuje i prati implementaciju strateških i operativnih planova Agencije, koordinira rad sa analitičarima u organizacionim jedinicama Agencije, prikuplja, analizira i izrađuje analitičke informacije, programe i izvještaje o radu Agencije, obavlja poslove koji se odnose na provođenje propisa o zaštiti ličnih podataka u Agenciji, stara se o dokumentima i materijalima koji se dostavljaju direktoru, vrši pripreme za održavanje savjetovanja i drugih sastanaka koje organizira Agencija, nadležan je za izradu analiza za interne i eksterne potrebe, praćenje realizacije zaključaka sa Stručnog kolegija, za obavljanje određenih poslova iz domena međunarodne i međuagencijske saradnje,

prevođenje i lektoriranje pisanih materijala, te radi i druge poslove u skladu sa zakonom.“(SIPA (n.d). izvor: www.sipa.gov.ba)

Uređenje sektora za planiranje i analitiku je sljedeće:

- Odsjek za strategiju, planiranje, analitičke poslove i zaštitu ličnih podataka
- Odsjek za međunarodnu i međuagencijsku saradnju
- Grupa za odnose s javnošću

Finansijsko-obavještajni odjel počeo je sa radom 2004. godine i predstavlja jedinu unutaragencijsku organizaciju ovakvog tipa u Bosni i Hercegovin, opis posla kojim se bave je sljedeći: ”Poslovi i nadležnosti Finansijsko-obavještajnog odjela propisani su, pored Zakona o SIPA-i, Zakonom o sprečavanju pranja novca i finansiranja terorističkih aktivnosti, na osnovu kojeg prima, sakuplja, evidentira i analizira podatke, informacije i dokumentaciju, te istražuje i prosljeđuje rezultate analiza i/ili istraga, podatke i dokumentaciju tužilaštvima i drugim nadležnim organima kako u BiH tako i u inostranstvu.” (ibid.)

Uređenje ovog odjela je sljedeće:

- Analitički odsjek
- Odsjek za istrage
- Odsjek za pravna pitanja, međunarodnu saradnju i podršku

Sektor za administraciju i unutrašnju podršku, ovaj sektor je nama od važnosti zato što se odnosi na ljudske resurse, raspoređivanje, obućavanje i prijem novih službenika. Sam djelokruh i nadležnosti ovog sektora su sljedeće: “Sektor izrađuje programe, informacije, izvještaje, ostvaruje internu i eksternu saradnje u vezi sa poslovima iz nadležnosti Sektora, prati i proučava dejstvo zakona na rad Agencije, daje stručna objašnjenja, s ciljem jedinstvenog provođenja i primjene propisa, prati i analizira usklađenost propisa koje primjenjuje Agencija, te inicira njihovo donošenje, izmjene i dopune, prati i analizira stanje kadrova u vezi sa prijemom i prestankom rada zaposlenih, obavlja stručne poslove za potrebe Agencije u dijelu uređenja radno-pravnog statusa zaposlenih, te uspostavlja i vodi propisane evidencije, obavlja poslove upravnog rješavanja, te priprema akte kojima se reguliraju statusna pitanja

zaposlenih, učestvuje u planiranju, organizaciji i koordinaciji obuka zaposlenih u Agenciji, obavlja i druge poslove u skladu sa zakonom."(ibid.)

Organizacija ovog sektora je sljedeća:

- Odsjek za normativno-pravne poslove
- Odsjek za kadrovske poslove, razvoj ljudskih resursa i obuke
- Pisarnica i arhiva

Sektor za operativnu podršku djeluje kao podrška ostalim sektorima i posjeduje sljedeće nadležnosti: , "Sektor za operativnu podršku provodi po naredbi suda mjere i radnje koje se odnose na posebne istražne radnje i to: nadzor i tehničko snimanje telekomunikacija, pristup kompjuterskim sistemima i kompjutersko sravnjavanje podataka, nadzor i tehničko snimanje prostorija, tajno praćenje i tehničko snimanje osoba i predmeta, nadzirani prevoz i isporuka predmeta krivičnog djela." (ibid.)

Ovaj sektor čine sljedeće organizacije:

- Operativno-komunikacioni odsjek
- Odsjek za operativno-tehnički nadzor i informatičku podršku
- Odsjek za informatiku, komunikacije i sigurnost informatičkih sistema
- Odsjek za zakonito presretanje komunikacija
- Odsjek za protivdiverzionu, protiveksplozivnu i tehničku zaštitu
- Grupa za kriminalističku tehniku i poligrafsko vještačenje
- Helikopterska grupa

Odjel za unutrašnju kontrolu nadležnosti ovog odjela a koje su interesantne za naš rad su sljedeće: "Odjel vrši osnovne sigurnosne provjere, obavlja poslove i preduzima mjere fizičke, tehničke i druge zaštite dokumenata u vezi sa zakonitim raspolaganjem, čuvanjem, otpremom i uništavanjem zaštićenih dokumenata, brine se za usavršavanje i provođenje fizičkih, organizacionih i tehničkih standarda zaštite tajnih podataka u SIPA-i, te radi i druge poslove u skladu sa zakonom."(ibid.)

Odjel za unutrašnju kontrolu je organizovan na sljedeće jedinice:

- Odsjek za unutrašnje istrage
- Odsjek za sigurnosne provjere

- Grupa za unutrašnju inspekciju i profesionalne standarde
- Grupa za podregistar tajnih podataka

Granična policija Bosne i Hercegovine osnovana je 2004. godine Zakonom o graničnoj policiji Bosne i Hercegovine, po svojoj prirodi posla, u velikoj mjeri se oslanja se na razmjenu i upravljanja informacijama kako na unutardržanom nivou, tako i na regionalnom i međunarodnom nivou. Granična policija BiH u svom biltenu (2021:15) navodi unaprijeđenje na tehnološkom nivou i nivou opremljenosti, "U proteklom razdoblju se nastavilo sa aktivnostima sistematske softversko/ hardverske nadogradnje jedinstvenog informacionog sistema (JIS) GPBiH, na poboljšanju kvaliteta procesa granične kontrole te radu na optimizaciji i maksimalnom ubrzavanju poslovnih procesa u GPBiH". Po samoj prirodi posla potreba i težnja ka najpouzdanijim praksama se prepoznaje i u radu Granične policije BiH što se navodi i u sljedećem dijelu "Kontinuirano se radi na informacionom uvezivanju graničnih prijelaza kao i implementiranju svih bitnih servisa sve do nivoa graničnog prijelaza. Ovo se odnosi na dokument menadžment sistem (DMS), jedinstveni e-mail sistem, intranetski portal, kao i novouspostavljene". (ibid., 2021:15)

Od važnosti za naš rad je Centralni istražni ured Granične policije Bosne i Hercegovine. Centralni istražni ured se sastoji od sljedećih odsjeka:

- Odsjek za operativnu i administrativnu podršku,
- Odsjek za istrage,
- Odsjek za kriminalističko-obavještajne, analitičke i poslove analize rizika,
- Odsjek sa prikrivena operacije,
- Odsjek za nadzor i osmatranje 1 Sarajevo, i
- Odsjek za nadzor i osmatranje 2 Bosansko Grahovo.

U biltenu (2021:24) Granične policije BiH za rad Centralnog istražnog ureda se navodi sljedeće: "Centralni istražni ured Granične policije BiH, intenzivno radi na sprječavanju, otkrivanju i istraživanju kaznenih djela usmjerenih protiv sigurnosti državne granice ili protiv obavljanja poslova i zadataka iz nadležnosti GPBiH."

U vezi sa obradom i prikupljanjem podataka za ovaj odjel se navodi sljedeće: "Ova organizacijska postrojba prikuplja i obrađuje obavještajne podatke u vezi s navedenim kaznenim djelima, prati i analizira

stanje organiziranog kriminala i pravi strateške analize i procjenu rizika u vezi s istim te prikuplja informacije, obavijesti i druge podatke u vezi s organiziranim kriminalom, izravno provodi složene policijske istrage i provodi posebne istražne radnje u skladu sa zakonom i drugo".(ibid.,2021:24)

Direkcija za koordinaciju policijskih tijela Bosne i Hercegovine osnovana je 2008. godine Zakonom o Direkciji za koordinaciju policijskih tijela i o agencijama za podršku policijskoj strukturi Bosne i Hercegovine. Direkcija je organizovana kroz sljedeće odjele:

- Kabinet direktora,
- Ured za profesionalne standarde,
- Sektor za koordinaciju i saradnju,
- Sektor za međunarodnu operativnu policijsku saradnju,
- Sektor za osiguranje VIP osoba i objekata,
- Sektor za stratešku analizu, procjene i planiranje i IT podršku, i
- Sektor za ljudske resurse, pravne, materijalno - finansijske poslove i pisarnicu.

Rad *Sektora za profesionalne standarde* pored Odsjeka za unutrašnju kontrolu, posjeduje odsjek i za zaštitu tajnih podataka. Sektor za koordinaciju i saradnju pored poslova saradnje, komunikacije i koordinacije sa drugim agencijama i organizacijama unutar BiH i nadzora nad sprovođenjem međunarodnih ugovora o policijskoj saradnji same Direkcije, također vrši i poslove koji se odnose poslove prikupljanja informacija, "Svakodnevno prikuplja i objedinjava sigurnosne informacije koje su relevantne za BiH, uz praćenje sigurnosnog stanja u BiH, te obavještava nadležna policijska i druga tijela u Bosni i Hercegovini".(Direkcija za koordinaciju policijskih tijela BiH, izvor: www.dkpt.ba)

Sektor za međunarodnu operativnu policijsku saradnju "predstavlja jedinstvenu tačku za razmjenu infomacija na strateškom i operativnom nivou u sklopu provođenja međunarodnih istraga. Ostvaruje međunarodnu policijsku saradnju, pri čemu osigurava, provodi i unapređuje saradnju domaćih policijskih, sudskih i drugih tijela sa srodnim tijelima zemalja svijeta, primjenjujući najbolje prakse. Saradnja se ostvaruje sa Interpolom, Europolom i SECI[6] centrom, kao i drugim tijelima skladno

[6] The Southeast Europe Cooperative Initiative Regional Center for Combating Trans-border Crime- skr. SECI

potpisanim ugovorima“(DKPT BiH, izvor: www.dkpt.ba). Iz navedenog vidimo da je ovaj sektro zadužen za informisanje i razmjenu informacija na međunarodnom nivou.

Sektor za strateško analizu, procjene i planiranje i IT podršku je također od veoma velike važnosti za naš rad, poslovi ovog sektora se odnose na “ Analizira podatake prikupljene od policijskih agencija i drugih organa, te sačinjava analitičke izvještaje i preporuke koji se odnose na sigurnosnu situaciju u BiH. Kroz koordinaciju aktivnosti učestvuje u razvoju i primjeni strateških i akcionih planova, te prati njihovu implementaciju.“(DKPT BiH, izvor: www.dkpt.ba)

5.1.2 Entitetski nivo i nivo Brčko distrikta Bosne i Hercegovine

Ovaj dio će obuhvatiti odjele i sektore policijskih agencija na nivou entiteta i Brčko distrikta Bosne i Hercegovine. Na nivoima entiteta postoje Ministarstvo unutrašnjih poslova Federacije BiH i Ministarstvo unutrašnjih poslova RS, dok policijske poslove u Brčko distriktu obavlja Policija Brčko distrikta Bosne i Hercegovine.

Sektori i odsjeci koji su od važnosti za naš rad, a dio su strukture ***Ministarstva unutrašnjih poslova FBiH*** su:

- Odsjek za međunarodnu saradnju (unutar kabineta ministra),
- Odsjek za studijsko-analitičke poslove i poslove izrade programa i projekata za potrebe policije iz oblasti evropskih integracija, i
- Odsjek za informativne poslove.

Poslovi Odsjeka za međunarodnju saradnju se ogledaju kao i što sam naziv kaže u organiziranju saradnje na međuanrodnom nivou između Federalnog ministarstva i međunarodnih organizacija na način kako je to zakonom propisano. Ovaj odsjek također sudjeluje u saradnji sa državnim ministarstvima, Ministarstvom sigurnosti BiH i drugim ministarstvima i institucijama.

Djelokrug Odsjeka za studijsko-analitičke poslove i poslove izrade programa i projekata za potrebe policije iz oblasti evropskih integracija je sljedeći:

- prati studijsko-analitičke i druge poslove za potrebe Ministarstva, o čemu sačinjava potrebne izvještaje;
- analizira, priprema i provodi programe i druge akte koji se odnose na jačanje profesionalizma u Ministarstvu i Upravi policije vezano za smanjenje i suzbijanje korupcije i borbu protiv organiziranog kriminala u saradnji s Upravom policije, a naručito o pitanjima organizacionog, kadrovskog i materijalno-tehničkog jačanja policije na osnovu službenih podataka i podataka prikupljenih od drugih organa uprave, o čemu sačinjava odgovarajuće projekte i prati njihovu realizaciju;
- organizira, priprema, prati i dostavlja obavještenja o provođenju federalne politike i federalnih zakona iz nadležnosti Ministarstva premijeru Vlade Federacije, predsjedniku i potpredsjednicima Federacije i Parlamentu Federacije obavezno dva puta godišnje, a po potrebi i češće;
- priprema i sačinjava izvještaje o sigurnosnoj situaciji na teritoriji Federacije na osnovu službenih podataka i podataka koje dostavi Uprava policije i kantonalna ministarstva unutrašnjih poslova koje dostavlja Parlamentu Federacije i radnim tijelima Parlamenta Federacije;
- organizira dostavljanje izvještaja o radu Nezavisnog odbora Vladi Federacije;
- priprema informacije i druge analitičko-dokumentacione materijale za predsjednika i potpredsjednike Federacije, Parlament Federacije, Vladu Federacije i nadležne komisije Parlamenta Federacije i Vlade Federacije, kao i za nadležne sigurnosne organe na nivou Bosne i Hercegovine;
- analizira provođenje mjera i radnji koje se odnose na područje nasilja u porodici i provođenje mjera upozorenja i drugih mjera i radnji koje se izriču prema maloljetnim učiniocima krivičnih dijela u saradnji sa drugim organizacionim jedinicama Ministarstva; i
- analizira provođenje mjera i radnji koje su utvrđene drugim propisima u kojima je utvrđena nadležnost Ministarstva u saradnji sa drugim organizacionim jedinicama Ministarstva (zaštita tajnih podataka, kaznene evidencije, evidencije koje se vode po osnovu Zakona o zaštiti ličnih podataka, Zakona o policiji). (MUP FBiH, izvor: www.fmup.gov.ba)

Djelokrug Odsjeka za informativne je sljedeći:

- Obavlja poslove prikupljanja i sređivanja podataka i informacija iz nadležnosti Ministarstva u saradnji sa drugim organizacionim jedinicama Ministarstva;
- organizira i obavlja vezano za uspostavu jedinstvenog funkcionalnog informacijskog sistema te vodi zajedničke baze podataka iz oblasti unutrašnjih poslova zasnovane na elektronskoj obradi podataka u skladu sa propisom koji donosi ministar na osnovu člana 66. stav (5) Zakona;
- obavlja poslove na formiranju informaciono–telekomunikacionog sistema i mreže za potrebe Ministarstva;
- učestvuje u pripremi ekspozea, referata i drugih analitičko-dokumentacionih materijala za istupanje ministra na sjednicama, simpozijima, konferencijama i drugim skupovima u zemlji i inozemstvu po zahtjevu Kabineta ministra;
- organizira poslove izdavačke djelatnosti iz nadležnosti Ministarstva iz oblasti unutrašnjih poslova i poslova policije u saradnji sa drugim organizacionim jedinicama Ministarstva i Upravom policije u skladu sa propisom iz člana 14. stav (1) tačka 27) Zakona;
- vodi i koordinira naučnoistraživačke poslove iz okvira djelatnosti Ministarstva u saradnji sa drugim organizacionim jedinicama Ministarstva;
- provodi saradnju sa fakultetima, institutima i drugim znanstvenim i stručnim tijelima koja se bave pitanjima iz oblasti kriminaliteta i sigurnosti;
- priprema i izrađuje informacije, izvještaje i druge informativno-dokumentacijske materijale iz djelokruga Ministarstva u saradnji sa drugim organizacionim jedinicama Ministarstva;
- osigurava i prati primjenu stručnih i naučnih metoda u oblasti analitike i izvještavanja i informatičkog sistema te pomaže drugim organizacioni. (MUP FBiH, izvor: http://www.fmup.gov.ba/)

Ministrastvo unutrašnjih poslova RS-a organizovano je u devet policijskih uprava i to: PU Banja Luka, PU Doboj, PU Bijeljina, PU I. Sarajevo, PU Zvornik, PU Prijedor, PU Trebinje, PU Mrkonjić Grad, PU Foča i PU Gradiška. Za naš rad važno je navest rad i nadležnosti Uprave za informacijsko-komunikacijsko poslove.

Nadležnosti ove Uprave su sljedeće:

- planira, organizuje, realizuje i nadzire rad u oblasti informaciono-komunikacionih tehnologija u Ministarstvu unutrašnjih poslova Republike Srpske kroz projektovanje, implementaciju i administriranje integrisanog informaciono-komunikacionog sistema Ministarstva,
- izrađuje Plan bezbjednosti informaciono-komunikacionog sistema Ministarstva, u skladu sa Zakonom o informacionoj bezbjednosti RS i podzakonskim aktima, Zakonom o zaštiti ličnih podataka BiH, Zakonom o zaštiti tajnih podataka BiH;
- izrađuje Politiku bezbjednosti IK sistema Ministarstva,
- prati propise i predlaže normativno regulisanje iz oblasti IKT,
- nosilac je poslova na unapređenju i razvijanju sistema zaštite informaciono-komunikacionih sistema,
- planira i uvodi odgovarajuće tehnologije i procedure i definiše mehanizme zaštite podataka,
- utvrđuje i organizuje jedinstven funkcionalni sistem elektronske obrade, prenosa, kriptozaštite i razmjene klasifikovanih podataka u Ministarstvu i stara se o njegovom održavanju i funkcionisanju,
- koordinira rad iz oblasti primjene IKT sa organizacionim jedinicama Ministarstva u sjedištu i policijskim upravama vrši instruktivno-nadzornu funkciju nad radom unutrašnjih organizacionih jedinica po liniji rada Uprave,
- predlaže i organizuje stručno-specijalističke obuke i druge načine usavršavanja za zaposlene. (MUP RS, izvor: mup.vladars.net)

Nadležnosti ***Policije Brčko distrikta Bosne i Hercegovine*** regulisane su Zakonom o Policiji Brčko distrikta Bosne i Hercegovine, te se u članu 13. ovog zakona navodi sljedeće ”Prikuplja, analizira i koristi kriminalističko-obavještajne informacije i podatke koristeći informante i druge operativne izvore podataka i informacija“, tako da i ova policija ima nadležnosti koje odnose na temu našeg rada.

Policija Brčko distrikta BiH je organizovana u sljedeće sektore koji su od važnosti za ovaj rad, a to su:

- Operativno komunikacijski centar,
  - Odsjek za informatiku i komunikacije,
- Jedinica kriminalističke policije, i

- Jedinica za administrativno-finansijske, tehničke poslove i logistiku.

5.1.3 Kantonalni nivo

U ovom dijelu će biti prikazani svi sektori i odijeli kantonalnih ministarstava unutrašnjih poslova:

MUP Kantona Sarajevo u Sektoru uniformisane policije postoji Odjeljenje za kripto-zaštitu i radio vezu, te u Sektoru kriminalističke policije postoje odjeljenja Odjeljenje za borbu protiv kompjuterskog i visokotehnološkog kriminala **i Krim-obavještajna jedinica.**

MUP Hercegovačko– neretvanskog kantona u Sektoru za potporu djeluje Odjela za informacijski sustav, dok u Upravi policije i Sektoru kriminalističke policije postoji Odjel za kriminalističko obavještajne poslove.

MUP Zapadno – hercegovačkog kantona je organizovan u četiri policijske uprave i to PU Grude, PU Ljubuški, PU Posušje i PU Široki Brijeg. Kao i MUP HNK MUP ZHK posjeduje Sektor za potporu koja ima direktora koji je nadležan za poslove Uprave policije.

Uprava policije MUP-a Kantona 10 u svojoj organizaciji posjeduje sljedeće odsjeke: Odsjek za analitičke poslove, Odsjek za informatičke poslove, Odsjek za zaštitu tajnih i osobnih podataka i praćenje propisa, zatim posjeduje Operativno komunikacijski centar i Odjel za informatičku potporu.

MUP Srednjobosanskog kantona u svojoj strukturi posjeduje Operativni centar, zatim Kriminalistička policija koja posjeduje odjel za kompjuterski kriminal.

MUP Bosanskopodrinjskog kantona u Sektoru kriminalističke policije posjeduje Odsjek kriminalističke tehnike i kriminalističko obavještajne poslove, Ured komesara zadužen kroz Odsjek za zaštitu tajnih podataka i analitiku, dok je Sektor uniformisane policije kroz odsjeke Operativnog centra i centra komunikacija te Odsjeka za vezu i informatiku.

Kroz *MUP Zeničko – dobojskog kantona* samo ministarstvo je zaduženo kroz Sektor za administraciju te Odsjek za informatiku, baze podataka i lične dokumente. Uprava policije je zadužena kroz Ured policijskog komesara za Odsjek za informatiku i Odsjek za komunikacije. Sketor kriminalističke policije

posjeduje Odsjek za kriminalističko-obavještajni rad, te kroz Jedinici za profesionalne standarde i Odsjek za razvoj načela i procedura i zaštitu tajnih podataka.

Uprava policije u *MUP-u Tuzlanskog kantona* u Sektoru kriminalističke policije ima Odsjek za kriminalističko-obavještajnu podršku, dok u Sektoru za materijalno, finansijske i opće poslove posjeduje Odsjek za telekomunikacije, Odsjek za analitiku i planiranje i Odsjek za informatiku. Jedinica za profesionalne standarde u svojoj organizaciji ima Odsjek za praćenje primjene propisa i zaštitu tajnih i ličnih podataka.

Za *MUP Posavskog kantona* se na web stranici jedino navodi nadležnost za obavljanje kriminalističko-tehničkih poslova.

Na web stranici *MUP-a Unsko – sanskog kantona* nije dostupna organizaciona šema, dostupan je dokument pod naslovom Inedeks registar informacija u posjedu MUP-u USK koji nam navodi nadležnosti sektor unutar ovoga ministarstva.

6. UPRAVLJANJE INFORMACIJAMA I ZAŠTITA PODATAKA U NATO SAVEZU

6.1 *Upravljanje informacijama i zaštita podataka u NATO savezu*

Ovaj dio rada će biti posvećen načini upravljanja informacijama u NATO savezu sa osvrtom na zaštitu podataka u Sjevernoatlantskom savezu. Za segment upravljanja informacija u većoj mjeri zadužen je NATO-ov Savjetodavni, komandni i kontrolni odbor, za dio upravljanja informacija uključeni su i Vojni, politički, sigurnosni i arhivski komitet NATO-a. Kada govorimo o vrstama informacija NATO navodi sljedeće:

1. informacije sa oznakom *neklasificirano* koje se javno objavljuju automatski, 1. januara dolazeće godine;
2. informacije sa oznakom *ograničeno* koje se poveravaju nakon 12 meseci i shodno tome automatski objavljuju javnosti 1. januara naredne godine; i
3. informacije sa oznakom povjerljivo, tajno i vrlo tajno za koje će se predlože skidanje tajnosti i pristup javnosti.(NATO, 2018:2-1)

Radi boljeg razumijevanja bit će predstavljen kratki historijat samog saveza i transformacije kroz koje prolazi u odnosu na sigurnosno okruženje, te politike, direktive, smjernice, standardi i pojmovi koji se koriste u ovom segmentu rada.

6.1.1 Osnivanje NATO saveza

Poslije Drugog svjetskog rata ambijent na tlu Europe je bio takav da se težilo ka što boljem pozicioniranju i zapadnih i istočnih aktera ovog velikog sukoba. Ovaj savez nastaje kao plod zajedničke želje zapadnih država i kao blok država koje su dijelile zajedničke interese i viziju Europe. U *Brošuri Uvid u novi NATO: pregled na zemlje partnere* (NATO, n.d.:2) se za samo osnivanje navodi „Nakon Drugog svjetskog rata istočnu i zapadnu Europu razdvojile su ideološke i političke podjele hladnog rata. Istočna Europa podlegla je dominaciji Sovjetskog saveza. Dvanaest država s obje strane Atlantika osnovale su, 1949. godine, Sjevernoatlantski savez (North Atlantic Treaty Organisation - NATO) kako bi suzbile rizik

pokušaja Sovjetskog saveza da proširi svoju kontrolu Istočne Europe i na druge dijelove europskog kontinenta“.

Kao i u svim proekonomskim i prodemokratskim procesima širom Europe, ali i svijeta glavnu riječ vodile su Sjedinjene Američke Države (u daljem tekstu SAD). Maršalov plan koji se odnosio na obnovu i stabilizaciju država Europe je svakako bio proces u kojem je bio uključen i sam Sjevernoatlantski savez te se tako navodi: „Uloga NATO-a, kao političkog i vojnog saveza, sastojala se u osiguravanju kolektivne obrane od bilo kojeg oblika agresije, te u održavanju sigurnog okružja za razvoj demokracije i gospodarskog rasta. Po riječima predsjednika SAD-a Harrya S. Trumana: "Marshallov plan i NATO dvije su dvije iste medalje".”(NATO, n.d.:2). Iz navedenog možemo vidjeti zašto je izraz vojno-politički savez postao ustaljen. Svakako najbitnija odlika saveza i interes samih članica je kolektivna odbrana u slučaju napada na državu članicu.

NATO savez je svojim osnivanjem i djelovanjem svakako opravdao svoju svrhu i obezbjedio ekonomski napredak, političku stabilnost, vojnu razvijenost i mnoge druge pozitivne karakteristike savremenih država.

6.1.2 Politika upravljanja informacijama u NATO-u

Kada govorimo o Politici upravljanja informacijama u NATO-u za sami početak možemo navest najvažnija obilježija same politike. Politiku upravljanja informacijama u NATO karakterišu tri ključne značajke koje mogu definisati i samu svrhu ovakvog dokumenta a to su sljedeće:

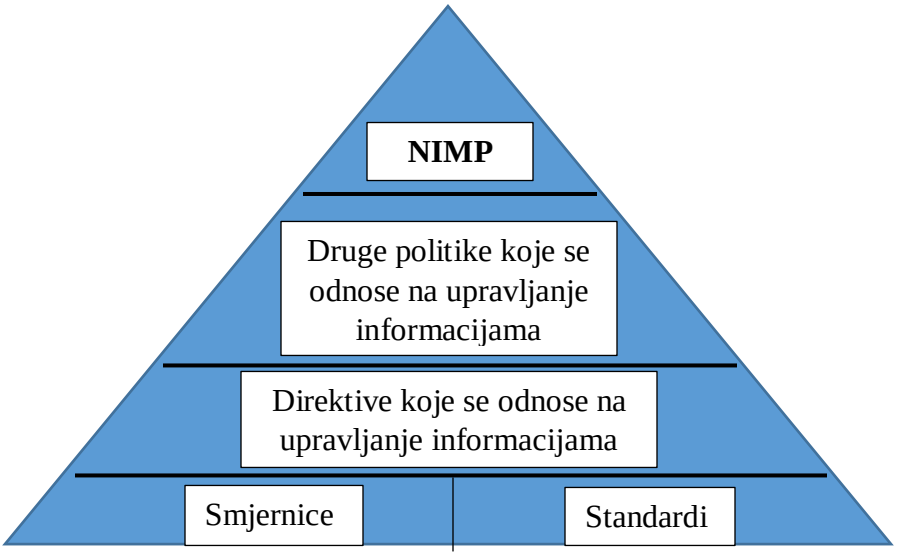
1. postizanje superiornosti informacija prvenstveno u okviru umreženog okruženja za razmjenu informacija;
2. efektivno i efikasno korištenje informacionih resursa;
3. identifikacija i očuvanje informacija od trajne vrijednosti za NATO. (Csanádi, 2018:146)

Pojam superiornosti informacija u ovom kontekstu predstavlja “relativnu prednost u pogledu na informacije koje posjedujemo. Ovo je sposobnost da se isporuče prave informacije pravim ljudima u pravo vrijeme, istovremeno smanjujući iste sposobnosti protivnika.“(ibid,2018:138)

Efektivno i efikasno korištenje informacija je težnja svakog ozbiljne organizacije i sistema, te identifikacija i očuvanje informacija od vrijednosti su svakako karakterstike sigurnosnih organizacija i na nižim nivoima.

Kada govorimo o procesu upravljanja informacijam u NATO savezu moramo u obzir uzeti dinamiku promjena u samom društvu, te samu potrebu za povećeanom pažnjom i obućenosti kada je u pitanju sektor sigurnosti. Kada govorima o literaturi i izvorima koji se odnose na ovaj sektor oni se većinom odnose na politici "need to know" kako navodi autor Csanádi (2018:138), isti autor navodi i da istraživanjem u ovom polju upravljanja informacija koje vežemo za NATO ne treba očekivati otkrivanje nekih tajnih informacija, te da se istraživanja po ovom pitanju većinom informišu iz politika, priručnika i dostupnih NATO dokumenata. Za "need-to-know" autor Csanádi (2018:138) navodi da je to princip koji se odnosi na način dijeljenja informacija NATO-a kako bi se dostavile informacije kome se tiču, bez obzira na klasifikaciju. Ova metoda dostavljanja informacija je odbrambena mjera.

Kada govorimo o okviru upravljanja informacijama u NATO-o tada navodimo ilustraciju koja se odnosi na NATO Information managment policy, u literaturi skraćenica se navodi na engleskom jeziku i glasi NIMP, dok bi prevod kod nas glasio Politika upravljanja informacija u NATO-u. Autor Csanádi (2018:139) navodi sljedeću šemu koja se odnosi na NATO okvir upravljanja informacijama



Slika br.7- NATO okvir za upravljanje informacijama

Kao što vidimo na samom vrhu okvira koji se odnosi na upravljanje informacijama nalazi se Politika upravljanja informacijama, odnosno engleska skraćenica NIMP. Za drugi nivo koji se odnosi na Druge politike koje se odnose na upravljanje informacijama navode se sljedeći primjeri:

1. Sigurnost unutar Organizacije Sjevernoatlantskog pakta (NATO) (C-M(2002)49): Publikacija Sjevernoatlantskog vijeća. Utvrđuje osnovne principe sigurnosti koje treba primijeniti od strane NATO-a, uključujući sigurnosne programe u cilju zaštite povjerljivih informacija. (Csanádi, 2018:139)
2. Upravljanje ne-klasificiranim informacijama (C-M(2002)60): Publikacija Sjevernoatlantskog vijeća koja uspostavlja principe zaštite i rukovanja neklasificiranim informacijama NATO-a. Ovaj dokument podržava prethodnu verziju Politike upravljanja informacijama NATO-a (NIMP) (PO(99)47) (Csanádi, 2018:139)
3. NATO politika i direktiva o javnom objelodanjivanju (C-M(2008)0116): Publikacija Sjevernoatlantskog vijeća. Utvrđuje principe politike o javnom objavljivanju NATO informacija i utvrđuje procedure, kao uloge i odgovornosti. (Csanádi, 2018:139)
4. Politika zadržavanja i raspolaganja NATO informacijama (C-M(2009)0021): Publikacija Sjevernoatlantskog vijeća. Određuje politiku zadržavanja i raspolaganja NATO informacijama. (Csanádi, 2018:139)
5. Politika NATO evidencije (C-M(2011)0043): Publikacija Sjevernoatlantskog vijeća. Ova politika uspostavlja okvir kako bi se osiguralo da se dokumentima NATO-a postupa efikasno, efektivno i bezbjedno kako bi služili interesima NATO-a. (Csanádi, 2018:140)

U gore navedenom dijelu vidimo da su politike koje se odnose na samo upravljanje informacijama duboko povezane i da imaju potrebu šireg pristupa ovom važnom dijelu organzacije. Kada navodimo direktive koje se odnose na upravljanje informacijama, predstavljenje su sljedeće:

1. Primarna direktiva o upravljanju informacijama (C-M(2008)113) Direktiva Sjevernoatlantskog vijeća za podršku implementaciji NIMP-a sa fokusom na superiornost informacija, uloge i odgovornosti i omogućavanje razvojnih direktiva i smjernica. (Csanádi, 2018:140)

2. Uprava NATO-a za upravljanje informacijama (NIMA) (C M(2009)0035) Organizacioni aranžmani Sjevernoatlantskog vijeća za upravljanje informacijama unutar NATO-a koji sadrže uspostavljanje NATO tijela za upravljanje informacijama i postavljaju specifične organizacijske uloge i odgovornosti i odnos s drugim akterima upravljanja informacijama.

I posljednji dio koji se odnosi na smjernice i standarde predstavlja dio za koji su zadužena tijela i uprave unutar NATO saveza, te one na osnovu politika i međusobnih ugovora uređuju ovaj dio Politike NATO-a o upravljanju informacijama.

6.1.3 Zaštita podataka- NATO i EU

Kada govorimo o zaštiti podataka u NATO-u moramao uzeti u obzir i regulaciju ovog polja i u drugim međunarodnim zajednicama koje su i članice NATO-a i u našem primjeru Europske unije. Kada govorimo o zaštiti podataka kao oblasti koja može biti i regulisana na nivou NATO, EU i na nacionalnom nivou. Izazov u ovome predstavlja usaglašavanje sve tri strane, odnosno pravnu ispravnost bilo kojeg procesa, procedure ili bilo čega drugog što se odnosi na zaštitu podataka.

Potreba za konstanim unaprijeđenjem i reformama ove oblasti prepoznata je od Europske Unije i to na način koji se odnosi na donošenje Opštom uredbom o zaštiti podataka (eng. General data protection regulation- skr. GDPR) koja je zamijenila do tada zastarjelu Direktivu o zaštitu podataka iz 1995. godine. Agencija za zaštitu podataka Bosne i Hercegovine (n.d.) u vezi Opće uredbe o zaštiti podataka navodi sljedeće „Novi Generalni propis o zaštiti podataka Europske unije (EU General Data Protection Regulation - GDPR) nazvan Opšta uredba o zaštiti podataka je Uredba (EU) 2016/679Europskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka, te o stavljanju izvan snage Direktive 95/46/EC, kojom se reguliše zaštita podataka i privatnost lica unutar Europske unije, a donosi i propise vezane za iznošenje podataka u treće zemlje“. Ova uredba EU se odnosi na zaštitu i sigurnost ličnih podataka i podataka kompanija, tako da ova uredba reguliše prava nosioca podataka, zatim unosi nove definicije i pojmove koji do tada nisu bili toliko zastupljeni u ovoj sferi, također reguliše i polja koja se odnose na obaveze i nadzor podataka i kazenu politiku po tom pitanju.

Kada su u pitanju kompanije uredba EU navodi sljedeće: “Što se tiče kompanija, novo zakonodavstvo se ne odnosi na sve kompanije u istoj mjeri, što ovisi o njihovoj veličini i tipu podataka koje prikupljaju, te načinu kako ih koriste.Manje kompanije morat će samo štititi svoje podatke o klijentima u skladu "sa zdravim razumom", dok će kompanije koje prikupljaju velike količine podataka poput tehnoloških kompanija, maloprodajnih firmi, pružatelja zdravstvenih usluga, banaka, osiguravajućih društava i sl. morati smanjiti količine podataka koje koriste i tačno odrediti koji impodaci doista trebaju i kako ih zaštititi“ (Agencija za zaštitu ličnih podataka BiH, n.d.).

Kada govorimo u saradnji EU i NATO-a autorica Zapala (2019:130-131) navodi sljedeće “ Imajući u vidu podjelu prava EU na primarno i sekundarno pravo, može se smatrati da su oni primarni zakon NATO-a, jer su donjeti u prvim godinama djelovanja Organizacije i predviđaju norme koje su činile funkcionisanje NATO-a“. Radi boljeg razumijevanja moramo u kratkim crtama i predstaviti šta znači peimarno i sekundarno pravo. Kratki vodič o Europskoj uniji (2022:1) nam za to navodi sljedeće:

Europska unija ima pravnu osobnost te kao takva ima vlastiti pravni poredak koji je odvojen od međunarodnog prava. Nadalje, pravo EU-a ima izravan ili neizravan učinak na zakone država članica te postaje dio pravnog sustava svake države članice. Europska unija sama je po sebi izvor prava. Pravni poredak obično se dijeli na primarno zakonodavstvo (Ugovore i opća pravna načela), sekundarno zakonodavstvo (koje se temelji na Ugovorima) i dodatno zakonodavstvo.

Argument da NATO spada u primarno pravo, odnosno zakonodavsto EU se izvodi iz tumačenja o ugovorima i pravnim načelima koje između država članice sa NATO-om, ali i EU i NATO.

Ako se vratimo na stavove o podjeli prava, EU i NATO koje navodi autorica Zapala (2019:130-131) te navodi “Ova podjela EU se možda neće odraziti na NATO nivou. Ovaj argument se zasniva na dva osnova. Prvo, NATO nema zakonodavnu nadležnost; sve odluke se donose konsenzusom. Drugo, pravne norme koje donosi centrala obavezuju samo unutar tog sjedišta. U tom smislu, usvojene mjere se mogu smatrati internim propisima, a ne NATO (sekundarnim) zakonom“. U ovim navodima možemo uvidjeti razliku koja se odnosi na EU i NATo i težnja ka približavanju ciljeva ovih aktera, donešenje odluka konsenzusom predstavlja usaglašavanje većeg broja aktera na širem polju, tako da uređenje polja zaštite podataka NATO-a na razini internih dokumenata koji to regulišu. U svojim zaključnim razmatranija a

koji se odnose na moguću konfrontaciju koja se odnosi na norme zaštite podataka od strane NATO-a i EU Zapala (2019:135) iznosi " Kako je utvrđeno, NATO nije obavezan GDPR-om, jer nije članica EU. Jedini subjekti koji su direktno obavezni da se pridržavaju ove Uredbe na nivou NATO-a su zajedničke države članice EU i NATO. Ove države su istovremeno vezane normama koje proizilaze iz obje Organizacije. Smatra se da u slučaju sukoba između standarda koje nameće svaka Organizacija, takva neslaganja treba da budu riješena u skladu sa opštim normama međunarodnog javnog prava". Svakako ranije prepoznata tri aktera po ovom pitanju NATO, EU i same države članice ovih organizacija svakako samim članstvom teže ka užom saradnjom i usaglašavanjem ovih organizacijam u mjeri u kojoj je to što više moguće.

6.2 *Savremeni izazovi u kontekstu podataka u NATO-u*

Naučni članak "NATO Decision-making: promises and perils of the Big Data age", u čijoj su izradili učetvovali NATO, Univerzitet u Bolonji i Institut za međunarodne poslove u Rimu tretira izazove sa kojima se susreće NATO, odnosno sa problemom "velikih podataka" u savremenom svijetu. Razvoj svih sfera društva, a pogotovo tehnološki razvoj natjerao je sve organizacije da svoje politike, smjernice i standarde koje primjenjuju urede na način efikasnijeg i što bržeg djelovanja i riješavanja nastalih problema, i, ili saniranja mogućih posljedica.

U samom uvodu u kontekstu izazova sa "velikm podacima" navodi se " Zasnovanje odluka na mnogo većoj količini informacija nego što je ranije bilo moguće moglo bi dovesti do prave revolucije u procesima donošenja odluka složenih organizacija, posebno zato što bi se te informacije ticale različitih dimenzija stvarnosti i stalno bi se ažurirale"(NATO, 2021:7). Potreba za sistemom koji bi se nosio sa navedenom dinamikom pristizanja informacija je svakako jedan od izazova sa kojim se susreću organizacije.

Pored ogromne količine dostupnih informacija, velika brzina kojom se podaci generišu i treba ih obraditi je još jedan odlučujući faktor velikih podataka. Takođe, oni će se obično nabaviti iz različitih izvora i njihova pouzdanost se mora pažljivo procijeniti. Konačno, bilo koji podatak može imati različitu vrijednost u različitim fazama procesa donošenja odluka. Sve ove karakteristike nameću posebne

zahtjeve organizacijama koje imaju za cilj korištenje velikih podataka kako bi smanjile neizvjesnost u kojoj rade.(ibid.)

Gore navedene činjenice svakako dovode u pitanje kapacitete arhiva, i u tradicionalnom smislu ali i u pohranjivanja tih informacija, zatim obrada i organizacija tih podataka i informacija. Sve te karakteristike savremenih izazova zahtijevaju dobro osmišljene politike i strategije koje su sveobuhvatne, provodive, efikasne i fleksibilne. Organizacije koje se suočavaju sa ovim izazovima zahtijevaju tehnološku razvijenost na veoma visokom niovu, zatim jako osposobljen i obučen kadar koji bi se konstantnim edukacijama i seminarima držao u korak sa tehnološkim dostignućima. Svi ovi akteri arhivskih kapaciteta, tehnološke savremenosti organizacija, strategija, politika, smjernica i nivoa ubučenosti kadra su faktori koji se mogu nositi sa izazovima koje nosi savremeno doba.

Kada govorimo korištenju tehnologije u sektoru sigurnosti autor Lucarelli i ostali (2021:10) u dijelu koji se odnosi na Tehnološke promjene i transformisano međunardonos sigurnosno okruženje navode sljedeće stavke koji su od važnosti:

- bolja svijest o situaciji,
- rano upozorenje na prijetnje i rizike,
- sposobnost sprečavanja i/ili zaustavljanja napada,
- korištenje tehnologije protiv tehnologija protivnika, i
- konačno odvraćanje od vrhunskog hibridnog ratovanja ili, barem, povećanje otpornosti na njega.

Prve tri stavke možemo posmatrati u domenu preventivnih mjera, dok zadnje dvije, u koliko se koriste u istom procesu možemo posmatrati kao vid represivnih mjera protiv neprijatelja. Kad pogledamo godinu u kojoj je ovaj naučni članak pisan 2021., sa trenutnim dešavanjima u svijetu sa sljedećim pretpostavkama, koje u to vrijem iznosi autor ” Dok digitalne tehnologije nastavljaju da dramatično rastu u opsegu i relevantnosti, one su duboko ugrađene u širi geopolitički okvir, uz ponovnu pojavu multipolarizma i nadolazeću konfrontaciju velikih sila. O ovoj povezanosti treba razgovarati i razumjeti jer ona utječe ne samo na sigurnost već i na ekonomske i tehnološke domene”(ibid.,2021:11). Previđanje ovog tipa, kojeg u današnje vrijeme možemo vidjeti kroz rat u Ukrajini, i multipolarizma koje se javlja

kroz Rusiju na jednoj strani i SAD-e i NATO na drugoj strani, možemo svesti pod gore navedenu stavku koja se odnosi *na bolju svijest u situaciji*.

Također određeni vakum u međunarodnom pravu u kontekstu upravljanja informacija i zaštite podataka predstavlja određenu prepreku smatra Lucarelli sa svojim saradnicima (2021:11): ”Velike i srednje sile se sve više oslanjaju na suprotstavljeno oružje, kako fizičko tako i sajber, koje je u stanju da stvori štetu brzo, širom svijeta iu velikim razmjerima. Međutim, u međunarodnom pravu ostaje vakuum. A takav vakuum je teže popuniti zbog spomenute interakcije geopolitike i tehnologija. Različite sile zamišljaju tehnologiju – i ono što im ona može donijeti u smislu koristi – na različite načine, i nisu spremne međunarodno regulisati ovo polje konkurencije i ratovanja”. Razlog vakuma možemo tumačiti kao interes u zloupotrebi ovakvih sredstava, razlog tome može biti efikasnost ovakvih sredstava, djelovanje i po horizontali i vertikali u različitim dijelovima svijeta, najkraće rečeno ovakva sredstva djelovanja su poprilično jeftina s obzirom na konvencionlne oružja, te je njihova efikasnost određena ciljem nanošenja štete.

Težnja NATO-a se odnosi na relalnu situaciju, te zaštitu strukture i građana ”U tako brzo promjenjivom sigurnosnom okruženju, aktivnosti NATO-a i saveznika direktno ili indirektno brane svakodnevni život građana. U doba velikih podataka, umjetne inteligencije i sveprisutnog korištenja interneta, izazov je odbraniti informacijsko okruženje koje se stalno širi uz zadržavanje svih njegovih funkcionalnosti” (Lucarelli, et al.,2021:11). Zadržavanje što boljeg sigurnosnog ambijenta kao cilj NATO, je težnja svih pojedničnih aktera, u savremenom svijetu svakako je neophodna modernizacija i prilagođavanje na različite situacije.

7. CYBER SIGURNOST U BOSNI I HERCEGOVINI I MEĐUNARODNI STANDARDI

7.1 *Cyber sigurnost Bosne i Hercegovine u kontekstu informaciono-komunikacijskih sistema*

Narušavanje sigurnosti kroz napade, prijetnje, opasnosti i izazove iz cyber prostora su postali uobičajne pojave u savremenom svijetu, te su postali pojmovi i teme sa kojima se susrećemo na dnevnom nivou. Ovaj dio rada će predstavljati prostor u kojem ćemo predstaviti i definisati pojmove koji se odnose na na prijetnje i izazove iz cyber prostora, te samu definiciju cyber prostora. Autor Vajzović (2019:531) navodi da "život modernih informacijskih društva sve više integriše u cyber prostor, a samim time i sigurnosni izazovi sve više proizlaze iz istog domena", neminovan razvoj svih društvenih sfera sa sobom nosi nove izazove i prijetnje, također se predstavlja i način moguće prevencije negativnih posljedica na sljedeći način, a koji je povezan sa prethodno navedenim tekstom "Ima li se to na umu, jasno će biti zašto se otpornost jednoga društva, države, političkog, ekonomskog i sigurnosnog sistema, medijska i informacijska pismenost sve očitije percipira kao jedna od ključnih kompetencija - i svakoga građanina pojedinačno i društva u cjelini".(ibid.)

7.1.1 Cyber prostor

Postoji početna potreba za definisanjem pojma cyber prostor, iz razloga odvijanja svih procesa i aktivnosti koji se odvijaju u tom prostoru. NATO prepoznaje cyber prostor kao domen svojih operacija, te se navodi:

NATO je 2016. godine priznao cyber prostor kao domen operacija uz tradicionalne domene zraka, kopna i mora. Ovo omogućava vojnim zapovjednicima NATO-a da bolje zaštite misije i operacije od kibernetičkih prijetnji, uključujući korištenje nacionalnih cyber sposobnosti saveznika. Saveznici zadržavaju potpuno vlasništvo nad ovim sposobnostima – baš kao što saveznici posjeduju tenkove, brodove i avione. Kao i u svim drugim domenima, u cyber-prostoru akcije NATO-a su defanzivne, proporcionalne i u skladu sa međunarodnim pravom. Saveznici se slažu da svi možemo imati koristi od pravila zasnovanog, predvidljivog, otvorenog, slobodnog i sigurnog cyber prostora. (NATO, 2020)

Prepoznavanje potencijala cyber prostora, odnosno rizika, izazova i prijetnji koje mogu doći baš iz tog prostora i NATO svsrtavanje u svoje domene operacija, pored zraka, kopna i mora, nam još dodatno ukazuje na bitnost regulisanja, i preventivnog djelovanja prije ozbiljnijih posljedica. Također 2018.godine NATO je osnovao Operativni centar za cyber prostor.

Prema definiciji Nacionalnog instituta za standarde i tehnologiju SAD-a (2012:B-3), ***cyber prostor*** se definiše kao "Globalni domen unutar informacionog okruženja koji se sastoji od međuzavisne mreže informacionih infrastrukturnih sistema, uključujući internet, telekomunikacione mreže, računarske sisteme i ugrađene procesore i kontrolore".

Dok u Smjernicama za strateški okvir cyber sigurnosti u Bosne i Hercegovine (2019:5) za pojam cyber se navodi da je "Termin „cyber" (sajber; kibernetski / kibernetički prostor; eng. Cyber (space)) se koristi u ovom dokumentu i označava prostor koji je široko rasprostranjen i međupovezan digitalnim tehnologijama, uspostavljen uz pomoć i posredovanje kompjutersko-digitalne tehnologije. Pojam cyber prostor se danas koristi za sve što je na Internetu". Bosna i Hercegovina nema usvojenu državnu strategiju po pitanju cyber sigurnosti, te će nam dokument koji se odnosi na Smjernice za starteški okvir cyber sigurnosti u Bosne i Hercegovine iz 2019. godine biti od velikog značaja za naš rad. Svakako politike, strategije, smjernice, standardi i pravilnici su od ogromnog značaja za sigurnost u cyber prostoru, kako pojedinca tako i strukture.

Pitanjem cyber prostora se bavila i administracija 44. američkog predsjednika Baraka Obame. Prepoznavanje potencijala, kapaciteta, opasnosti, izazova, rizika i svega onoga što dolazi iz cyber prostora, prepoznato je u strategiji koju je objavljena 2011. godine se navodi:

Temelj međunarodne politike cyber prostora Sjedinjenih Država je uvjerenje da umrežene tehnologije imaju ogroman potencijal za našu naciju i svijet. U posljednje tri decenije mi, Sjedinjene Države, gledali smo kako ove tehnologije revolucioniraju našu ekonomiju i transformiraju naš svakodnevni život. Svjedoci smo i vanmrežnih izazova, poput eksploatacije i agresije, koji se kreću u cyber prostor. Kako se prilagođavamo suočavanju s tim izazovima, vodit ćemo primjerom. Sjedinjene Države će voditi međunarodnu politiku sajber prostora koja osnažuje inovacije koje pokreću našu ekonomiju i

poboljšavaju živote ovdje i u inostranstvu. U cijelom ovom radu temeljimo se na principima bitnim ne samo za američku vanjsku politiku, već i za budućnost samog interneta.

Prepoznavanje važnosti cyber prostora od Nacionalnog instituta za standarde i tehnologiju SAD-a, NATO-a i administracije Baraka Obame samo po sebi predstavlja veliko interesovanje za ovo polje, razlog tome možemo uvidjeti u opasnostima koji vrebaju iz ovog prostora po pojedince, kompanije, organizacije, institucije i sve državne strukture.

Kada je u pitanju nivo prepoznavanja i regulisanosti cyber prostora u Bosni i Hercegovini, u Smjernicama za strateški okvir cyber sigurnosti u Bosne i Hercegovine (2019:6), navodi se sljedeće: " Postojeći ljudski i materijalni kapaciteti, te kapaciteti organizacija nisu dovoljni da osiguraju potreban nivo sigurnosti u cyber prostoru u Bosni i Hercegovini. Različiti nivoi vlasti imaju različite nivoe pripremljenosti, koji su doveli do različitog pristupa pitanjima cyber sigurnosti u okviru Bosne i Hercegovine. Rezultat je nejednak nivo zaštite korisnika, kako u javnom, tako i u privatnom sektoru, a koji podriva ukupni nivo zaštite cyber prostora, ranjivost na prijetnje i napade, te nemogućnost pravovremenog djelovanja, saradnje i koordinacije sa ostalim državama u regiji i svijetu". Prepoznavanje potrebe za promjenama, unapređenjim i reformama može se prepoznati i u ovom polju društva. Shvatanje ozbiljnosti i potencijala cyber prostora za narušavanje sigurnosnog ambijenta vjerovatno će biti prepoznata nakon štetnih posljedica.

7.1.2 Cyber sigurnost i informaciono-komunikacijski sistemi

Centralni pojam ovog dijela rada je cyber sigurnost, za ovaj pojam postoji veliki broj definicija pa tako iz sfere ekonomija prema The Economic Times (n.d.) nju definišemo kao „Cyber sigurnost ili bezbjednost informacionih tehnologija su tehnike zaštite računara, mreža, programa i podataka od neovlaštenog pristupa ili napada koji su usmjereni na neovlašteno prisvajanje". Dok druga definicija cyber sigurnosti glasi da je to "Sposobnost zaštite ili odbrane korištenja cyber prostora od cyber napada" (Nacionalnog instituta za standarde i tehnologiju SAD-a, 2012:B-3). Tehnike, sposobnosti, mjere, aktinosti, procedure, su svakako pojmovi koje moramo uključiti u samu definiciju cyber sigurnosti.

Informaciono-komunikacione sisteme definišemo kao:

a. bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka;

b. digitalni podaci koji se pohranjuju, obrađuju, dobivaju ili prenose elementima opisanim u „a.“ u svrhu njihova rada, upotrebe, zaštite i održavanja; (Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini, 2019:34)

Aktivnosti koje provode međunarodne organizacije u BiH po pitanju cyber sigurnosti se ogledaju na način osnaživanja institucija koje se bave ovom problematikom, tako OSCE[7] za svoj angažman po unapređenja cyber sigurnosti predstavlja kroz sljedeće aktivnosti:

Angažman Misije OSCE-a u BiH (Misija) u oblasti cyber sigurnosti usmjeren je na unapređenje kapaciteta BiH da odgovori na sigurnosne prijetnje koje proizlaze iz cyber prostora u skladu s njezinim obavezama kao države članice OSCE-a. Pri radu se koristi racionaliziran i sveobuhvatan pristup koji uključuje spektar podrške u rasponu od strateške do operativne. Ovi napori uključuju podršku razvoju harmonizovanog strateškog okvira za cyber sigurnost, uspostavljanje timova za reagovanje u urgentnim cyber situacijama (CERT[8]) i izgradnju kapaciteta za borbu protiv cyber kriminala.

Preporuke date u Smjernicama za strateški okvir cyber sigurnosti u BiH po pitanju zaštite informaciono-komunikacionih sistema, sama važnost ovih sistema u svakodnevnom životu i radu je nemjerljiva, rizici koji se odnosne na ove sisteme koji se koriste u sektoru sigurnosti su još veća potencijalna meta napada i ometanja. Potrebe za efikasne mjere i aktivnosti koje bi se odnosile na zaštitu informaciono-komunikacijskih sistema bi trebale biti obrađene u državnoj strategiji, u Smjernicama za strateški okvir (2019:12) se navodi da “Informaciono-komunikacioni sistemi koji omogućavaju pružanje usluga ključnih za održavanje kritičnih društvenih i ekonomskih aktivnosti, treba da budu posebno zaštićeni. Skup ključnih usluga i baza podataka od kritičnog značaja, spisak operatora ključnih usluga i baza podataka i kritična informaciono-komunikaciona infrastruktura trebaju biti zakonski definisani. Uz definiciju treba biti propisana obaveza zaštite kritične informaciono-komunikacione infrastrukture operatorima ključnih usluga i baza podataka. Za sve operatore ključnih usluga i baza podataka potrebno je propisati minimalne sigurnosne mjere koje je potrebno poduzeti. Ove mjere treba da budu u skladu sa

[7] OSCE- eng. Organisation for Security and Co-operation in Europe. Bos.- Organizacija za sigurnosnu saradnju u Europi.
[8] CERT- eng.- Computer Emergency Response Team

cyber sigurnosnim standardima za sektor kojem taj operator pripada. Svaki od operatora ključnih usluga i baza podataka treba poduzeti mjere smanjivanja rizika po kritičnu informaciono-komunikacionu infrastrukturu. Ove mjere treba da budu rezultat provedene analize u skladu sa propisanom metodologijom analize rizika. Operatorima ključnih usluga i baza podataka potrebno je propisati obavezu redovne provedbe analize rizika.“

Aktivnosti koje se odnose na zaštitu informaciono-komunikacionih sistema su sljedeći:

1. Usvojiti metodologije analize rizika za sve operatore ključnih usluga i baza podataka po ključnim uslugama i sektorima u skladu sa nadležnostima;

2. Svaki operator treba identificirati informaciono-komunikacionu infrastrukturu koja je kritična za pružanje ključnih usluga za koje je on odgovoran;

3. Procijeniti rizik od ugrožavanja sigurnosti svih dijelova prethodno identifikovanih informaciono-komunikacionih sistema, poredati ih po negativnom utjecaju koji mogu imati i izračunati vjerovatnoću dešavanja;

4. Odlučiti koje rizike umanjiti i kojim mjerama, koje prihvatiti i za koje ne treba poduzimati nikakve mjere (nepoduzimanje mjera obavezno obrazložiti);

5. Napraviti registar identifikovanih rizika;

6. Propisati redovnu obavezu stalnog nadzora slabosti i prijetnji, te ažuriranja informacija o time izazvanim promjenama rizika. (Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini, 2019:13-14)

Pojedinačne odgovornosti aketera u zaštiti informaciono-komunikacionih sistema se ogledaju kroz metodologije analize rizika, identifikacije kritičnih tačaka za nesmetano pružanje ključnih usluga, procjene rizika, odabir eventualnih mjera za smanjenje rizika, pravljenje registra prepoznatih rizika, te kroz analizu, nadzor i informisanost pratiti tok mogućih promjena rizika.

Poboljšanje oblasti sigurnosti informaciono-komunikacionih sistema se ogleda i na poboljšanje možemo reči “civilnih“ odnosno javnih informaciono-komunikacijskih sistema. Prema dokumentu Smjernice za

strateški okvir cyber sigurnosti u Bosni i Hercegovini (2019:17-18) ova infrastrukturna oblast bi trebala biti uređena na sljedeći način:

„Operatori ove infrastrukture su svi nositelji dozvola koje izdaje Regulatorna agencija za komunikacije Bosne i Hercegovine. To uključuje davaoce usluge pristupa Internetu (eng. ISP), mobilnoj i fiksnoj telefoniji, te mrežne operatere. Ovi operatori treba da imaju zakonski propisanu obavezu provođenja cyber zaštite svojih sistema. Da bi se osiguralo provođenje zaštite, neophodno je definisati minimalno potrebne mjere zaštite i parametre čijim se nadzorom kontroliše provođenje zaštite. Operatore treba obavezati da koriste neutralnu tačku za razmjenu internetskog saobraćaja (IXP) za saobraćaj između institucija, te stimulisati da je koriste za sav saobraćaj unutar BiH. Privatne operatore treba stimulisati da ulažu u cyber zaštitu".

Politikama i strategijama uređenje ove oblasti kroz kontinuirane mjere nadzora, analiza i kontrole, se mogu podići na viši nivo, koji u konteksu zaštite građana treba da postoji. Saradnja operatera sa institucijama je neophodna, unapređenje, obučavanje i stimulacije kako operatera, tako i zaposlenika predstavljaju potrebu za održavanje i zadržavanje sigurnijeg ambijenta.

Preporuka za unapređenje sigurnosti razmjene informacija između institucija se odnosi na "Upotreba neutralne tačke za razmjenu internetskog saobraćaja (IXP[9]) eliminiše nepotrebno putovanje internet saobraćaja, između dva korisnika u zemlji, preko ISP-a[10] iz drugih zemalja. Ovo smanjuje sigurnosne rizike po podatke i snižava troškove za ISP. Bosna i Hercegovina ima uspostavljen jedan IXP u Univerzitetskom tele-informatičkom centru (UTIC) Univerziteta u Sarajevu, ali ih u budućnosti može biti i više. ISP-ovi treba da se obavežu, da saobraćaj između institucija u Bosni i Hercegovini koje koriste različite ISP-ove, isključivo putuje preko IXP-a, a nikad van zemlje" (Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini, 2019:18). Povezanost agencija iz oblasti sigurnosti preko IXP-a bi u velikoj mjeri povećalo sigurnost prilikom razmjene informacija i podataka.

Definisanjem usluga *Cloud computinga,* i nivoa sigurnosti koje ova usluga pruža treba razmotriti na način buduće upotrebe u startegijama i politikama iz ovog polja sigurnosti. U Smjernicama za strateški okvir cyber sigurnosti u Bosni i Hercegovine (2019:19) se za pojam Cloud computing-a navodi " Cloud

[9] IXP- eng. Internet exchange point- bos. neutralna tačka za razmjenu internetskog saobraćaja

[10] ISP- Internet service provider- bos. davalac usluge pristupa internetu

computing omogućava racionalnu i ekonomičnu upotrebu računarskih resursa. U slučaju upotrebe usluga cloud computing podaci se šalju i obrađuju van organizacije koja je njihov vlasnik. Mjesto obrade može biti i u drugoj državi. Ovo otvara pitanje provođenja sigurnosti ovakvih podataka i odgovornosti. Da bi se osigurao potreban nivo sigurnosti potrebno je koristiti samo davaoce usluga cloud computing koji imaju certifikate da zadovoljavaju međunarodne sigurnosne standarde, a posebno one koji se odnose na cloud sigurnost. Primjeri ovakvih standarda su porodica ISO 27000 standarda, a posebno ISO27017 fokusiran na cloud. Potrebno je razmotriti da li postoje podaci koji se ne bi smjeli slati u cloud ili u cloud van Bosne i Hercegovine. Takve podatke bi trebalo definisati i osigurati da se za njih ne koristi cloud, odnosno cloud van Bosne i Hercegovine.“

Preporuke koje se odnose na stimulaciju privatnih operatera iz informaciono-komunikacionog sektor, teže ka pronalasku najboljeg načina za rješavanje ovog pitanja, koje bi rezultiralo zadovoljstvom obje strane, odnosno institucija koje bi bile uključene i samih operatera. Potreba za organizovanu podršku, saradnju i oporavak nakon mogućih napada i incidenata bi predstavljalo dobar vid saradnje obje uključene strane.

Smjernice za javno-privatna saradnju po pitanju razmjene informacija bi se odnosilo na “Razmjena informacija o cyber sigurnosno interesantnim događajima između svih organizacija, javnih i privatnih, omogućava pravovremeno i adekvatno reagovanje na njih. Potrebno je imati uspostavljene mehanizme razmjene i zaštite i tajnih podataka između domaćih i stranih privatnih kompanija i korporacija i javnog sektora u BiH. Potrebno je osigurati da sve uključene strane mogu aktivno učestvovati u razmjeni informacija u skladu sa zakonima“ “ (Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini, 2019:27).

Dokument Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini predstavlja odličnu osnovu za izradu strategija na državnom nivou po pitanju cyber sigurnosti, razlog i karakteristike takvih strategija navodi nam Vajzović (2019:535) u svom radu Medijska i informacijska pismenost u sistemu cyber sigurnosti, „U okruženju cyber prijetnji (koje je promjenljiva kategorija), države moraju imati fleksibilne i dinamične strategije cyber sigurnosti. Državna strategija za cyber sigurnost jest plan mjera namijenjen poboljšanju sigurnosti i otpornosti infrastruktura i usluga; njome se određuje niz nacionalnih ciljeva i prioriteta koji bi se trebali postići u određenom vremenskom okviru“.

7.2 *Međunarodni standardi – ISO 27000*

Pored politika i strategija vezanih za sigurnost informacija i informacionih sistema važan segment na tom području su i međunarodni standardi iz te oblasti, u ovom slučaju to je standard ISO 27000 i ostali standardi iz ove serije. Standardizacija i certificranje po međunarodnim standardima je težnja svake ozbiljne kompanije, organizacije, institucije ili agencija, a pogotovo onih koji se bave razmjenom informacija iz polja sigurnosti. Autori Calder i Watkins (2015:38) navode sljedeće standarde iz ove serije:

- ISO/IEC 27000 – ISMS[11] pregled i rječnik;
- ISO/IEC 27001 – ISMS zahtjevi,
- ISO/IEC 27002 – Kodeks prakse za menadžment sigurnosti informacija,
- ISO/IEC 27003 – Smjernice za implementaciju ISMS-a;
- ISO/IEC 27004 – Mjerenje upravljanja sigurnošću informacija i metrika;
- ISO/IEC 27005 – Upravljanje rizikom sigurnosti informacija;
- ISO/IEC TR 27008 – Smjernice za revizore o kontroli informacione sigurnosti;
- ISO/IEC 27031 – ICT[12] spremnost za kontinuitet poslovanja.

Danas imamo preko 35 standarda koji su proistekli iz standarda ISO 27000, te se samim time vidi potreba za regulisanjem oblasti koja se odnosi na sigurnosti informacija.

Posljednji standard iz ove oblasti je ISO 27001:2022, noviteti koje donosi ovaj standard su sljedeći:

- Kontekst i opseg

Sada morate identificirati "relevantne" zahtjeve zainteresiranih strana i odrediti koji će biti adresirani kroz ISMS (sistem upravljanja sigurnošću informacija).

ISMS sada eksplicitno uključuje „potrebne procese i njihove interakcije".

- Planiranje

[11] ISMS- eng. Information Security Managment System
[12] ICT- eng. Information and Communications Technology

Ciljevi informacione sigurnosti sada se moraju pratiti i učiniti „dostupnim kao dokumentovana informacija“.

Postoji novi odjeljak o planiranju promjena u ISMS-u. Ovo ne navodi nikakve procese koji moraju biti uključeni, tako da biste trebali odrediti kako možete pokazati da su promjene ISMS-a zaista planirane.

- Podrška

Zahtjevi da se definira ko će komunicirati i procesi za ostvarivanje komunikacije zamijenjeni su zahtjevom da se definira „kako komunicirati“.

- Operacija

Zahtjev da se planira kako postići ciljeve informacione sigurnosti zamijenjen je zahtjevom da se uspostave kriteriji za procese za implementaciju radnji identifikovanih u klauzuli 6, i da se ti procesi kontrolišu u skladu sa kriterijima.

Od organizacija se sada traži da kontrolišu “procese, proizvode ili usluge koje se pružaju izvana” relevantne za ISMS, a ne samo procese.

- Učinak i evaluacija

Metode praćenja, mjerenja, analize i procjene efikasnosti ISMS-a sada moraju biti uporedive i ponovljive.

Pregled menadžmenta sada također mora uzeti u obzir promjene u potrebama i očekivanjima zainteresiranih strana. (IT governance, n.d., izvor: itgovernance.co.uk)

Veliki broj standarda reguliše ovo polje sigurnosti informacija, tako da postoje posebni standardi za različita polja, sektor zdravstva, bankarstva, interneta i aplikacija su samo neki za koje postoje standardi. U Bosni i Hercegovini Institu za standardizaciju Bosne i Hercegovine ima nadležnosti koje se odnose na sačinjavanje smjernica za strategije, te strategije iz ove oblasti. Također Institut za Mjeriteljstvo Bosne i Hercegovine i Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine su ispunile sve potrebne procedure i procese za certificiranje po međunarodnom standardu ISO 27001:2013. Stimulisanje i saradnja na ovom polju bi svakako povećao broj certificiranih agencija u Bosni i Hercegovini po ovom pitanju.

8. ZAKLJUČNA RAZMATRANJA

Važnost teme koja se obrađuje u ovom radu se ogleda u prepoznavanju jednog jako bitnog segemta u svim organizacijama, a pogotovo onih koje se bave sigurnosnim pitanjima, segment informacija i podataka, odnosno segment upravljanja i zaštite informacijama i podataka.

Generalna hipoteza ovog rada je glasila *Država Bosna i Hercegovina koja teži ka članstvu u EU i NATO-u mora da posjeduje efikasan način upravljanja i zaštite informacija i podataka u sistemu sigurnosti*, da bi posjedovali efikasan način upravljanja i zaštite potrebno je ulagati u tehnološku modernizaciju i obučavanje i ospobljavanje kadra. Uključivanje akademske zajednice koja se bavim sigurnosnim studijama, saradnja sa drugim državama i organizacija, učenje iz iskustva, samo su neki od načina kojima bi unaprijedili ovaj bitan segment. Također dobra opremljenost i osposobljenost policijskih agencija na svim nivoima može u velikoj mjeri uticati na efikasnost i kredibilitet sistema upravljanja informacijama i zaštite podataka u BiH.

Preventivni i represivni potencijal IT sektora je odavno prepoznat u mnogim državama, Bosna i Hercegovina i državne istitucije imaju ispred sebe puno posla po pitanju regulisanja i uređenja ovog sektora. Uvršavanje IT sektora u Sigurnosnu politiku je neophodno, definisanje kratkoročnih, srednjoročnih i dugoročnih ciljeva za regulisanje ove oblasti je od velikog značaja. Usvajanje strategija je od veoma velike važnosti za ostvarivanje ciljeva po pitanju nadzora i regulisanja IT sektora.

Smjernice i pravilnici su fundament za regulisanje oblasti upravljanja informacija i zaštite podataka, njih možemo svrstati u kratkoročne i srednjoročne planove za ostvarivanje određenih ciljeva. Politike i strategije bi pronašli u dugoročnim planovima, ali također i srednjoročnim. Preklapanja u kontekstu srednjoročnog planiranja u politikama, strategijama, smjernicama i pravilnicima se ogleda u jednoj zajedničkoj osobini koju bi trebali posjedovati, a to je fleksibilnost. Fleksibilnost bi se odnosila na adekvatnim i efikasnim odgovorima na prijetnje, opasnosti i izazove narušavanja integriteta sistema sigurnosti.

Sistem sigurnosti Bosne i Hercegovine pored svih prepreka i poteškoća kroz koje prolazi i na koje nailazi, uspijeva sačuvati efikasno funkcionisanje svih bitnih i vitalnih funkcija državnog sistema sigurnosti.

Glavni resurs koji održava rad ovog sistema je ljudski resurs, zapravo oni ljudi koji su opredjeljeni da sačuvaj integritet sigurnosnog sistema i suverenitet države Bosne i Hercegovine.

9. LITERATURA

Knjige:

1) Ibrahimagić O., Seizović. Z., Arnautović, S. (2010). *Politički sistem Bosne i Hercegovine 4 (Tom II)*, Promocult, Sarajevo.
2) Klaić, B. (2004). *Rječnik stranih riječi*. Matica Hrvatska. Zagreb.
3) Lisica, D; Bajramović, Z. (2021). *Planiranje u sektoru sigurnosti*. Fakultet političkih nauka. Univerzitet u Sarajevu. Sarajevo.
4) Zapala, I. (2019). Relationship between the EU and NATO Based on the Example of Data Protection Policy. Comparative Law. Nicolaus Copernicus University. Poljska. Toruń.
5) Abazović, M. (2012). *Državna bezbjednost*. Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije.
6) Beridan, I., Tomić, I., Kreso, M. (2001). *Leksikon sigurnosti*. DES. Sarajevo.
7) Cikotić, S. (2013). *Sigurnosne pretpostavke Bosne i Hercegovine*. Vijeće Kongresa bošnjačkih Intelektualaca. Sarajevo.
8) National Institute of Standards and Technology (2012). Information security. Guide for Conducting Risk Assessments. U.S. Department of Commerce.
9) Calder, A., Watkins S., (2015). IT governance: an international guide to data security and ISO27001/ISO27002. Sixth edition.
10) Csanádi, G. (2018). Information management in NATO (Part one). How NATO Defines and Organizes Information Management, Strategies and its Point of View. Applied Military Sciences.
11) International standard ISO/IEC 27000 (2016). Information technology- Security techniques- Information security management systems- Overview and vocabulary. Četvrto izdanje. Švicarska. Ženeva.
12) IT Governance (n. d.). ISO 27001 and ISO 27002:2022 updates. Izvor: https://www.itgovernance.co.uk/iso27001-and-iso27002-2022-updates
13) Lisica, D. Bajramović, Z. (2021). Planiranje u sektoru sigurnosti. Univerzitet u Sarajevu. Fakultet političkih nauka. Sarajevo.
14) Lucarelli, S., Marrone, A., Moro, F. N. (2021) Technological changes and a transformed international security environment.
15) NATO (2021). NATO Decision-Making in the Age of Big Data and Artificial Intelligence. NATO. Univerzitet u Bolonji. Institut za međunarodne poslove u Rimu. Belgija. Brisel.

Zakoni, politike i strategije:

1) Odbrambena politika Bosne i Hercegovine (2008). broj: 01-011-2978-51/08.
2) Opšti okvirni sporazum za mir u Bosni i Hercegovini (Daytonski mirovni sporazum).
3) Predsjedništvo BiH (2006). Sigurnosna politika Bosne i Hercegovine. Sarajevo,
4) Zakon o Direkciji za koordinaciju policijskih tijela i o agencijama za podršku policijskoj strukturi Bosne i Hercegovine (2008). PSBiH broj 180/08. Bosna i Hercegovina. Sarajevo.
5) Zakon o Državnoj agenciji za istrage i zaštitu (2004). "Službeni glasnik BiH", br. 27/2004, 63/2004, 35/2005, 49/2009 i 40/2012. Bosna i Hercegovina. Sarajevo.

6) Zakon o Graničnoj policiji Bosne i Hercegovine (2004). "Službeni glasnik BiH", broj: 50/04, 27/07 i 59/09. Bosna i Hercegovina. Sarajevo.
7) Zakon o odbrani Bosne i Hercegovine (2005). PSBiH broj 226/05. Bosna i Hercegovina. Sarajevo.
8) Zakon o Policiji Brčko distrikta Bosne i Hercegovine (2009). "Sl. glasnik Brčko distrikta BiH", br. 6/2021". Bosna i Hercegovina. Brčko distrikt Bosne i Hercegovine.
9) Zakon o Sigurnosno-obavještajnoj agenciji Bosne i Hercegovine (2004). PSS BiH broj 22/04. Bosna i Hercegovina. Sarajevo.
10) Zakon o zaštiti tajnih podataka (2009). "Službeni glasnik BiH" broj 12/09. Bosna i Hercegovina. Sarajevo.
11) Politika upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017-2022. godine (2017). Službeni glasnik BiH, broj 38/17.
12) Ministarstvo odbrane Bosne i Hercegovine (2021). Indeks registar informacija koje možete dobiti od Ministarstva odbrane Bosne i Hercegovine.
13) The White House (2011). International strategy for cyberspace. Prosperity, Security, and Openness in a Networked World.

Naučni članci, priručnici i bilteni:

1) Čutura, D. ...*et al.* (2010). Rad policije u zajednici u Bosni i Hercegovini – Priručnik. CPU d.o.o. Sarajevo.
2) Europski parlament (2022). Kratki vodič o Europskoj uniji - 2022.. Članak.
3) Kržalić, A., Purišević, F., Alispahić, B. (2020). Pojam i elementi sistema sigurnosti. Društvena i tehnička istraživanja.
4) Mecanović, I.(1991). Marketing informacija. Znanstveni rad. Pravni fakultet Osijek.
5) Ministarstvo sigurnosti Bosne i Hercegovine (2021). Granična policija Bosne i Hercegovine. Bilten. Bosna i Hercegovina. Sarajevo.
6) NATO (2018). Directive on the Public Disclosure of NATO Information. AC/324-D(2014)0010-REV.
7) NATO (2020). NATO Cyber Defence. Public Diplomacy Division (PDD). Press & Media Section.
8) NATO (n.d.). Uvid u novi NATO: pregled za zemlje-partnere. NATO Office of Information and Press. Brošura. Belgija. Brisel.
9) OSCE (2019). Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini. Bosna i Hercegovina. Sarajevo.
10) OSCE (n.d.). Cyber sigurnost. Misija OSCE u Bosni i Hercegovini. Sarajevo.
11) Vajzović, E. (2019). Medijska i informacijska pismenost u sistemu cyber sigurnosti. Kriminalističke teme. Zbornik radova.

Web izvori:

1) Agencija za zaštitu ličnih podataka Bosne i Hercegovine (n.d.). Šta je Opšta uredba o zaštiti ličnih podataka (GDPR). Izvor: www.azlp.ba. Pristupljeno: 20.10.2022.
2) Institut za standardizaciju Bosne i Hercegovine (n. d.) izvor: isbih.gov.ba. Pristupljeno: 20.10.2022.
3) Ministarstvo odbrane Bosne i Hercegovine (n.d.). Izvor: www.mod.gov.ba. Pristupljeno: 19.09.2022.
4) Ministarstvo sigurnosti Bosne i Hercegovine (n.d.). Izvor: www.msb.gov.ba. Pristupljeno: 20.09.2022.

5) Obavještajno-sigurnosna agencija Bosne i Hercegovine (n.d.). Izvor: www.osa-oba.gov.ba. Pristupljeno: 03.11.2022.
6) The Economic Times. (n. d.). What is 'Cyber Security'. Izvor: https://economictimes.indiatimes.com/definition/cyber-security. Pristupljeno: 06.11.2022.

Popis slika:

Naziv odsjeka i/ili katedre: Odsjek za sigurnosne i mirovne studije
Predmet: /

IZJAVA O AUTENTIČNOSTI RADOVA

Ime i prezime:	Nihad Malagić
Naslov rada:	Upravljanje informacijama i zaštita podataka u sistemu sigurnosti Bosne i Hercegovine
Vrsta rada:	Završni magistarski rad
Broj stranica:	90.

Potvrđujem:

- da sam pročitao/la dokumente koji se odnose na plagijarizam, kako je to definirano Statutom Univerziteta u Sarajevu, Etičkim kodeksom Univerziteta u Sarajevu i pravilima studiranja koja se odnose na I i II ciklus studija, integrirani studijski program I i II ciklusa i III ciklus studija na Univerzitetu u Sarajevu, kao i uputama o plagijarizmu navedenim na web stranici Univerziteta u Sarajevu;
- da sam svjestan/na univerzitetskih disciplinskih pravila koja se tiču plagijarizma;
- da je rad koji predajem potpuno moj, samostalni rad, osim u dijelovima gdje je to naznačeno;
- da rad nije predat, u cjelini ili djelimično, za stjecanje zvanja na Univerzitetu u Sarajevu ili nekoj drugoj visokoškolskoj ustanovi;
- da sam jasno naznačio/la prisustvo citiranog ili parafraziranog materijala i da sam se referirao/la na sve izvore;
- da sam dosljedno naveo/la korištene i citirane izvore ili bibliografiju po nekom od preporučenih stilova citiranja, sa navođenjem potpune reference koja obuhvata potpuni bibliografski opis korištenog i citiranog izvora;
- da sam odgovarajuće naznačio/la svaku pomoć koju sam dobio/la pored pomoći mentora/ice i akademskih tutora/ica.

Mjesto, datum **Potpis**

Sarajevo, 8.12.2022. godine _____