

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Gorazd Rednak

**Vpliv varnostne kulture na varovanje tajnih podatkov v
Ministrstvu za obrambo**

Magistrsko delo

Ljubljana, 2016

**UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE**

Gorazd Rednak

Mentor:

red. prof. dr. Miro Haček

Somentor:

red. prof. dr. Anton Grizold

**Vpliv varnostne kulture na varovanje tajnih podatkov na
Ministrstvu za obrambo**

Magistrsko delo

Ljubljana, 2016

Ne misli, da si dober, če si najboljši med najslabšimi.

(latinski pregovor)

Zahvaljujem se vsem, ki so mi pomagali in me spodbujali pri nastanku pričujočega dela. Še posebej se moram zahvaliti svoji družini za razumevanje in ženi, ki me je več kot vztrajno spodbujala pri delu, ter profesorici Klemenšek za pomoč pri lektoriranju naloge.

Gorazd Rednak

IZJAVA O AVTORSTVU MAGISTRSKEGA DELA

Podpisani Gorazd Rednak, z vpisno številko 21051212, sem avtor magistrskega dela z naslovom: **Vpliv varnostne kulture na varovanje tajnih podatkov v Ministrstvu za obrambo.**

S svojim podpisom zagotavljam, da:

- da je predloženo delo plod izključno mojega lastnega raziskovalnega dela;
- sem poskrbel, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbel, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisal v predloženem delu;
- se zavedam da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli z. ideje predstavljene kot moje lastne – kaznive po zakonu (Zakon o avtorskih in sorodnih pravicah (UL RS, št. 16/07-UPB3, 68/08, 85/10 Skl.US: U-I-191/09-7, Up-916/09-16)), prekršek pa podleže tudi ukrepom Fakultete za družbene vede v skladu z njenimi pravili;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za družbene vede;
- je elektronska oblika identična s tiskano obliko magistrskega dela ter soglašam z objavo magistrskega dela v zbirki »Dela FDV«.

V Ljubljani, dne _____

Podpis avtorja: _____

Vpliv varnostne kulture na varovanje tajnih podatkov na Ministrstvu za obrambo

Magistrsko delo je prispevek k poglobljenemu razumevanju normativne ureditve varovanja tajnih podatkov v R Sloveniji in na Ministrstvu za obrambo. Kljub tako postavljenemu institucionalnemu okvirju varovanja tajnih podatkov v R Sloveniji in izgrajenemu sistemu preverjanja, varovanja in dostopanja do tajnih podatkov se tajni podatki preko anonimk razkrivajo v javnosti. Največji problem je v tem, da se v javnosti pojavljajo tajni podatki Ministrstva za obrambo.

Magistrsko delo vključuje raziskovanje in vlogo že izgrajenega nacionalnega sistema varovanja tajnih podatkov v državi ter na ministrstvu za obrambo kot del širšega nacionalno varnostnega sistema varovanja tajnih podatkov v R Sloveniji. Že izgrajen del nacionalnega varnostnega sistema varovanja tajnih podatkov bom primerjal z rešitvami v NATO in izbranimi državami EU.

V prvem delu magistrsko delo obsega opredeljevanje teoretičnih pojmov od tajnosti, tajnih podatkov, varnostne kulture do dovoljenja za dostop do tajnih podatkov. Predstavljen je nacionalni sistem varovanja tajnih podatkov z vlogo in pomenom Urada za varovanje tajnih podatkov kot nacionalne varnostne avtoritete. Predstavljen je Zakon o varovanju tajnih podatkov v primerjavi z rešitvami v nekaterih izbranih državah Evropske unije. Podrobneje je analiziran sistem varovanja tajnih podatkov na ministrstvu ter sistem izobraževanja in usposabljanja zaposlenih za delo in ravnanje s tajnimi podatki. Poseben poudarek je na izvajanju tematskih nadzorov na področju tajnih podatkov v upravnem delu ministrstva in v Slovenski vojski.

V drugem delu predstavljam analizo do sedaj izgrajenega sistema varovanja tajnih podatkov na ministrstvu, kjer so posebej analitično obdelani pridobljeni podatki s pomočjo anketnega vprašalnika, ki so ga izpolnjevali zaposleni tako v upravnem delu kot v Slovenski vojski. Analiza izpolnjenih anketnih vprašalnikov je pokazala, da gre pri razkrivanju podatkov ministrstva v javnosti za željo po opozarjanju zaposlenih nad slabimi razmerami v ministrstvu. Na drugi strani pa, kot kažejo podatki, se zaposleni v obrambnem sistemu z razkrivanjem tajnih podatkov ministrstva v javnosti na določen način maščujejo ministrstvu zaradi slabega vodenja ministrstva.

Ključne besede: tajni podatek, sistem varovanja tajnih podatkov, nacionalno varnostni sistem, varnostna kultura, razkrivanje tajnih podatkov v javnosti.

The impact of security culture on protection of classified information within the Defence Ministry

This master's thesis makes a contribution to an in-depth understanding of the regulatory framework of the protection of classified information at the Ministry of Defence of the Republic of Slovenia. One of the main problems arising in this context is the disclosure of the Ministry's classified information in the public. In order to ensure the confidentiality of the information, the Ministry has adopted the necessary measures which include: security clearance of persons that have access to classified information, establishment of appropriate security areas, and implementation of technical and physical security measures; nevertheless, the Ministry's classified information keeps appearing in the public.

Therefore, the thesis includes a research of the already established national system for protection of classified information in Slovenia and at the defence Ministry, which forms part of the wider national security system for protection of classified information in the Republic of Slovenia. The already established national security system for protection of classified information is compared to solutions within NATO and the EU. The first, theoretical part of the thesis defines theoretical terms, breaks down the national system for protection of classified information in the Republic of Slovenia, with the emphasis on the Classified Information Act and its comparison to the solutions within NATO and the EU, and the system of education and training of employees in the work with and handling of classified information. Special attention is given to thematic surveillance of classified information both in the civilian part of the Ministry and in the Slovenian Armed Forces.

The second part of the thesis analyzes the already established system for protection of classified information within the Ministry and provides a detailed processing of information by surveying employees of both the civilian part of the Ministry and the Slovenian Armed Forces. The results of the survey demonstrate that when disclosing the Ministry's classified information in the public, the Ministry's employees either wish to warn of the bad situation within the Ministry or to take revenge on the Ministry's leadership for their poor management.

Key words: classified information, classified information protection system, national security system, security culture, disclosure of classified information in public.

KAZALO

UVOD	1
1 METODOLOŠKI OKVIR	5
1.1 PREDMET RAZISKOVANJA	5
1.2 RAZISKOVALNI CILJI IN POMEN MAGISTRSKEGA DELA	5
1.3 RAZISKOVALNI VPRAŠANJI	7
1.4 METODOLOGIJA	8
2 TEORETIČNI OKVIR	10
2.1 TEMELJNI POJMI	11
2.1.1. Varnost	11
2.1.2. Tajnost	13
2.1.3. Tajni podatek	13
2.1.4. Dovoljenje za dostop do tajnih podatkov	14
2.1.5. Varnostni zadržek	14
2.1.6. Varnostna kultura	16
3 SISTEM VAROVANJA NACIONALNIH TAJNIH PODATKOV V SLOVENIJI	19
3.1 STOPNJE TAJNOSTI V NACIONALNEM SISTEMU VAROVANJA TAJNIH PODATKOV	23
3.1.1 Stopnje tajnosti v NATO	24
3.1.2 Spreminjanje stopenj tajnosti v NATO	26
3.1.3 Stopnje tajnosti v EU	26
3.2 PREVERJANJE IN DOSTOPANJE DO TAJNIH PODATKOV V NEKATERIH IZBRANIH DRŽAVAH EVROPSKE UNIJE	27
3.2.1 Nemčija	28
3.2.2 Nizozemska	29
3.2.3 Švedska	30
3.2.4 Vloga in pomen nacionalnega varnostnega organa ter sistem	31
dostopanja do tajnih podatkov	31
3.3 ZAKON O TAJNIH PODATKIH	33
3.3.1 Nacionalni sistem preverjanja in varovanja tajnih podatkov	35
4 VAROVANJE TAJNIH PODATKOV V MINISTRSTVU ZA OBRAMBO	36
4.1 NOTRANJA ORGANIZACIJSKA STRUKTURA MO	36
4.2 LONGITUDIALNA ANALIZA ORGANIGRAMOV MO	38
4.3. SPREMEMBE V NOTRANJI ORGANIZIRANOSTI NA MO	39
4.3.1 Hierarhični nivoji na ministrstvu za obrambo	41
4.3.2 Organizacijska razvejanost ministrstva od leta 1990 do 2006	44
4.4 PRAVNA UREDITEV VAROVANJA TAJNIH PODATKOV NA MINISTRSTVU	47
4.5 PRAVILNIK O VAROVANJU TAJNIH PODATKOV V MO	48
4.5.1 Osnovno in dodatno usposabljanje za ravnanje s tajnimi podatki	53
4.5.2 Tematski nadzori nad tajnimi podatki v MO in SV	56
4.5.3 Bistvene ugotovitve po tematskih nadzorih v upravnem delu MO	58
4.6 VARNOSTNA OBMOČJA V MINISTRSTVU ZA OBRAMBO	59
4.6.1 Načrti za varovanje tajnih podatkov	60
4.6.2 Splošni del načrta varovanja	60
4.6.3 Posebni del načrta varovanja	62
4.6.7 SMERNICE TEHNIČNEGA VAROVANJA IN OBJEKTOV MINISTRSTVA	64
5 UGOTAVLJANJE VZROKOV ZA RAZKRIVANJE TAJNIH PODATKOV MO	65
5.1 ANKETIRANJE ZAPOSLENIH V MINISTRSTVU LETA 2013	75
6 VREDNOTENJE PODATKOV IZ ANKETNIH VPRAŠALNIKOV	78
7 SKLEP	80

7.1. VERIFIKACIJA RAZISKOVALNIH VPRAŠANJ	82
8 LITERATURA	86

PRILOGA ANKETNI VPRAŠALNIK

KAZALO TABEL:

TABELA 2.1: SPEKTER VOJAŠKE KULTURE	17
TABELA 4.1: SPREMEMBE V NOTRANJJI ORGANIZACIJI MORS-A OD 1990 DO 2006.....	40
TABELA 4.2.: SPREMEMBE ŠTEVILA HIERARHIČNIH NIVOJEV V MO	42
TABELA 4.3: ORGANIZACIJSKA RAZVEJANOST V MINISTRSTVU PO POSAMEZNIH SPREMEMBAH	44
TABELA 5.1. VARNOSTNA OSVEŠČENOST NOVO SPREJETIH DELAVCEV V MO (v %)	66
TABELA 5.2. ODNOS ANKETIRANCEV DO SODELAVCEV, KI ZUNAJ MO RAZKRIVAJO TAJNE PODATKE (v %)	67
TABELA 5.3. RAZLOGI ZA RAZKRIVANJE TAJNIH PODATKOV IN ZAUPNIH PODATKOV ZUNAJ MO (v %).....	67
TABELA 5.4. STALIŠČA POSAMEZNIKOV GLEDE ANONIMK KOT SREDSTVA ZA REŠEVANJE NOTRANJNH TEŽAV IN PROBLEMOV V MO (v %)	69
TABELA 5.5. OCENA RAVNANJA Z ZAUPNIMI DOKUMENTI IN PODATKI V VARNOSTNEM SMISLU V MO S STRANI ZAPOSLENIH (v %) ...	70
TABELA 5.6. STALIŠČA GLEDE USPOSABLJANJA GLEDE RAVNANJA S TAJNIMI PODATKI (v %).....	72
TABELA 5.7. STALIŠČA GLEDE NAČRTA VAROVANJA TAJNIH PODATKOV I. (v %).....	73
TABELA 5.8. STALIŠČA GLEDE NAČRTA VAROVANJA TAJNIH PODATKOV II. (v %).....	74

UVOD

Varnost je v zadnjih letih postala dobrina, vrednota in potreba, ki se vsak dan bolj in bolj nanaša na kakovost življenja. Še posebej se o varnosti sprašujemo zaradi dogodkov, ki so se letos zgodili v Bruslju in lanskega novembra v Parizu. Sodobne države se na tovrstne grožnje odzivajo z izgrajevanjem sodobnih nacionalno varnostnih sistemov, v katerih imajo v zadnjem obdobju vse večjo vlogo obveščevalne in varnostne službe.

Širšo dimenzijo varnosti je zelo dobro izpostavil Grizold v svoji sedaj že kar klasični definiciji, v kateri je zapisal, da je varnost stanje, v katerem je uravnotežen fizični, duhovni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave (Grizold 1999,).

Varnost ni povezana z le enim področjem človekovega delovanja, ampak je potreba po varnosti prisotna na vseh področjih človekovega delovanja in delovanja širše skupnosti, v katere se povezuje človek. To dimenzijo varnosti je izpostavil Anžič, ko pravi:

»Zavestno prizadevanje za vzpostavitev stanja varnosti je civilizacijska in kulturna kategorija, ki zajema vse vidike varnosti, tj. gospodarsko, socialno, kulturno, politično, pravno, ekološko, obrambno, itd., se pravi tiste pojavne oblike družbenega življenja, ki se štejejo za družbene vrednote. Oblike družbene organiziranosti zajemajo regionalno, nacionalno, mednarodno in svetovno varnost.«

Nacionalna varnost se opredeljuje tudi kot varnost državnega ozemlja, prebivalstva in njihove lastnine, ohranjanje nacionalne suverenosti kot zagotavljanje ustreznih razmer za uresničevanje temeljnih funkcij družbe (Anžič 1997, : 18). Nacionalna varnost sicer res na eni strani zagotavlja varnost svojih državljanov ter odpravlja vire njihovega ogrožanja. Toda hkrati preko svojih varnostnih organov tudi sama lahko postane vir ogrožanja individualne varnosti.

Zaradi potrebe po usklajenem delovanju vseh akterjev nacionalne varnosti se čedalje bolj pojavlja potreba po prikrivanju ali skrivanju podatkov in informacij, ki so v

nacionalnem interesu. Pojav tajnosti na področju nacionalne varnosti se je pojavil kot logična posledica zaščite države, prebivalstva, suverenosti in državnega ozemlja.

»Tajnost je kompleksen pojav, ki vključuje potrebo in pravico države do zasebnosti in do varovanja svojih tajnosti« (Brezovšek, Črnčec 2010, 16). Zaradi varovanja državnih tajnosti in skrivnosti so države v okviru nacionalno varnostnih sistemov razvile poseben sistem varovanja tajnih podatkov. Ta sistem vključuje postopke varnostnega preverjanja, izdaje dovoljenj za dostop do tajnih podatkov in poseben sistem fizičnih in tehničnih ukrepov za varovanje tajnih podatkov. Tudi R Slovenija kot suverena država, je takšen sistem pričela graditi leta 2002. Tega leta je namreč Vlada R Slovenije sprejela sklep o formiranju in določitvi nalog Urada Vlade R Slovenije za varovanje tajnih podatkov.

Na ta način smo dobili v Sloveniji organ, ki ga lahko poimenujemo tudi drugače, kot Nacionalni varnostni organ. Glavna naloga Urada Vlade R Slovenije za varovanje tajnih podatkov – v nadaljevanju UVTP – je organizacija in koordinacija dela posameznih organov, ki izvajajo izdajanje dovoljenj za dostop do tajnih podatkov in varovanje tajnih podatkov v okviru posameznih vladnih resorjev.

UVTP je v dosedanjem štirinajstletnem obdobju poskrbel, da je R Slovenija na nacionalnem nivoju dobila ustrezen institucionalni okvir za izgradnjo svojega lastnega sistema za varovanje tajnih podatkov. Institucionalni okvir smo gradili na podlagi izkušenj nekaterih držav Evropske unije, ki so se pri gradnji svojih sistemov, povejmo pošteno, zgledovale po zvezi NATO.

Ali je ta nacionalni sistem preverjanja, izdajanja in dostopanja do tajnih podatkov ustrezen za R Slovenijo? Mar ni preteklo že dobrih deset let, kar se je Zakon o tajnih podatkih zadnjič spremenil. V trenutno veljavnem zakonu imamo zapisane dvoje vrst varnostnih zadržkov, ki se niso spremenili vse od leta 2001 dalje, ko je bil sprejet prvi zakon. Glede na razpoložljive podatke v petnajstih letih v R Sloveniji ni bil niti eni osebi izrečen varnostni zadržek zaradi *»članstva ali sodelovanja v organizacijah ali skupinah, ki ogrožajo vitalne interese Republike Slovenije ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je Republika Slovenija.«* (ZTP-UPB2 50/06). Zakaj? Ker organi, ki izvajajo varnostno preverjanje, ne vedo, katere so tiste

organizacije ali skupine, ki bi ogrožale vitalne interese članice političnih in obrambnih varnostnih zvez, katerih članica je Republika Slovenija.

V zvezi z varnostnim preverjanjem in nastopom ekonomske krize v državi se vedno več vprašanj pojavlja v zvezi s t. i. prezadolženostjo oseb, ki posedujejo veljavno dovoljenje za dostop do tajnih podatkov. Kako opredeliti prezadolženost zaposlenega? Je to 250 EUR ali 25.000 EUR. Seveda je v zvezi z zakonom o tajnih podatkih potrebno omeniti »nesrečni« tretji člen zakona, ki osebam z nastopom mandata omogoča dostop do vseh tajnih podatkov v R Sloveniji. V Sloveniji imamo devetnajst različnih kategorij oseb, ki se jim dovoljenje za dostop do tajnih podatkov »avtomatsko podeli«, brez vsakega varnostnega preverjanja. Tako naši poslanci samo podpišejo izjavo, da so seznanjeni z vsemi predpisi na področju tajnih podatkov in že lahko dostopajo do vseh tajnih podatkov. Ko pa dobijo v branje taje dokument, se po mojih izkušnjah niti na evidenčni list ne zanjo podpisati! Kdo jih je usposobil za določanje stopenj tajnosti, ali sploh vedo, kateri sta tisti dve značilnosti, ki določen podatek ali informacijo določita za taje podatek?

Evropske države takšnih izjem pri dostopanju do tajnih podatkov ne poznajo. V času pridruževanja NATO in EU je bil nacionalni sistem varovanja tajnih podatkov deležen vrste inšpekcij. Pri teh inšpekcijah, katerih namen je bil ugotoviti, na kakšen način bo R Slovenija varovala tajne podatke EU ali NATO, ni bilo večjih težav. Ampak res vsakokrat so se inšpekcije zaustavile pri naših izjemah pri dostopanju do tajnih podatkov in nam svetovale, da to poizkušamo spremeniti. Pa nismo od leta 2001 nikoli. Ali je morebiti kdo odgovarjal za to? Za politiko nacionalni sistem tajnih podatkov ni bil nikoli v prvem planu, zato se tega področja niso dotikali. No morebiti so se ga enkrat, leta 2003, ko so povsem spremenili osnutek zakona o tajnih podatkih, katerega je šest mesecev pripravljala medresorska delovna skupina. Spremenili pa so ga tako, da so v tretji člen med izjeme zapisali poslance, župane in občinske svetnike.

Magistrsko delo je v večjem delu osredotočeno na vprašanje varovanja tajnih podatkov na Ministrstvu za obrambo v povezavi z varnostno kulturo zaposlenih za obravnavanje in varovanje tajnih podatkov. Zakaj varnostna kultura zaposlenih? Menim, da obstaja vzročna povezava med varnostno kulturo zaposlenih in razkrivanjem tajnih podatkov

ministrstva v javnosti. Spomnimo se samo leta 2000 in takratne afere »Sava«¹, s katero je bilo močno povezano Ministrstvo za obrambo oziroma Obveščevalno varnostna služba ministrstva. Kaj se je zgodilo?

Meseca junija 2000 je novinar časopisa Večer objavil podatke o domnevnem sodelovanju med OVS in eno izmed tujih tajnih služb na področju Balkana. Glede na to, da imata obe državi, ki sta bili omenjeni v aferi, eno skupno točko, reko Savo, je afera dobila ime po reki Savi. Objava članka je imela velik odmev na celem Balkanu in tudi širše. Praktične posledice te afere so bile v velikem zmanjšanju sodelovanja tujih služb z OVS, pa tudi Ministrstvu za obrambo so se zaprle možnosti sodelovanja z drugimi državami.

Pregon storilcev je bil uspešen, saj so bili v relativno kratkem času odkriti in tudi kazensko ovadeni. Nihče pa ob takšnem dogodku in incidentu ter razkritju tajnih podatkov ni ugotavljal, kako je bilo z varnostjo prostorov, v katerih so se nahajali domnevno odtujeni dokumenti. Resnično se lahko vprašamo, kdo in na kakšen način je usposabljal zaposlene za varovanje dokumentov, kaj se odgovorne osebe v službi naredile za izgradnjo ustrezne varnostne kulture med zaposlenimi.

Odtekanje oz. razkrivanje tajnih dokumentov ministrstva v javnosti je velik problem Ministrstva za obrambo. Pristojni organi, po mojem vedenju, zbirajo podatke in informacije o vsakem primeru razkritja podatkov v javnosti, vendar se razkrivanje in odtekanje informacij preko anonimk, ministrstvu še vedno dogajata.

Kaj so motivi oseb, ki razkrivajo tajne podatke? Svetovno najbolj znani »žvižgač«, Edward Snowden, je ob prihodu na moskovsko letališče pojasnil njegove vzgibe in vzroke za razkritje tajnih podatkov. *»Glavni motiv je bil v tem, da obvesti javnost, kaj se dogaja v njenem imenu in proti njej. Želel je osvestiti ljudi, da jih ameriška vlada nadzoruje, s čimer krši ustavo in zakone ter njihove pravice«* (Prezelj, Grizold 2015, 682).

¹ Štiri osebe so bile zaradi storitve kaznivega dejanja kazensko ovadene, nihče ni bil pravnomočno obsojen. Sodišče je zahtevalo, da ministrstvo poda za vsakega ovadenega, oceno škodljivih posledic storitve dejanja!

1 METODOLOŠKI OKVIR

1.1 Predmet raziskovanja

Predmet raziskovanja magistrskega dela je varnostna kultura zaposlenih v Ministrstvu za obrambo v povezavi z varovanjem in dostopanjem do tajnih podatkov. V okviru tega opredeljenega predmeta raziskovanja se delo osredotoča na pregled in razvoj nacionalnega sistema preverjanja in varovanja tajnih podatkov v R Sloveniji ter v okviru tega pregled in razvoj podsistema varovanja, preverjanja in usposabljanja zaposlenih v Ministrstvu za obrambo. V okviru pregleda se bo preverilo, kako se zaposleni v ministrstvu usposablja za varovanje tajnih podatkov in na kakšen način se izvaja notranji nadzor nad tajnimi podatki v ministrstvu. Namen tega pregleda je ugotavljanje vzrokov, zakaj se tajni podatki ministrstva razkrivajo izven obrambnega sistema.

1.2 Raziskovalni cilji in pomen magistrskega dela

Glavni raziskovalni cilj magistrskega dela je povezati teoretska spoznanja o varnosti, o varnostni kulturi, o tajnosti, skratka o nacionalno varnostnem sistemu preverjanja za dostopanje do tajnih podatkov s problemom, ki se dnevno pojavlja, to je odtekanje tajnih podatkov Ministrstva za obrambo v javnost. Ali je problem v Zakonu o tajnih podatkih, Uredbi o varnostnem preverjanju ali v sistemu tehničnega varovanja na ministrstvu, to ni povsem jasno. Morebiti je vzrok za skoraj tedensko razkrivanje podatkov v javnosti v nepopolnem sistemu izobraževanja in usposabljanja do tajnih podatkov na ministrstvu. Je pomanjkljivost v izvajanju inšpekcijskih in tematskih nadzorov na tem področju? V okviru svojega magistrskega dela želim tudi analizirati pravni okvir sistema varovanja tajnih podatkov na ministrstvu, predvsem interni pravni akt Pravilnik o varovanju tajnih podatkov na MO, ki je izvedbeni akt zakona o tajnih podatkih. Na vsa ta vprašanja želim dobiti odgovore skozi teoretični in empirični del svojega magistrskega dela, ki jih bom v sklepnem delu predstavil in predstavil rešitve problema.

Upam, da bodo sklepne ugotovitve, zaključki in priporočila mojega dela prispevali k temu, da bodo odgovorne osebe za delovanje in funkcioniranje sistema varovanja tajnih podatkov na ministrstvu, ukrepale in izboljšale stanje na tem področju.

Na podlagi glavnega raziskovalnega cilja pa so zastavljeni posebni raziskovalni cilji tako teoretičnega kot tudi empiričnega dela.

V teoretičnem delu so glavni cilj naloge, da se preveri stopnja izgradnje nacionalno varnostnega sistema varovanja tajnih podatkov ter vloga in pomen UVTP-ja kot najvišjega nacionalnega varnostnega organa na področju tajnih podatkov v R Sloveniji. Analiziral bom naš Zakon o tajnih podatkih ter se posebej posvetil sistemu preverjanja in izdajanja dovoljenja za dostop do tajnih podatkov. Rešitve, ki so zapisane v našem zakonu, bom primerjal z rešitvami v drugih državah. Posebno pozornost bom posvetil Nemčiji, po kateri smo se v Sloveniji leta 2001 zgledovali pri pisanju našega prvega zakona. V tem delu bom pozornost posvetil tudi nacionalnemu varnostnemu organu, ki ima pomembno vlogo pri koordinaciji dela v okviru nacionalnega sistema varovanja tajnih podatkov. V tem delu bom primerjal posamezne rešitve označevanja tajnih podatkov z zvezo NATO in EU.

Posebna pozornost bo v prvem delu naloge posvečena Zakonu o tajnih podatkih, posameznim specifičnostim naše ureditve, kot je npr. vodenje postopka v skladu z Zakonom o splošnem upravnem postopku. Sledila bo analiza varovanja tajnih podatkov na ministrstvu, pred tem pa se bom posvetil organizacijski strukturi ministrstva, kako se je skozi leta razvijalo kot organizacija.

V empiričnem delu so glavni cilji naloge: analiza vzrokov razkrivanja tajnih podatkov ministrstva v javnosti s pomočjo izvedenih anketnih vprašalnikov v preteklih letih.

S pomočjo anketnega vprašalnika bodo teoretična spoznanja o varovanju tajnih podatkov pokazala, ali se na tem področju varovanja tajnih podatkov dela dobro ter katera področja je potrebno izboljšati.

Predmet moje raziskave in pričujočega magistrskega dela so torej vse teoretične značilnosti varnosti, tajnosti, dovoljenja za dostop do tajnih podatkov, varnostni

zadržek pri izdaji dovoljenja in pojem varnostna kultura; institucionalni okvir nacionalnega sistema varovanja tajnih podatkov, vloga in pomen Urada vlade R Slovenije za tajne podatke, značilnosti krovnega Zakona o tajnih podatkih v primerjavi z rešitvami v NATO² in EU; analiza nacionalnega podsistema varovanja tajnih podatkov na Ministrstvu za obrambo s poudarkom na pravilniku o tajnih podatkih, sistem izobraževanja za varovanje in dostopanje do tajnih podatkov, izvajanju tematskih nadzorov na področju tajnih podatkov; analiza podatkov, pridobljenih s pomočjo izvedbe anketnega vprašalnika med zaposlenimi v MO in SV.

1.3 Raziskovalni vprašanja

V okviru na ta način določenih raziskovalnih ciljev problema raziskovanja ter glede na izkušnje, ki sem si jih pridobil skozi leta pri izvajanju varnostnega preverjanja oseb za dostop do tajnih podatkov pri varovanju in obravnavanju tajnih podatkov na ministrstvu ter ugotavljanje vzrokov za razkrivanje tajnih podatkov izven ministrstva, se mi porajajo dvomi o pravilnosti ukrepov za zaščito tajnih podatkov na ministrstvu in zato si postavljam naslednjo **raziskovalno vprašanje**, ki ga bom v skladu s ciljem svojega magistrskega dela tudi poizkušal utemeljiti:

»Visoka stopnja varnostne kulture pri zaposlenih pozitivno vpliva na varovanje tajnih podatkov.«

Glede na številne afere, ki so bile v zadnjih letih povezane z odtekanjem in razkrivanjem tajnih podatkov ministrstva, domnevam, da sistem usposabljanja za delo s tajnimi podatki in nadzora nad tajnimi podatki v ministrstvu ni najbolj učinkovit.

Na podlagi dosedanjih teoretičnih spoznanj s tega področja postavljam še naslednjo **dodatno raziskovalno vprašanje**:

² North Atlantic Treaty Organization, ali tudi NATO zveza.

»Samo enoten sistem usposabljanja, nadzora in kontrole nad tajnimi podatki v organizaciji lahko zagotovi višji nivo stopnje varovanja tajnih podatkov.«

1.4 Metodologija

Metodološki pristop k zastavljenemu predmetu preučevanja temelji na znanstvenih disciplinah. Za doseg zastavljenih ciljev in namena izdelave magistrskega dela bom pri svojem delu uporabil kombinacijo različnih znanstvenih metod. Naj navedem le najpomembnejše med njimi:

- analiza sekundarnih virov (analiza in pregled relevantne domače in tuje znanstvene in strokovne literature),
- analiza primarnih virov ter primerljive mednarodne literature (pregled ter analiza in pregled normativnega okvirja varovanja tajnih podatkov v R Sloveniji, primerljivost našega sistema varovanja tajnih podatkov z nekaterimi državami EU, primerljivost stopenj tajnosti med našim nacionalnim sistemom in stopnjami tajnosti v NATO in EU),
- analiza normativnega pravnega okvirja na ministrstvu za obrambo s posebnim poudarkom na Pravilniku o tajnih podatkih na MO in SV, pregled izvajanja osnovnega in dodatnega usposabljanja, inšpekcije oz. tematski nadzori nad tajnimi podatki v ministrstvu, pregled in analiza organizacijske strukture delovanja ministrstva, ugotavljanje vzrokov razkrivanja tajnih podatkov ministrstva v javnosti s pomočjo anketnega vprašalnika (analiza izvedenega anketiranja med zaposlenimi v MO in SV, dojemanju varnosti, varnostne kulture, dostopanjem do tajnih podatkov, ravnanjem in varovanjem tajnih podatkov, zadovoljstva zaposlenih z izobraževanjem na področju tajnih podatkov, odnos zaposlenih do oseb, ki tajne podatke razkrivajo v javnosti, varnostna območja in načrti varovanja tajnih podatkov kot eden izmed elementov varnostne kulture),

- metoda analize in združevanja sekundarnih virov (analiziral bom podatke iz treh različnih projektov, ki so obravnavali izbrano tematiko s področja tajnih podatkov).

2 TEORETIČNI OKVIR

V tem poglavju bodo opredeljeni temeljni pojmi, kar je osnova nadaljnjega raziskovanja teme magistrskega dela. Pojmi varnost, tajnost, tajni podatek, dovoljenje za dostop do tajnega podatka, varnostni zadržek in varnostna kultura so morebiti na prvi pogled povsem nasprotujoči si. Ko pa jih podrobneje analiziramo, ugotovimo, da so povezani in zelo pomembni, če govorimo o sistemu varovanja tajnih podatkov.

Varnost ni povezana z le enim področjem človekovega delovanja, ampak je potreba po varnosti prisotna na vseh področjih človekovega delovanja in delovanja širše skupnosti, v katere se povezuje človek. To dimenzijo varnosti je izpostavil Anžič, ko pravi: *»Varnost se nanaša tako na družbo kot tudi na državo. Je torej človekovo zavestno prizadevanje za vzpostavitev takšne civilizacijske in kulturne kategorije, ki bo zajemalo vse vidike varnosti: politične, gospodarske, pravne, zdravstvene, socialne, kulturne in številne druge«* (Anžič 2002, 454)

»Zavestno prizadevanje za vzpostavitev stanja varnosti je civilizacijska in kulturna kategorija, ki zajema vse vidike varnosti, t. j. gospodarsko, socialno, kulturno, politično, pravno, ekološko, obrambno, itd., se pravi tiste pojavne oblike družbenega življenja, ki se štejejo za družbene vrednote. Oblike družbene organiziranosti zajemajo regionalno, nacionalno, mednarodno in svetovno varnost.« (Anžič 2002, 454).

Potreba po varnosti je prisotna pri človeku, odkar obstaja in funkcioniра kot razmišljajoče bitje. Sodobna varnostna paradigma obravnava varnost v okviru treh temeljnih konceptualnih okvirov kot individualno varnost, nacionalno varnost in mednarodno varnost. Če je individualna potreba po varnosti, ki jo čuti posameznik, zadovoljena, mu je omogočen kakovosten razvoj in obstoj. Individualna varnost je vedno relativna.

»Zagotavljanje nacionalne varnosti Republike Slovenije temelji na delovanju obrambnega sistema, sistema notranje varnosti ter sistema varstva pred naravnimi in drugimi nesrečami.« (RSNV 2010). Nacionalna varnost sicer res na eni strani zagotavlja varnost svojih državljanov ter odpravlja vire njihovega ogrožanja. Toda

hkrati preko svojih varnostnih organov, varnostnih in obveščevalnih služb tudi sama lahko postane vir ogrožanja individualne varnosti.

2.1 Temeljni pojmi

V nadaljevanju opredeljujem nekatere temeljne pojme, ki so pomembni za razumevanje celotnega magistrskega dela.

2.1.1. Varnost

Varnost je strukturna prvina obstoja in delovanja posameznika, družbe, države in mednarodne skupnosti. Kot takšna ima različne pojavne oblike, kot so: ideja, cilj, vrednota, potreba, interes, stanje, dejavnost, sistem itd. Potreba po varnostni obstaja, odkar obstaja človek kot razmišljujoče bitje. Človek je kot odgovor na oblike ogrožanja intenzivno razvijal zaščitna sredstva in svojo zavest. Z razvojem družbenega življenja, ko se je dvigala raven organiziranosti varnostne dejavnosti, je postopoma pomembno vlogo dobivala država (Brezovšek in Haček, 2006).

Do osemdesetih let prejšnjega stoletja je proučevanje varnosti temeljilo predvsem na realističnem in idealističnem pristopu. Realisti so, izhajajoč iz teorije moči, predvsem poudarjali pomen države in njene moči za zagotavljanje svoje varnosti. Če so varnost države razumeli kot cilj, so njeno moč postavljali kot instrument za doseg tega cilja. Idealisti pa so na drugi strani problem varnosti skušali rešiti z razpletom problema vojne. Zanje je ureditev konfliktov med državami pomenila rešitev problema nacionalne varnosti. V osemdesetih letih prejšnjega stoletja pa se področje preučevanja varnosti močno razširi, kar je predvsem sad praktičnih izkušenj in rezultat vpliva procesov globalizacije in internacionalizacije.

Nov koncept sodobne varnosti, ki je utemeljen na ideji o skupni varnosti (common security), je rezultat sinteze med logiko realistične in idealistične šole. Varnost je kompleksna in dinamična kategorija. Sodobne teorije o varnosti pa pojem varnost povezujejo s političnim, ekonomskim, sociološkim, okoljskim in seveda tudi z vojaškim aspektom (Baylis, Smith and Owens, 2008). Pojem varnosti se pojavlja skozi celotno

človeško zgodovino in je v osnovnem pomenu povezan predvsem z eksistencialnimi vprašanji (kakovost življenja, smrt) posameznika in njegovega odnosa z višjimi ravni družbenega organiziranja (država, meddržavna skupnost, svet kot celota). Prav zaradi te povezanosti je nujno celostno razumevanje pojma varnosti, vključujoč vse vidike človekovega obstoja in delovanja v družbi.

Potreba po varnosti je nekakšna nadgradnja nagona po samoohranitvi, zato je v tem kontekstu termin varnosti identičen terminom, kot so samoobramba, zaščita ali obramba. Za človeka je varnostna aktivnost vedno pomenila mnogo več kot preživetje; pomenila je eno temeljnih gibal človeškega razvoja, saj je človek kot odgovor na oblike ogrožanja intenzivno razvijal zaščitna sredstva in svojo zavest. V prvih oblikah človekovega socialnega življenja so področje varnosti regulirali predvsem običaji in določene moralne norme. Z razvojem družbenega življenja pa se je dvigal tudi nivo organiziranosti varnostne aktivnosti. Tako postopoma pride do transferja pravice ali potrebe po obrambi in varnosti v sfero države. Martin Edmonds (Jelušič, L. 1992 : 87) razlikuje dve vrsti pojmovanja varnosti.

Po Edmondsu je lahko varnost sredstvo ter tudi metoda zavarovanja družbenih vrednot. Pri tem je ključnega pomena zavarovanje ravnotežja med obema imperativoma, saj je v primeru nagnjenosti nacionalno varnostnega sistema k varnosti kot sredstvu problematično zagotavljanje legitimnosti oz. preprečevanje (vojaškega) posredovanja zunaj legitimnih meja. Nasprotno lahko model varnosti kot cilja privede v nevarnost predimenzioniranja nacionalno varnostnega sistema in zanemarjanja drugih pomembnih družbenih dejavnosti.

Varnost bi lahko opredelili tudi kot stanje, v katerem so presežene oblike ogrožanja. Takšno stanje je seveda lahko le teoretska predpostavka in o njem je mogoče govoriti le v relativnem smislu. To je torej tisto stanje, h kateremu je usmerjena obrambno-varnostna aktivnost posameznika in družbe.

2.1.2. Tajnost

Za pojem tajnost se v praksi kot sinonima uporabljata pojma skrivnost in zaupnost. Semantična razlaga po Slovarju slovenskega knjižnega jezika (SSKJ, spletna izdaja 2000) vse tri pojme v njihovem prvem pomenu razlikuje. Pojem tajnost pojmuje kot »značilnost tajnega«, kar bi lahko razumeli kot skrito pred javnostjo. Skritost razlaga kot »lastnost nečesa, kar je skrito«, tajni podatki pa že po svoji naravi morajo biti skriti.

Najpogosteje se kot sinonim za tajnost uporablja pojem skrivnost. V Slovarju slovenskega knjižnega jezika je skrivnost opredeljena kot nekaj, kar se ne da razumeti, dojeti, pojasniti. Kot je zapisal že Anžič, tajnost ni nekaj nerazumljivega, temveč gre za nekaj znanega. Po navadi vsebino tajnosti pozna ožek krog ljudi, ki tajnost skriva pred nepoklicanimi osebami, ki lahko vedo za obstoj tajnosti, vendar ne poznajo vsebine in jim je ta nedostopna.

2.1.3. Tajni podatek

Tajni podatek je »dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve, obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v istem zakonu, zavarovati pred nepoklicanimi osebami, in ki je v skladu z zakonom določeno in označeno za tajno« (ZTP-UPB2).

Za tajnega se vedno določi podatek, ki je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale oz. bi lahko nastale škodljive posledice za varnost države, njene politične ali gospodarske koristi.

Pri tajnih podatkih gre vedno za zelo občutljive podatke, ki morajo biti zaradi njihove občutljivosti označeni in varovani po najvišjih standardih. Ko se nek podatek ali informacija razglasi za tajne podatke, je potrebno za vsak tajen podatek zapisati pisno oceno škodljivosti razkritja tajnega podatke. V tej oceni se zapišejo razlogi, zakaj je bil podatek označen kot tajni podatek, s kakšno stopnjo tajnosti je bil označen in način, na kakšen način tajnemu podatku preneha stopnja tajnosti.

2.1.4. Dovoljenje za dostop do tajnih podatkov

Dovoljenje za dostop do tajnih podatkov ima v nacionalnem sistemu preverjanja za dostop do tajnih podatkov R Slovenije status odločbe. S to odločbo organ, pristojen za izvajanje varnostnega preverjanja, posamezniku podeli - dodeli pravico za dostopanje do tajnih podatkov v obsegu in trajanju, kot je to na dovoljenju za dostop zapisano.

Vsa delovna mesta v javni upravi, na katerih se predvideva dostop do nacionalnih tajnih podatkov, morajo biti določena. Zaposleni v javni upravi morajo biti o potrebi po pridobitvi dovoljenja za delo s tajnimi podatki seznanjeni s strani predpostavljenih. Da bi se postopek pridobivanja dovoljenja sploh lahko pričel, mora vsak zaposleni s tem soglašati. O tem mora podati pisno izjavo. Brez privolitve – pisne izjave – se postopek izdaje dovoljenj ne more pričeti. Če zaposleni ne želi podpisati soglasja za pridobitev dovoljenja, potem na tistem delovnem mestu ne more nadaljevati z delom in ga je potrebno premestiti na drugo delovno mesto. Na mesto, kjer ne potrebuje dovoljenja za dostop do tajnih podatkov.

S podpisom pisne izjave zaposleni soglaša, da lahko pristojen organ pri določenih organih in službah v R Sloveniji preveri njegove navedbe v vprašalniku.

Na podlagi zakona je določeno, da se dovoljenja izdajajo v ministrstvu, pristojnem za notranje zadeve, v ministrstvu, pristojnem za obrambo, in v Slovenski obveščevalno varnostni službi,³ za zaposlene v tej službi. Dovoljenje za dostop do tajnih podatkov stopnje zaupno velja deset let. Dovoljenje za dostop do tajnih podatkov velja pet let, enako velja dovoljenje za dostop do strogo tajnih podatkov.

2.1.5. Varnostni zadržek

³ Slovenska obveščevalno varnostna služba opravlja varnostno preverjanje in izdaja dovoljenja za dostop do tajnih podatkov samo za svoje zaposlene, medtem ko pa MO in MNZ opravljata preverjanje tudi za pogodbeno izvajalce del na ministrstvih ali preko javnih razpisov.

V postopku varnostnega preverjanja pristojni organ ugotavlja, ali je oseba zanesljiva, verodostojna, lojalna ter da ne obstaja nikakršen dvom v osebo, da bo varno obravnavala zaupane tajne podatke, ko ji bo podeljeno dovoljenje za dostop do tajnih podatkov. Če obstaja dvom, da oseba ne bo ravnala s tajnimi podatki, kot se od nje pričakuje, se osebi izda varnostni zadržek za dostop do tajnih podatkov. Organ mora svoj zadržek pisno utemeljiti. Zoper takšen varnostni zadržek ima oseba v R Sloveniji možnost pravnega varstva s pritožbo na Upravno sodišče R Slovenije.

Pri ugotavljanju varnostnega zadržka za dostop do tajnih podatkov organi pričakujejo, da bodo osebe v vprašalnik vpisale vse svoje podatke po resnici ter da se pri tem ne bodo lagali ali prikrivali določenih podatkov. Navajanje lažnih podatkov ali navajanje napačnih odgovorov pri razgovorih so eden izmed najpogostejših vzrokov za izdajo varnostnega zadržka. Če organ pri preverjanju ugotovi, da je kandidat za dovoljenje v svojem vprašalniku lagal, to pomeni avtomatsko zavrnitev izdaje dovoljenja ali t. i. obligatorni razlog za zavrnitev.

Med varnostne zadržke spadajo tudi pravnomočne obsodbe za kazniva dejanja, ki se preganjajo po uradni dolžnosti, dokončni disciplinski ukrepi zaradi kršitev s področja tajnih podatkov, zasvojenost z alkoholom, drogami ali drugimi oblikami zasvojenosti. Med tiste obvezne varnostne zadržke spadajo tudi članstvo ali sodelovanje v organizacijah ali skupinah, ki ogrožajo vitalne interese Republike Slovenije ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je Republika Slovenija.⁴

Organ, ki izvaja varnostno preverjanje, lahko ugotovi, da je oseba v vprašalniku navajala netočne ali le delno točne podatke. Da prikriva, da je v kazenskem postopku, da so zoper njega podane pravnomočne obtožnice ipd. Zato ima organ možnost, da tudi zaradi tega zavrne izdajo dovoljenja, ker ocenjuje, da oseba vzbuja dvom, da ni dovolj verodostojna, lojalna in zanesljiva, da bi imela dostop do tajnih podatkov in jih obravnavala. Ti zadržki so poznani kot ne obligatorni.

⁴ Problem tega varnostnega zadržka je v tem, da organizacije ali skupine, ki ogrožajo vitalne interese RS, sploh niso določene in organi, ki izvajajo varnostno preverjanje, ne vedo na kaj naj bodo pozorni pri preverjanju določenih oseb.

2.1.6. Varnostna kultura

Varnostno kulturo nekateri avtorji razumejo kot skupen nabor različnih idej, norm in praks, ki služijo za povečanje varnosti družbenih akterjev in držav. »Pojem varnosti se v zadnjih desetletjih v vedno večji meri obravnava tudi z vidika različnosti virov ogrožanja, pristopov k razumevanju varnosti; strokovna literatura s področja varnostne kulture se je nezadržno premaknila proti sociološkemu razumevanju varnosti. To razumevanje poudarja varnost kot občutek posameznika, da ima kognitivni nadzor nad kontekstom medsebojnega vplivanja – tovrstno razumevanje varnosti se ozko povezuje s konceptom zaupanja« (Giddens v Haacke, 2003: 4).

Študij (politično) vojaške kulture znotraj neke družbe zahteva podrobno, večslojno raziskovalno strategijo, ki mora vsebovati tri osnovne empirične naloge (Berger v Katzenstein, 1996: 328). Prvič, potrebno je raziskati izviren niz zgodovinskih izkušenj, ki opredeljujejo pogled neke družbe na vojsko, nacionalno varnost in na uporabo sile. Pri tem je potrebno posvetiti posebno pozornost še zlasti interpretaciji teh zgodovinskih izkušenj v različnih skupinah znotraj družbe.⁵ Drugič, potrebno je raziskati politični proces, skozi katerega se je neka varnostna politika oblikovala; ob tem je potrebno raziskati tudi načine, na katere so bile določene odločitve kasneje legitimirane. V tem smislu je nujno opredeliti ključne sestavine tako politično-vojaške kulture kot tudi varnostne politike v povezavi z *določenim časovnim obdobjem*. Tretjič, potrebno je raziskati razvoj tako politično-vojaške kulture kot tudi obrambnih politik skozi čas, pri tem pa opazovati, kako so se razvijale skozi različne zgodovinske dogodke.

V naslednji tabeli je prikazan spekter vojaške kulture po Dunivinu, katerega skrajnosti ponazarjata medsebojno povezana, a hkrati tudi različna modela. Prvi je tradicionalni model vojaške kulture, katerega temeljna značilnost je konservativizem: homogena, moška vojna sila, moške vrednote in norme ter izključevalne politike in zakoni.

⁵ Pod predpostavko seveda, da takšne različne interpretacije sploh obstajajo.

Tabela 2.1: Spekter vojaške kulture

Kulturna spremenljivka	Tradicionalni model	Razvojni model
Navade	Konservativizem, moralizem	Konservativizem, moralizem
Enkulturacija	Boj, moški bojevniki	Boj, moški bojevniki
Zakoni, politike	Izključitev	Vključitev
Struktura vojne sile	Homogenost	Heterogenost
Vedenje	Separatizem	Egalitarizem
Večinske/manjšinske interakcije	Sovražnost	Toleranca

(Vir: Dunivin, 1994 : 535)

Na drugem koncu spektra je razvojni model, katerega temeljna značilnost je egalitarizem: družbeno heterogena vojna sila, mnogovrstne vrednote in norme ter inkluzivne politike in zakoni. Seveda vojaška kultura nikoli popolnoma ne ustreza enemu ali drugemu modelu; vsekakor pa razvojni model opozarja na pojavljajoče se trende znotraj vojaške kulture. Kot teoretični konstrukti so modeli seveda odprti za znanstveno razpravo; tako nekateri trdijo, da je vojska preveč tolerantna do različnosti in inkluzivnih politik, drugi pa trdijo, da vojaška kultura ostaja družbeno konservativna kultura, ki se upira večini družbenih sprememb (Dunivin, K.O. 1994 : 534).

Močna in spoštovana vojska predstavlja soliden družbeni temelj za promocijo obrambne kulture, ki skuša usmerjati državljane, da bi se čimbolj identificirali s cilji svoje države. Močna obrambna kultura služi tudi kot osrednja točka za spodbujanje oz. povečevanje nacionalne kohezivnosti (Ji You, 2004, : 248). Tovrstna obrambna kultura služi kot temelj za konstrukcijo nacionalnega ponosa, saj skuša promovirati osnovno interpretacijo nacionalne zgodovine, tradicij in samopodobe (Whiting, 1989, : 15). V mnogih družbah je še vedno zaslediti tudi nacionalen konsenz, ki pravi, da brez močne vojske ni mogoče doseči nacionalne suverenosti (Ji You, 2004, : 251).

Nacionalna varnost Republike Slovenije se zagotavlja z vsemi zmožnostmi države, ki je zato, da lahko uspešno izkoristi svoje potenciale, organizirala sistem nacionalne varnosti, ki je sestavljen iz treh podsistemov, in sicer obrambnega podsistema, podsistema notranje varnosti in podsistema varstva pred naravnimi in drugimi nesrečami, ki jih bo Republika Slovenija tudi v bodoče nadgrajevala, dopolnjevala in povečevala njihovo učinkovitost.

3 SISTEM VAROVANJA NACIONALNIH TAJNIH PODATKOV V SLOVENIJI

Zakon o državni upravi določa, da je uprava dolžna zagotavljati javnost svojega dela, upošteva omejitve, ki izhajajo iz predpisov, ki urejajo varovanje osebnih in tajnih podatkov ter drugih predpisov. Vprašanja javnosti dela in dostopnosti do podatkov in informacij državnih organov, zlasti državnih upravnih organov, so neločljivo povezana z vprašanji ureditve določanja in varovanja tajnih podatkov in informacij. Pravna ureditev teh vprašanj mora v demokratični državi upoštevati vsa tista temeljna pravna načela, na katerih takšne države temeljijo, zlasti pa mora spoštovati in omogočati uveljavljanje vseh temeljnih človekovih pravic in svoboščin, ki so s tem povezane. Med temi načeli je pri tem še posebej pomembna zahteva po transparentnosti delovanja državne uprave.

Transparentnost delovanja nosilcev vseh vej državne oblasti, zlasti transparentnost delovanja državne uprave, njenih dejanj, postopkov, ukrepov in odločitev, s katerimi se tako ali drugače vpliva ali posega v življenje in delo ljudi ter njihovih organizacij, je pomemben atribut sleherne moderne demokratične države (Debelak in Rakočević, 2002, : 183).

»Javnost dela organov oblasti in pravica vsakogar, da od teh organov dobi podatke in informacije z njihovega delovnega področja, je v demokratičnih družbah splošno sprejeto načelo, obenem je tudi pogoj in zagotovilo normalnega delovanja teh organov, ki brez zaupanja, sodelovanja in podpore javnosti praktično ne morejo biti učinkoviti« (Antončič, M. 2003, : 88).

Razumljivo je, da načelo javnosti ne more veljati neomejeno. Načelo javnosti in odprtosti ter dostopnosti do podatkov in informacij državnih organov ne more pomeniti, da lahko vsakdo v vsakem trenutku zahteva katerikoli podatek od nekega državnega organa. Stvar pravnega reda vsake države je, da uredi ta vprašanja in določi oblike in načine uresničevanja teh načel v praksi. Demokratična načela delovanja moderne države in njenih institucij zahtevajo, da so državljani o vseh aktivnostih državnih organov obveščeni. To je njihova ustavna pravica, obenem pa mora biti določena tudi

kot pravna obveznost organov državne uprave kakor tudi drugih državnih organov in institucij. Razumljivo je, da načelo javnosti dela in dostopnosti do podatkov in informacij državnih organov ne more biti brez omejitev. Načini in oblike uresničevanja javnosti dela so v veliki meri odvisne od vrste državnega organa, njegovega položaja, značilnosti njegovih nalog in vsebine ter narave njegovega dela.

Dejstvo je, da je treba v vsaki državi dostop do določenih podatkov in informacij omejiti zaradi zaščite državnih interesov. Takšni podatki in informacije se določijo za tajne. Določitev nekaterih podatkov in informacij za tajne, kar ima praviloma za posledico poseben režim njihovega varovanja, predvsem omejitev njihove splošne dostopnosti na določen, bolj ali manj ozek krog oseb, je seveda v nasprotju z načelom javnosti. Državni organi morajo komunicirati z javnostjo, jo obveščati in seznanjati s številnimi državnimi zadevami, vprašanji in ukrepi. Svoboda javnega obveščanja je ustavno zajamčena človekova svoboda, s katero je posamezniku omogočeno, da enakopravno z drugimi sodeluje pri upravljanju javnih zadev. Iz navedene ustavne določbe izhaja dolžnost državnih organov, da v okviru z zakonom določenih pogojev in omejitev vsakomur zagotovijo prost dostop do informacij, do katerih je upravičen. Ustava pri tem postavlja poseben pogoj, in sicer izkazan pravni interes posameznika do določene informacije (Debelak in Rakočevič, 2002, : 183–186).

Zakon o medijih v pravi: *»Državni organi, organi lokalnih skupnosti, posamezniki, ki opravljajo javne funkcije, javni zavodi in javna podjetja ter druge pravne ali fizične osebe, ki opravljajo javno službo, morajo dajati resnične, popolne in pravočasne informacije o vprašanjih s svojega delovnega področja tudi prek medijev.«*⁶

⁶ Zakon o medijih. (ZMed-UPB1).

Javne osebe lahko odrečejo dajanje informacij le v naslednjih primerih:

- če so zahtevane informacije na predpisan način določene za državno, vojaško, uradno ali poslovno skrivnost,
- če bi to pomenilo kršitev tajnosti osebnih podatkov v skladu z zakonom, razen če se z njihovo objavo lahko prepreči hujše kaznivo dejanje,
- neposredna nevarnost za življenje ljudi in njihovo premoženje,
- če bi to škodilo sodnemu ali pred kazenskem postopku.

Določitev določenih podatkov in informacij z delovnega področja državnih organov za tajne, s čimer se jih podredi posebnemu režimu varovanja, s katerim se odtegnejo nepooblaščenim osebam in seveda javnosti v celoti, je v nasprotju z načelom javnosti dela. Razrešitev tega nasprotja, ki je prisotno v vseh demokratičnih državah, je prvovrstno politično in pravno vprašanje. Določitev podatkov in informacij za tajne je namreč lahko najenostavnejša možnost in način omejevanja javnosti dela državnih organov, ki se lahko zlorablja za prikrivanje različnih nepravilnosti ali celo nezakonitosti v teh organih.

»Na drugi strani ohlapen odnos do instituta tajnosti podatkov v državnih organih lahko povzroči, da prihajajo v javnost podatki in informacije, katerih razkritje lahko ogrozi interese in koristi države«. (Antončič M. 2003, : 88).

Podatek, ki mu je bila tajnost določena zato, da bi se prikrilo storjeno kaznivo dejanje, prekoračitev ali zloraba pooblastil ali prikrilo kakšno drugo nezakonito dejanje ali ravnanje, ni tajen (ZTP-UPB2). Vsak posameznik, ne glede na to, ali je državljan ali tujec, ima pravico, da zahteva katerokoli informacijo, ki se nahaja v spisih državnih organov, razen tistih, ki jih je zakon izrecno izvzel iz splošne dostopnosti (Debelak in Rakočević 2002, :187).

Za tajnega se lahko določi podatek, ki je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale ali bi očitno lahko nastale škodljive posledice za varnost države ali za njene politične ali gospodarske koristi in se nanaša na:

- javno varnost,
- obrambo,
- zunanje zadeve,
- obveščevalno in varnostno dejavnost državnih organov RS,
- sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije.

V večini demokratičnih držav so razlogi, zaradi katerih se lahko omeji javnost dela državnih organov in dostopnost do njihovih podatkov, podobni. Največkrat se ti razlogi nanašajo na varnost države, obrambo in obrambne sile države, monetarno stabilnost države, mednarodne odnose, na različne interese in koristi določenih državnih organov, institucij, služb ali posameznikov. Tako se pri pravnem urejanju teh vprašanj soočamo z zapleteno kolizijo interesov in pravic.

Na eni strani gre za interes javnosti in posameznikov po transparentnosti oblasti in oblastnega delovanja ter pravica državljana, da dobi informacijo javnega značaja. Na drugi strani pa je pravica države, da zavaruje pomembne državne interese in koristi (Rakočević 2003, : 5). Določanje tajnih podatkov je dejanje ali postopek, s katerim se podatek oceni za tajnega in se mu določi stopnja in rok tajnosti.

Določanje in varovanje tajnih podatkov v bistvu pomeni, da se prepreči dostop do nekaterih podatkov in informacij nepooblaščenim osebam in javnosti zato, da se zavarujejo določeni državni interesi. Določene podatke in informacije se podvrže posebnemu pravnemu režimu, s katerim se zaradi legitimnih interesov države omeji njihova splošna dostopnost in uporaba. Tajen podatek ni neznan podatek, ampak je znan podatek, znana informacija in znano dejstvo, ki iz določenih zakonitih razlogov ne sme postati javen, ampak je lahko znan oziroma dostopen samo določenemu krogu oseb. Tak podatek, informacija ali dejstvo je lahko poznan samo določenemu krogu oseb, ki mora biti po možnosti čim bolj natančno določen in dolžan spoštovati pravni

režim, ki je glede njegovega varovanja predpisan. Morebitne kršitve predpisanih pravil ravnanja potegnejo za seboj uveljavitev različnih vrst odgovornosti: kazensko, disciplinsko, odškodninsko, politično z vsemi posledicami, ki so predvidene v zakonu.

V Slovarju slovenskega knjižnega jezika je tajnost (državna, poslovna, službena, vojaška) opredeljena kot vse »*kar je tajno*«, pojem - pridevnik »*tajen*« se opisuje kot nekaj, s čimer se javnost, ljudje ne morejo seznaniti oziroma kot nekaj, za kar ve le ozek krog ljudi (Debelak in Rakočevič 2002, : 189–190).

Tajnost v smislu varovanja znanega in za širšo javnost nedostopnega ne smemo enačiti s pojmom skrivnost. Tajnost ni nekaj neznanega, temveč obratno, gre za znano stvar, ki je njen posestnik ne sme ali noče narediti dostopno širši javnosti. Tajnost torej pomeni obstoj znanih dejstev o družbenih ali naravnih pojavih, ki so posameznikom zaupane v uporabo in varovanje in jih ti zaradi obstoja različnih, velikokrat konfliktnih interesov, na zavesten, organiziran in formaliziran način skrivajo pred javnostjo (Anžič 1997, :156).

Za varovanje tajnih podatkov je gotovo ključnega pomena opredelitev, kateri podatek se sploh lahko šteje za taje. Tajni podatek je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v tem zakonu, zavarovati pred nepoklicanimi osebami in ki je v skladu z zakonom določeno in označeno za tajno .

3.1 Stopnje tajnosti v nacionalnem sistemu varovanja tajnih podatkov

V Republiki Sloveniji smo z Zakonom o tajnih podatkih iz leta 2001 dobili naslednje stopnje tajnosti:

STROGO TAJNO; s takšno oznako se določijo tisti tajni podatki, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese Republike Slovenije ali jim nepopravljivo škodovalo,

TAJNO; kot tajne se določijo tisti tajni podatki, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo varnosti ali interesom Republike Slovenije,

ZAUPNO; s to oznako se označijo tisti tajni podatki, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom Republike Slovenije,

INTERNO; s to oznako pa se označijo tisti tajni podatki, katerih razkritje nepoklicani osebi bi lahko škodovalo delovanju ali izvajanju nalog organa (ZTP, 13. člen).

Pri določanju slovenskih oznak stopenj tajnosti se je zgledovalo po oznakah, ki so takrat že veljale v zvezi NATO. Republika Slovenija si je zaradi svoje nacionalne varnosti in zagotavljanja širše varnosti močno prizadevala pridružiti že leta 1988 na vrhunskem zasedanju v Madridu. Ker nam je zmanjkalo nekaj osnovnih, sistemskih zakonov, kot npr. zakon o tajnih podatkih, smo to svojo »pomanjkljivost« do naslednje večje širitve NATO v letu 2003 ustrezno popravili.

3.1.1 Stopnje tajnosti v NATO

Določitev tajnosti podatkov kažejo na občutljivost informacij NATO in se uporabljajo zato, da opomnijo prejemnika, da zagotovi varovanje informacije glede na stopnjo škode, ki bi se lahko zgodila ob nepooblaščenem dostopu ali razkritju. NATO označbe tajnosti in njihovi pomeni so naslednji:

Zveza NATO ima na področju varovanja in označevanja različnih stopenj tajnosti bogato tradicijo. Že leta 1949 je namreč sprejela prvi krovni dokument, Varnostna politika zveze NATO, ki nosi oznako CM (2002)-49.

To osnovno varnostno politiko zveze NATO dopolnjujejo različne direktive, ki podrobneje urejajo področja na:

AC/35-D/2000	Directive on Personal Security,
AC/35-D/2001	Directive on Physical Security,
AC/35-D/2002	Directive on Security of Information,

AC/35-D/2003	Directive on Industrial Security,
AC/35-D/2004	Primary Directive on INFOSEC,
AC/35-D/2005	INFOSEC Management Directive for CIS. ⁷

COSMIC TOP SECRET (CTS) - nepooblaščno razkritje bi povzročilo izjemno veliko škodo organizaciji NATO,

NATO SECRET (NS) - nepooblaščno razkritje bi povzročilo veliko škodo organizaciji NATO,

NATO CONFIDENTIAL (NC) - nepooblaščno razkritje bi bilo škodljivo za NATO,

NATO RESTRICTED (NR) - nepooblaščno razkritje bi lahko bilo škodljivo za interese NATO.

Štiri stopnje tajnosti ter še dve posebni oznaki za omejevanje dostopa (t. i. »COSMIC« in »NATO« zasledimo v ureditvi zveze NATO in tudi v nekaterih državah EU.

Poleg štirih osnovnih stopenj tajnosti v zvezi NATO najdemo še dodatne oznake, ki pomenijo še večjo stopnjo varovanja glede na področje, s katerega podatki prihajajo:

- **ATOMAL** (podatki in informacije, ki se nanašajo na področje jedrskega orožja),
- **BOHEMIA** (podatki in informacije, ki so bile pridobljene s pomočjo SIGINT-a),
- **CRYPTO** (podatki in informacije, ki se dotikajo kriptiranja informacij in posredovanja le-teh podatkov uporabnikom).

Članice NATO ter civilni in vojaški organi NATO morajo sprejeti ukrepe za zavarovanje informacij, izdelanih ali dostavljenih NATO v obsegu, ki ustreza označeni stopnji. Ukrepi civilnih in vojaških organov NATO morajo predvsem vsebovati:

a) omejitev števila položajev s pooblastilom za določanje stopnje tajnosti;

⁷ V našem pravnem redu imajo te direktive status uredb in podpirajo osnovni dokument NATO CM (2002)-49. Tado dokument je NATO sprejel že leta 1949.

b) omejitev informacij, ki jim mora biti določena stopnja tajnosti, spodbujati pisanje občutljivih informacij v priloge teksta tako, da je glavni tekst lahko razširjan bolj na široko ter z manj strogimi varnostnimi ukrepi.

3.1.2 Spreminjanje stopenj tajnosti v NATO

Stopnjo tajnosti NATO tajnih podatkov lahko spreminja samo originator ali pa se spremeni, vendar samo z njegovim soglasjem. V primeru, ko originatorja ni mogoče ugotoviti, mora organizacija naslednica ali višji organ prevzeti njegove odgovornosti. V takšnih primerih se lahko izvedejo spremembe označitve samo po posvetovanju s članico NATO, civilnim ali vojaškim organom NATO, ki so zainteresirani za obravnavano vsebino.

Originator oziroma organizacija naslednica ali višji organ, kadar originatorja ni mogoče ugotoviti, so odgovorni za to, da so prejemniki obveščeni takoj, ko je do spremembe tajnosti prišlo.

3.1.3 Stopnje tajnosti v EU

Označevanje stopenj tajnosti v EU je podoben kot v NATO. Nekateri strokovnjaki s tega področja pravijo, da je EU enostavno prekopirala stopnje tajnosti iz NATO ter nekoliko modificirala stopnjo ogroženosti, kakšna škoda bi nastala z razkritjem teh tajnih podatkov. Stopnje razvrstitve tajnosti podatkov v evropskem pravu so naslednje:

EU TOP SECRET: ta stopnja tajnosti se uporablja samo za podatke in gradivo, katerih razkritje nepooblaščenim osebam bi lahko imelo izjemno težke posledice za bistvene interese EU ali ene ali več njenih držav članic,

SECRET EU: ta stopnja tajnosti se uporablja samo za podatke in gradivo, katerih razkritje nepooblaščenim osebam bi lahko resno škodovalo bistvenim interesom EU ali ene ali več njenih držav članic,

CONFIDENTIEL EU: ta stopnja tajnosti se uporablja za podatke in gradivo, katerih razkritje nepooblaščenim osebam bi lahko škodovalo bistvenim interesom EU ali ene ali več njenih držav članic,

RESTREINT EU: ta stopnja tajnosti se uporablja za podatke in gradivo, katerih razkritje nepooblaščenim osebam bi lahko bilo škodljivo za interese EU ali ene ali več njenih držav članic.

3.2. Preverjanje in dostopanje do tajnih podatkov v nekaterih izbranih državah Evropske unije

V sodobnih demokratičnih državah v Evropi pri dostopanju do tajnih podatkov velja načelo sorazmernosti in preverjenosti. Oseba lahko dostopa le do tistih tajnih podatkov, do katerih mora dostopati zaradi narave dela, ki ga opravlja. Pri preverjanju za dostop do tajnih podatkov gre za natančno določen postopek, ki ga izvedejo pristojni organi, s katerim se ugotavlja verodostojnost, lojalnost in zanesljivost osebe za varno obravnavanje tajnih podatkov.

»V državah članicah EU in Zveze NATO najdemo toliko različnih načinov urejanja in organiziranja sistema varstva tajnih podatkov, kolikor je članic, vendar pa vsi ti temeljijo na enotnih izhodiščih. Izhodišča pri pripravi nacionalnih zakonodaj so jim bili standardi NATO, ki bistveno ne odstopajo od standardov EU.« (Dimitrovski 2016, : 59).

Za primerjavo sem izbral Nemčijo, Nizozemsko in Švedsko. Gre za dva različna sistema, saj je Nemčija svoj sistem izgradila popolnoma na novo, medtem ko sta kraljevini Švedska in Nizozemska na tem področju imeli daljšo tradicijo. Ko smo v Sloveniji pričeli izgrajevati svoj sistem varovanja tajnih podatkov, je po moji oceni veliko rešitev prenesenih ravno iz nemškega sistema dostopanja in varovanja tajnih podatkov.

3.2.1 Nemčija

Varnostno preverjanje za dostop do tajnih podatkov se izvaja v naslednjih organih:

- Zvezni Urad za varstvo in zaščito (referat IS 4)
- Vojaška Protiobveščevalna služba – MAD
- Zvezna obveščevalna služba – BND

Varnostnemu preverjanju se lahko podvržejo osebe, ki so stare najmanj 16 let in ki bodo imele v okviru svojega dela dostop do tajnih podatkov. Oseba se lahko preveri po njenem predhodno podpisanem soglasju za varnostno preverjanje in ko oseba izpolni varnostni vprašalnik.

»V primeru, da so rezultati varnostnega preverjanja negativni in se osebi ne izda dovoljenje za dostop do tajnih podatkov, se oseba lahko pisno izjasni o izsledkih varnostnega preverjanja. Na zaslišanje lahko pride s svojim odvetnikom. Enako se oseba lahko pisno izjasni v primeru, da bi bil varnostni zadržek vezan na njegovega zakonca ali izven zakonskega partnerja.

Oblike varnostnega preverjanja:

a) enostavno oz. osnovno varnostno preverjanje – osebe se preverijo do stopnje zaupno (pri tem preverjanju gre za to, da se preverijo podatki, navedeni v osnovnem varnostnem vprašalniku v različnih evidencah državnih organov),

b) razširjeno varnostno preverjanje – osebe se preverijo do stopnje tajno (preverijo se navedbe v varnostnem vprašalniku, enako kot pri osnovnem varnostnem preverjanju, zbirajo se podatki iz policijskih postaj na območju, kjer je posameznik živel vsaj 5 let, preveri se zakonec in izvenzakonski partner, seveda ob njegovem soglasju),

c) razširjeno varnostno preverjanje z varnostnim poizvedovanjem – do stopnje strogo tajno (preverjanje je enako kot za stopnjo tajno, opravijo se še razgovori s tremi osebami, ki jih je oseba navedla v svojem vprašalniku).

Organ, ki izvede varnostno preverjanje, o svojih izsledkih obvesti organ, ki je za osebo predlagal varnostno preverjanje. Če iz ugotovitev varnostnega preverjanja izhajajo varnostni zadržki, jih organ, pristojen za varnostno preverjanje, podrobneje pisno pojasni. Predlagatelj varnostnega preverjanja na podlagi tega oceni, ali varnostni zadržek pomeni varnostno tveganje, zaradi katerega bo osebi zavrnil dostop do tajnih podatkov in s tem možnost zaposlitve v organu. V vsakem primeru pa ima varnostni interes prednost pred vsemi interesi.

Varnostni vprašalnik se osebi ponovno pošlje v izpolnjevanje vsakih 5 let. Za osebe, ki imajo dovoljenje za dostop do strogo tajnih podatkov, se varnostno preverjanje opravi vsakih deset let. Za imetnike dovoljenj tajno ali zaupno pa se varnostno preverjanje opravi le v primeru, če se ugotovijo podatki, na podlagi katerih je ponovno potrebno oceniti varnostno tveganje za organ, v kateri oseba dela.«⁸

3.2.2 Nizozemska

Varnostno preverjanje se opravlja v dveh organih:

- Civilna obveščevalna in varnostna služba (AIVD),
- Vojaška obveščevalna in varnostna služba (DISS).

Vojaška obveščevalna in varnostna služba izvaja varnostno preverjanje za vsa varnostno občutljiva delovna mesta in za vsa delovna mesta, na katerih imajo osebe dostop do podatkov o vojaški opremi in sistemih. Za vsa ostala delovna mesta v državi pa varnostno preverjanje izvaja civilna služba.

Vsa delovna mesta, na katerih delavci dostopajo do tajnih podatkov, se delijo na tri skupine:

- Skupina delovnih mest z oznako A, dostop do strogo tajnih podatkov,
- Skupina delovnih mest z oznako B, dostop do tajnih podatkov,

⁸ V predlogu sprememb zakona o spremembah in dopolnitvah zakona o tajnih podatkih (ZTP-A), nujni postopek z dne 18. 9. 2003, je predlagana sprememba glede preverjanja oseb za katere se ugotovi varnostni zadržek in imajo veljavno dovoljenje za dostop do zaupno ali tajno.

- Skupina delovnih mest z oznako C, dostop do zaupnih tajnih podatkov.

Delodajalec od delavca prejme izpolnjen vprašalnik glede na delovno mesto, na katerem bo delavec dostopal do tajnih podatkov. Vprašalnik mora biti v zaprti ovojnici. Skupaj z vprašalnikom mora delavec predložiti še kopijo osebnega dokumenta. Če pa gre za preverjanje do strogo tajnih podatkov še svojo fotografijo. Služba, ki izvaja preverjanje, mora svoje delo končati v osmih tednih.

Pred zaposlitvijo na takšnem delovnem mestu, kjer bo delavec potreboval dostop do tajnih podatkov, mora delodajalec delavcu sporočiti:

- da ga bo varnostno preverila obveščevalno varnostna služba,
- delodajalec mu pove, do kakšnih tajnih podatkov bo na tistem delovnem mestu dostopal,
- da se pri varnostnem preverjanju zbirajo tudi informacije, ki so pomembne iz varnostnega vidika ali vidika varovanja države,
- seznaniti ga z okoliščinami, zaradi katerih se mu prošnja za izdajo dovoljenja lahko zavrne, ter da ima možnost, da se zoper zavrnitev izdaje dovoljenja, lahko pritoži (Vir: lasten).

3.2.3 Švedska

Varnostno preverjanje za dostop do tajnih podatkov se opravlja v :

- civilna varnostna služba,
- vojaška varnostna služba.

Civilna varnostna služba je odgovorna za izvedbo varnostnega preverjanja in za preiskovanje vseh kaznivih dejanj, ki bi lahko imele vpliv na nacionalno varnost ali pa bi morebiti šlo za teroristično dejanje. Civilna varnostna služba je odgovorna za vse tujce, ki prebivajo ali vstopajo na Švedsko, ter za mednarodne organizacije, ki delujejo na Švedskem.

Vojaška varnostna služba je na drugi strani odgovorna za izvedbo varnostnega preverjanja v vseh primerih, ko osebe pridejo v stik z obrambnimi ali vojaškimi tajnimi podatki. Enako je ta služba odgovorna za vse vidike varnosti v sprejetih in podpisanih bilateralnih varnostnih sporazumih.

Na Švedskem ne poznajo enotne oblike prepisanih varnostnih vprašalnikov za izvedbo varnostnega preverjanja. Ob razgovoru z osebo se izpolni neke vrste vprašalnik. Seveda ta razgovor opravi oseba iz ene ali druge varnostne službe.

Po švedski ustavi imajo vsi državljani ustavno pravico, da lahko dostopajo do vseh službenih podatkov ali dokumentov. Javni dostop do uradnih dokumentov je omejen s posebnim zakonom. Ta zakon pa omejuje dostop do tajnih podatkov.

3.2.4 Vloga in pomen nacionalnega varnostnega organa ter sistem

dostopanja do tajnih podatkov

Sodobna demokratična država mora poskrbeti za učinkovit sistem preverjanja oseb za dostopanje do nacionalnih oz. državnih tajnosti. *»Za proces varovanja tajnih podatkov v sodobni državi morajo skrbeti odgovorne posebne institucije: nacionalni organ za varovanje tajnih podatkov, ki ima nadresorni pomen, in pa posamezni resorni organi, ki skrbijo za preverjanje in varovanje na svojem področju.«*(Prezelj, Tarman 2015, :692)

Nacionalni varnostni organ v R Sloveniji ali angl. National Security Authority (NSA) je formalno pričel s svojim delom na podlagi sklepa Vlade RS o ustanovitvi Urada Vlade R Slovenije za varovanje tajnih podatkov leta 2002.⁹ Njegova prva naloga je bila priprava osnutka zakona o tajnih podatkih, ki ga je pripravila medresorska delovna skupina.

⁹ Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov, pomeni formalno pričetek dela nacionalnega varnostnega organa v R Sloveniji.

Urad Vlade R Slovenije za varovanje tajnih podatkov (v nadaljevanju UVTP) kot nacionalni varnostni organ spremlja stanje na področju varovanja tajnih podatkov v R Sloveniji, usmerja in usklajuje delo organov, ki izvajajo varnostno preverjanje v ministrstvih, ter skrbi za pripravo predpisov s področja tajnih podatkov, izdaja dovoljenja za dostop do tajnih podatkov NATO in EU ter izvaja osnovno in dodatno usposabljanje. Glavna naloga UVTP-ja je trenutno izdaja dovoljenj NATO in EU na podlagi zahtevkov organov, ki izvajajo preverjanje za dostop do nacionalnih tajnih podatkov. Po trenutno veljavni zakonodaji to izvajajo v Ministrstvu za notranje zadeve, v Ministrstvu za obrambo in v Slovenski obveščevalno varnostni službi.

Vloga nacionalnega varnostnega organa v Sloveniji je v primerjavi s sosednjimi državami ter glede na naloge in pristojnosti nam primerljivih nacionalnih varnostnih organov, po mojem mnenju, povsem neprimerna in celo podcenjujoča. Urad se že dobrih 10 let bori s pomanjkanjem kadrov, financ in povsem neprimernih prostorov. Poleg tega je organizacijsko neprimerno, da je Urad umeščen v okviru Generalnega sekretariata Vlade R Slovenije. Trenutno se delo Urada omejuje na izdajo dovoljenj za NATO in EU in je povsem primerljivo manjšemu poštenu uradu. Na izdajo dovoljenja za dostop do tajnih podatkov NATO je tako potrebno čakati tudi do enega meseca.

Sistem dostopanja in preverjanja do nacionalnih ali tujih tajnih podatkov je v R Sloveniji povsem primerljiv z večino držav v Evropi. So manjše razlike, ki pa bistveno ne odstopajo od države do države.

Naš sistem je, kot sem že omenil, zelo dobra kopija nemškega sistema. Ena od bistvenih razlik je v tem, da v Nemčiji izvedejo varnostno preverjanje za dostop do strogo tajnih podatkov po 10 letih, medtem ko pri nas takšno dovoljenje velja samo 5 let. V R Sloveniji imamo v našem zakonu še eno specifičnost. Vsa opravila pri izvajanju varnostnega preverjanja za dostop do tajnih podatkov izvajamo na podlagi določil Zakona o splošnem upravnem postopku. Na ta način se pri varnostnem preverjanju, kjer gre za velik poseg v človekove pravice, zagotavlja maksimalno spoštovanje pravic osebe, ki se podvrže varnostnemu preverjanju in prosi za izdajo dovoljenja za dostop do tajnih podatkov.

V Sloveniji lahko oseba vpogleda v zadevo, kjer ima organ zbrane vse podatke o osebi, in tudi odgovore drugih organov, kjer se je oseba preverjala. Ravno tako se oseba na izdan varnostni zadržek za izdajo dovoljenja, lahko pritoži na Upravno sodišče R Slovenije. V Nemčiji je pri njihovem preverjanju ocena organa, ki je izvedel varnostno preverjanje, dokončna in na to odločitev, kjer igra pomembno vlogo morebitno ogrožanje nacionalnih interesov, ni mogoča pritožba.

3.3 Zakon o tajnih podatkih

»Zakon o tajnih podatkih določa skupne osnove enotnega sistema določanja, varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov Republike Slovenije, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države ter prenehanja tajnosti takšnih podatkov. Po tem zakonu se morajo ravnati državni organi, organi lokalnih skupnosti, nosilci javnih pooblastil ter drugi organi, gospodarske družbe in organizacije, ki pri izvajanju zakonsko določenih nalog pridobijo ali razpolagajo s tajnimi podatki ter posamezniki v teh organih. Vsak, ki mu je bil zaupan tajni podatek ali ki se je seznanil z vsebino tajnega podatka, je odgovoren za njegovo varovanje in ohranitev njegove tajnosti«. (ZTP, člen 1.)

Podatek določi za tajnega pooblaščen oseba, ki je:

- predstojnik organa, izvoljeni ali imenovani funkcionarji organa, ki so za določanje in posredovanje tajnih podatkov pooblaščen z zakonom oziroma s predpisom, izdanim na podlagi zakona ali jih je za to pisno pooblastil predstojnik in
- osebe, zaposlene v organu, ki jih je za to pisno pooblastil predstojnik tega organa.

»Stopnjo strogo tajno lahko določijo samo predsednik republike, predsednik državnega zbora, predsednik vlade, ministri in predstojniki organov v sestavi ministrstev, določeni

vojaški poveljniki, predstojniki vladnih služb, ki so neposredno odgovorni predsedniku vlade oziroma osebe, ki jih nadomeščajo» (ZTP, 10. člen).

V skladu z zakonom nobena druga oseba ne more določiti nekega podatka za tajnega. In če bi tajni podatek določila nepooblaščen oseba, ta podatek ne more veljati kot tajen. Razkritje takšnega podatka praviloma ne bi smelo imeti nobenih pravnih posledic. Splošna dolžnost vseh drugih oseb v javnih organih v zvezi z določanjem tajnih podatkov je, da v okviru svojih delovnih nalog in pristojnosti presojuje varnostni pomen podatkov in predlagajo pooblaščenim osebam, da določijo podatke za tajne, če ocenjujejo to za potrebno. Podatek lahko za tajnega v skladu z zakonom določi samo pooblaščen oseba.

»Pooblaščen oseba določi stopnjo tajnosti podatka ob njegovem nastanku oziroma ob začetku izvajanja naloge organa, katere rezultat bo tajen podatek« (ZTP, 11. člen).

»Podatek se določi za tajnega tako, da se mu določi stopnja tajnosti v skladu z zakonom. Pooblaščen oseba mora presoditi ali so izpolnjeni razlogi, ki jih določa zakon za določitev tajnosti ter oceniti varnostni pomen podatka glede na posledice, ki bi jih povzročilo njegovo razkritje nepoklicani osebi. Na podlagi takšne ocene se določi tudi stopnja tajnosti, in sicer najnižja, ki še zagotavlja varnostnemu pomenu podatka ustrezno varovanje. Ocena mora biti pisna, kar pomeni, da jo mora pooblaščen oseba obrazložiti.« (ZTP)

Podatek, ki se določi za tajnega, ima takšno naravo samo določen čas. To pomeni, da tudi tajni podatki po preteku določenega časa postanejo dostopni javnosti. Rok trajnosti podatka je seveda odvisen od konkretne vsebine tajnega podatka in od obstoja razlogov, zaradi katerih je dobil takšen značaj. Zato je treba hkrati z določitvijo nekega podatka za tajnega določiti tudi čas oziroma rok, ko njegova tajnost preneha. *»Prenehanje tajnosti podatka pomeni zakonito spremembo tajnega podatka v podatek, ki je splošno dostopen« (ZTP, 2. člen).*

Tajni podatek oziroma vsak dokument, ki vsebuje tajne podatke, mora biti označen na naslednji način:

- s stopnjo tajnosti,
- z načinom prenehanja tajnosti,
- s podatki o pooblaščenih osebah,
- s podatki o organu, če to že sicer ni razvidno.

Enako pomembno je, da se označi tudi način prenehanja tajnega podatka. Pri tem imamo naslednje možnosti označitve:

- na določen datum,
- z nastopom določenega dogodka,
- s potekom določenega časa,
- s preklicem tajnosti (ZTP, 18. člen).

Vsak tajeen podatek oziroma vsak dokument, ki vsebuje tajne podatke, mora biti označen kot tajeen. Nobenega dvoma ni, da so vsebinski razlogi ključni za zakonitost določitve tajnosti nekega podatka. Vendar pa lahko te razloge zakonito oceni samo pooblaščen oseb. Ta je torej dolžna tudi pisno utemeljiti svojo presojo. Za to presojo je pooblaščen oseb tudi odgovorna. Zaradi tega je seveda okoliščina, kdo je določil tajnost podatka, lahko zelo pomembna. Določanje tajnosti podatkov mora biti podvrženo ustrezni kontroli. »Nadzor nad določanjem tajnih podatkov lahko opravlja samo institucija, ki je neodvisna od tistega, ki tajnost v posameznem organu določa« (Debelak in Rakočević 2002, : 194).

3.3.1 Nacionalni sistem preverjanja in varovanja tajnih podatkov

Pravico dostopa do tajnih podatkov imajo samo tiste osebe, ki imajo dovoljenje in se morajo s tajnimi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog. Dostop imajo samo do tajnih podatkov stopnje tajnosti, določene v dovoljenju. Nihče ne sme dobiti tajnega podatka prej in v večjem obsegu, kot je to potrebno za opravljanje njegovih delovnih nalog ali funkcije (ZTP, 31. člen).

Dostop je seznanitev osebe s tajnim podatkom ali možnost osebe pridobiti tajni podatek na podlagi dovoljenja za dostop do tajnih podatkov (ZTP, 2. člen). Omejitev

dostopa do tajnih podatkov je temeljni ukrep glede varovanja tajnih podatkov. Z določitvijo podatka za tajnega se dostop do takšnega podatka omeji na točno določen krog oseb, ki morajo za dostop izpolnjevati predpisane pogoje. Omejitev dostopa je v vsakem primeru varnostni ukrep, ki je posledica določitve nekega podatka za tajnega. Vsi varnostni ukrepi, ki so sprejeti za varovanje takšnega podatka, imajo namen preprečiti dostop do podatka nepoklicanim osebam oziroma omogočiti dostop do tajnega podatka samo tistim, ki za to izpolnjujejo predpisane pogoje (Debelak in Rakočević 2002, : 195).

Prvi pogoj za dostop do tajnih podatkov je dovoljenje za dostop do tajnih podatkov, katerega posamezniku izda pristojni organ, če ni varnostnih zadržkov, ki bi to preprečevali. Dovoljenja za dostop osebe do tajnih podatkov stopenj zaupno, tajno ali strogo tajno izdajajo ministrstvo, pristojno za notranje zadeve, ministrstvo pristojno za obrambo, Slovenska obveščevalno-varnostna agencija (ZTP, 22. člen). Oseba, ki ima dovoljenje za dostop do tajnih podatkov, mora s pisno izjavo potrditi, da je seznanjena s predpisi, ki urejajo varovanje tajnih podatkov, sicer se ji dovoljenje prekliče. Dostop do tajnih podatkov ni pravica, ki bi jo lahko poljubno kdorkoli uveljavljal. Gre za konkretno dovoljenje, ki ga posameznik pridobi na podlagi odločitve posebej pooblaščenih oseb, če izpolnjuje zakonite pogoje (Debelak in Rakočević 2002, : 197).

4 VAROVANJE TAJNIH PODATKOV V MINISTRSTVU ZA OBRAMBO

4.1 Notranja organizacijska struktura MO

Da ugotovim, kateri so elementi, ki vplivajo na varovanje tajnih podatkov v Ministrstvu za obrambo, sem se odločil, da najprej analiziram samo notranjo organizacijsko strukturo ministrstva. V svojo analizo organizacijskih sprememb v ministrstvu sem vključil 21 sprememb Pravilnika o notranji organizaciji in delu ter sistemizaciji delovnih mest od 1990 do 30. 6. 2010, s katerim se je dejansko spreminjala notranja struktura organizacije. Na ta način želim ugotoviti, ali je morebiti notranja struktura ministrstva vzrok za slabše varovanje tajnih podatkov.

Instrumentalno proučevanje organizacij je tesno povezano s proučevanjem moči in procesa odločanja znotraj organizacije. Stopnja hierarhičnosti v organizaciji nam namreč omogoča zaznavanje stopnje avtoritarnosti in pozicije odločevalskih centrov pri shemi notranje strukture organizacije. Novejše teorije odločevanja nam tako omogočajo razumeti delovanje organizacije in vedenje članov organizacije ter pri tem zavračajo klasični model odločevanja, ki je temeljil na načelu »ekonomskega človeka«, to je osebk, katerega edini cilj je maksimizirati svoj profit v danih okoliščinah (Feldman in Kanter, 1965: 629).

Za določevanje tipa organizacije in za razumevanje, kam in kako določeno organizacijo umestiti v evolucijo organizacijske teorije, je potrebno analizirati **organizacijsko strukturo**. V tem smislu se relativna samostojnost strukture obravnava kot organizacijska variabla. Vendar pa jo je mogoče v praktičnem in teoretičnem smislu dojemati tako odvisno kot tudi neodvisno variabla. Kot odvisna variabla v primeru, da se jo je obravnavalo kot rezultat zunanjih in notranjih sil, kot neodvisna pa, ko se jo je obravnavalo kot temelj, katerega determinirajoč učinek deluje kot sila, ki oblikuje nekatere druge odvisne faktorje.

Eden izmed vidnejših teoretičnih pristopov k teoriji strukture je Webrova teorija birokratske organizacije. Weber namreč opazuje strukturo tako s stališča odvisnosti kot neodvisnosti. Tako označuje birokratsko organizacijo in njeno strukturo kot odvisno variabla, na katero vpliva mnogo različnih faktorjev skozi zgodovino organizacije (na primer: koncentriranost upravnih sredstev, kvalitativne in kvantitativne spremembe upravnih nalog ...).

Če pa se struktura organizacije opazuje kot neodvisna variabla, pa se njen vpliv na notranjo strukturo kaže kot princip pristojnosti določenih organov za opravljanje točno določenih nalog, pri čemer se upošteva v naprej določen vrstni red in nivoji odgovornosti (Weber 1987,: 374–383). Pri upoštevanju specifik upravnih organizacij, kamor spada tudi MO, je potrebno poleg vzvodov notranje strukture oziroma organizacije upoštevati tudi okolje, ki na upravno organizacijo vpliva. Izpostavimo lahko tri področja okolij, ki vplivajo na strukturo upravne organizacije: upravni sistem, politični sistem in civilno-družbena sfera. Uprava v modernem času namreč ni več tako visoko centralizirana in unificirana, kot je bila v preteklosti, temveč je vedno bolj

decentralizirana in diferencirana ter prevzema obliko privatnega sektorja (Franz, 1995).

Politični sistem je pri tem zaznamovan z dvojnostjo in potencialnim konfliktom, saj v svojem bistvu ne teži zgolj k izvajanju določenih javnih politik, ampak se obenem trudi ostati na oblasti. Novodobne kritike se osredotočajo bolj na to, da politični sistem vse težje odgovarja na kompleksna vprašanja v razvitih demokracijah. Pri tem upravne organizacije z ene strani zmeraj bolj sodelujejo pri oblikovanju in implementaciji političnih odločitev oziroma javnih politik, po drugi strani pa se poskušajo odmakniti od prevzemanja odgovornosti za legitimnost, politično podporo in kooperativnost.

V odnosu do državljanov (civilno-družbene sfere) pa v ospredje prihaja zahteva oziroma potreba po zadostni odzivnosti in efektivnosti upravnih organizacij, kot tudi transparentnost in ekonomičnost delovanja. Državljeni postajajo vse važnejše okolje upravnih organizacij, njihov vpliv pa ima posledice tudi in predvsem na notranjo strukturo organizacije. Nastajajo novi nivoji servisnih služb, oddelki za poslovanje z občani, pritožbeni oddelki ...

V tem smislu pa je potrebno izpostaviti, da državljani vplivajo na notranjo strukturo organizacije tudi preko predstavništev, torej izvoljenih teles. Zanimiv aspekt pri opazovanju odnosa med upravnimi organizacijami in civilno družbo je tudi aspekt moderne tehnologije, saj »komunikacijske tehnologije dopuščajo množičen dostop zainteresirane javnosti do delovanja in nudenja storitev upravne organizacije, ne le zgolj v številčnem ampak tudi v raznovrstnem smislu« (Gergen 1995,: 525).

4.2 Longitudinalna analiza organigramov MO

Analiziranje notranje organiziranosti določene organizacije je tesno povezano z določevanjem dejavnikov, ki na končno strukturo vplivajo v večji ali manjši meri. Poleg treh že omenjenih sklopov delujočih okolij (upravni sistem, politični sistem in civilna družba) lahko vplive na upravno organizacijo merimo z vnaprej določenimi spremenljivkami, ki so:

- hierarhičnost formalne strukture,
- vzpostavljenost in frekvenca uporabe formalnih in neformalnih kanalov v komunikacijski mreži,
- organizacijska kultura,
- organizacijska tehnologija,
- informacijska obremenjenost,
- finančna podpora političnega okolja.

Omenjene spremenljivke je možno meriti na več načinov. Lahko merimo število funkcionarjev v organizaciji ter njihov delež glede na število javnih uslužbencev, spremembe v številu funkcionarjev in javnih uslužbencev v določenem časovnem obdobju, štejemo lahko število nivojev v hierarhiji, štejemo število formalnih nivojev nasproti neformalnim, število delovnih mest na posameznem nivoju organizacije, povprečno število delovnih mest na vsakem hierarhičnem nivoju in podobno.

Število nivojev v hierarhičnosti upravne organizacije nam lahko da informacijo, kakšno formalno odločanje je v posamezni organizaciji predvideno, kot tudi kakšno je dejansko stanje hierarhičnosti in razvejanosti posamezne organizacije. Vendar je takšna analiza smiselna le v primeru, ko obravnavamo več upravnih organizacij skupaj in jih tako razvrščamo glede na hierarhičnost. Ne obstaja namreč neka univerzalna formula za normativni izračun visoke ali nizke stopnje hierarhičnosti, na podlagi katere bi lahko sklepali tudi na druge značilnosti organizacije.

Pri longitudinalni analizi organigramov MO od leta 1990 do leta 2006 (glej Tabelo 2) ugotavljamo naslednje:

- število sprememb v določenem časovnem obdobju (na leto),
- število hierarhičnih nivojev v organizaciji po vsaki spremembi strukture organizacije ter
- razvejanost organizacije (sem štejemo tudi organe v sestavi MORS-a).

4.3. Spremembe v notranji organiziranosti na MO

Število sprememb v organizaciji glede na časovno variabla nam pokaže pogostost spreminjanja notranje strukture v organizaciji, kar nam nadalje kaže na aktivnost zunanjega okolja, dinamičnost prilagajanja organizacije, odzivnost na potrebe (tako kadrovske, kot upravljaljske) in na potencialno nedograjenost »mlade« organizacije, ki s svojo izgradnjo oblikuje odsev potreb družbe v obdobju demokratičnega prehoda.

Tako je število sprememb letno, ne glede na to, ali so izvedene spremembe v strukturi vertikalne ali horizontalne, potrebno beležiti in slediti obliki razvoja notranje strukture organizacije. Glede na to, da kot vzvod za spreminjane znotraj organizacije delujejo tako notranji kot zunanji faktorji, lahko sklepamo, da so prvi posledica nekaterih notranjih premikov, specializacij določenih segmentov organizacije ali odsev potreb znotraj organizacije, drugi pa so praviloma posledica sprememb v političnem in civilno-družbenem okolju.

Glede na naravo dela MO-ja pa lahko sklepamo, da prevladuje vpliv političnega okolja. S tega stališča se lahko nadalje meri vplivanje na notranjo (re)organizacijo pri menjavi mandata, vstopanje v razna varnostno-politična združenja, odziv na globalizacijske procese v svetu in podobno.

Tabela 4.1: Spremembe v notranji organizaciji MORS-a od 1990 do 2006

LETO	ŠT. SPREMEMB*
1990	1
1991	1
1992	1
1993	1
1994	1
1995	1
1996	0
1997	1
1998	0
1999	2

2000	4
2001	1
2002	3
2003	0
2004	2
2005	1
2006	1

* Spremembe beležimo glede na spremembe Pravilnika o notranji organizaciji in delu ter o sistemizaciji delovnih mest MO.

Na podlagi pregleda števila sprememb lahko zaključimo, da se je MORS od svoje ustanovitve pa do leta 1999 razvijal relativno postopneje, s približno eno (včasih pa tudi nobeno) spremembo strukture notranje organiziranosti letno. Bolj dinamično spreminjanje organizacijske strukture se prične z letom 1999 (dve spremembi), nato s kar štirimi spremembami leta 2000 in tremi leta 2002. Po tem dinamičnem obdobju pa beležimo novo obdobje brez drastičnih sprememb v notranji strukturi organizacije.

4.3.1 Hierarhični nivoji na ministrstvu za obrambo

Število novonastalih ali eliminiranih hierarhičnih nivojev v upravni organizaciji nam nakazuje na to, kakšno delo organizacija opravlja in kako se odziva na dražljaje vseh treh okolij (upravni sistem, politični sistem in civilna družba). V obdobju od začetka oktobra 1990 je bilo v MORS skupaj 21 sprememb notranje organiziranosti (spremembe smo beležili le na formalnem nivoju glede na spremembe Pravilnika o notranji organizaciji in delu ter o sistemizaciji delovnih mest MO).

Tabela 4.2.: Spremembe števila hierarhičnih nivojev v MO

SPREMEMBA* (datum)	ŠT. NIVOJEV**
1 (2.10.1990)	2
2 (16.7.1991)	3
3 (30.6.1992)	3
4 (25.3.1993)	3
5 (18.2.1994)	3
6 (15.2.1995)	4
7 (30.9.1997)	4
8 (5.1.1999)	4
9 (6.10.1999)	4
10 (6.1.2000)	5
11 (28.3.2000)	5
12 (15.5.2000)	5
13 (28.8.2000)	5
14 (16.11.2001)	5
15 (25.1.2002)	5

16 (10.6.2002)	5
17(6.12.2002)	5
18 (2.6.2004)	5
19 (19.7.2004)	5
20 (3.8.2005)	5
21 (30.6.2006)	5

* Spremembe beležimo glede na spremembe Pravilnika o notranji organizaciji in delu ter o sistemizaciji delovnih mest MO.

** Meri se maksimalno število nivojev v globino.

Na podlagi gornjih rezultatov je mogoče zaključiti, da se je hierarhična piramida nivojev odločanja v MO-ju višala, kar pomeni, da se je število hierarhičnih nivojev konstantno povečevalo. Nikjer ni opaziti večjega preskoka v številu, kar pomeni, da povod za poglobljanje hierarhije niso bili drastični vplivi iz okolja (tako notranjega kot tudi zunanega), ampak potreba po nadaljnji specifikaciji dela v organizaciji. To je razvidno

tudi pri pregledu sprememb, saj se je število nivojev navadno poglobljalo le znotraj ene službe naenkrat, kar kaže na specifične potrebe po specifikaciji dela znotraj te službe.

Vendar pa je dejstvo, da je hierarhična piramida MO ne glede na dejstvo, da se počasi viša, precej nizka, kar nakazuje na **preobremenjenost prvega nivoja** organizacije (ministra in njegovega kabineta) zaradi velikega števila neposredno odgovornih (podrejenih) enot (direktoratov, uradov, služb, uprav).

Za učinkovito delovanje vrha organizacije oz. ministrstva je namreč nujno potrebna višja hierarhičnost v notranji strukturi organizacije. Po drugi strani pa je nižja piramida ugodna predvsem s stališča komuniciranja med vrhom in nivoji, saj se tako informacije ne »izgubljajo« ali »deformirajo«. Tok dialoga je jasen in hitro prenosljiv, vendar se ta oblika notranje organizacije praviloma uporablja v tržno naravnanih organizacijah (podjetjih v konkurenčnih panogah). Bolj poredko pa v upravnih organizacijah.

4.3.2 Organizacijska razvejanost ministrstva od leta 1990 do 2006

Poleg poglobljanja (večanja števila nivojev v hierarhiji organizacije) nas pri opazovanju spreminjanja notranje strukture upravne organizacije zanima tudi »širjenje« oziroma kakšno je število upravnih enot (oddelkov, služb, uprav, inšpektoratov) na posameznem nivoju.

Na podlagi tega lahko sklepamo, kako se je upravna piramida ožila oziroma širila; na podlagi te ugotovitve pa lahko izhajajoč iz teoretičnih izhodišč (zgoraj) sklepamo, s kakšnimi vplivi se je pri spreminjanju notranje organiziranosti proučevana organizacija soočala.

Tabela 1.3: Organizacijska razvejanost v ministrstvu po posameznih spremembah

SPREMEMBA* (datum)	ŠT. ENOT NA DRUGEM NIVOJU**	ŠT. ENOT NA TRETJEM NIVOJU**	ŠT. ENOT NA ČETRTEM NIVOJU**	ŠT. ENOT NA PETEM NIVOJU**
1 (2.10.1990)	11	/	/	/
2 (16.7.1991)	14	47	/	/
3 (30.6.1992)	15	45	/	/
4 (25.3.1993)	17	40	/	/
5 (18.2.1994)	17	54	/	/
6 (15.2.1995)	17	69	4	/
7 (30.9.1997)	23	94	92	/
8 (5.1.1999)	8	***	***	/
9 (6.10.1999)	10	20	122	/
10 (6.1.2000)	10	45	94	4
11 (28.3.2000)	14	47	***	***
12 (15.5.2000)	13	52	103	***
13 (28.8.2000)	12	62	17	***
14 (16.11.2001)	11	92	35	***
15 (25.1.2002)	11	62	74	***
16 (10.6.2002)	11	71	65	11
17 (6.12.2002)	11	69	72	11
18 (2.6.2004)	13	74	88	15
19 (19.7.2004)	14	72	82	9
20 (3.8.2005)	13	81	62	3
21 (30.6.2006)	13	80	68	5

* Spremembe beležimo glede na spremembe Pravilnika o notranji organizaciji in delu ter o sistemizaciji delovnih mest MO.

** Meri se maksimalno število nivojev v globino.

*** Ni podatka, na podlagi razpoložljivih podatkov ni mogoče sklepati.

Glede na razpoložljive podatke žal težje ocenjujem celotne notranje spremembe v MO, saj so mi bili nekateri podatki nedostopni in pomanjkljivi ali pa nezadostno označeni. Vendar pa na podlagi metodičnega sklepanja lahko sklepam o nekaterih splošnih zakonitostih organizacijskega razvoja MO:

a) Prva ugotovitev se kaže v postopnem povečevanju enot na drugem nivoju organizacije (torej organi, ki so neposredno odgovorni resornemu ministru) do leta 1997, ko število le-teh doseže višek; po letu 1997 pa se število enot na tem nivoju organizacije zopet sistematično zmanjšuje. To nakazuje na naglo povečevanje potrebe po različnih službah kmalu po vzpostavitvi ministrstva (po letu 1990). Po tem obdobju pa sledi obdobje racionalizacije znotraj strukture in povečevanje števila enot na tretjem, četrtem in petem nivoju organizacije, ki so sčasoma pričele prevzemati naloge prej razširjenega drugega nivoja.

b) Število enot na tretjem nivoju se je skladno s to predstavo o specializaciji ravno tako povečevalo (čeprav bolj nelinearno) in se je od začetka proučevanega časovnega obdobja, to je od leta 1990 do 2006, skoraj podvojilo. Pri natančnejši analizi sprememb lahko namreč ugotovimo prenos nekaterih nalog iz drugega na tretji nivo, kar kaže na zakonitosti višanja hierarhične piramide in večje stopnje specializacije posameznih enot in nivojev.

c) Malce težje določljive pa so spremembe pri notranji organiziranosti četrtega in petega nivoja MO. Čeprav je tukaj odklon zaradi pomanjkljivosti podatkov večji, pa se kaže nekakšna slika ustanavljanja posameznih organov po potrebi, glede na hipne potrebe ter njihovo naglo ukinjanje takoj, ko neke (začasne?) potrebe ni bilo več. Glede na to, da so nižji nivoji v organizacijah namenjeni operacionalizaciji dela v organizaciji,

bi bilo po moji oceni bolj smotrno obdržati nižje nivoje na račun širine hierarhične piramide in ne obratno.

Na podlagi te analize je mogoče reči, da je razvoj sprememb pri notranji organiziranosti MO od leta 1990 do 2011 v marsikaterem pogledu (odzivi na okolje, razvoj organizacije, potrebe specializaciji in spremembah) klasičen in razumljiv.

Po drugi strani pa je izrazito nizka (ploščata) in neenakomerno globinsko razvejana piramida znak nekonsistentnega in razdrobljenega, morda skorajda že osebnega pristopa vsake od vodilnih ekip na ministrstvu k razvoju organizacije, pri čemer pa ne gre pozabiti, da gre za vojaško in upravne organizacijo z nalogami zagotavljanja nacionalne varnosti, s čimer dobi tak pristop malce zaskrbljujoče poteze.

4.4 Pravna ureditev varovanja tajnih podatkov na ministrstvu

Zakon o tajnih podatkih je vsem državnim organom, ki pri svojem delu izdelujejo, obdelujejo ali prejemajo tajne podatke, v svojem 38. členu naložil, da morajo vzpostaviti takšen sistem varovanja teh podatkov, da bo nepoklicanim osebam onemogočeno dostopanje do njihovih tajnih podatkov. V nadaljevanju zakon o tajnih podatkih, v zvezi z varovanjem tajnih podatkov nalaga predstojnikom organov, da določijo posameznika ali organizacijsko enoto, ki bo v organu (ministrstvu) skrbela za enoten sistem varovanja, določanja in obravnavanja tajnih podatkov.

Na podlagi tega se je minister za obrambo odločil, da bo organ, ki bo skrbel za enoten sistem varovanja, Obveščevalno varnostna služba MO.¹⁰ Da bi bilo povsem jasno, katere naloge na področju tajnih podatkov ter na kakšen način jih bo služba opravljala, so izdelali in sprejeli Pravilnik o varovanju tajnih podatkov na MO,¹¹ s katerim se je vrsta zadev iz krovnega zakona o tajnih podatkih in uredb s tega področja podrobneje opredelila in določila.

¹⁰ Obveščevalno varnostna služba ima opredeljene svoje naloge in pooblastila v členih od 32. do 36. člena Zakona o obrambi.

¹¹ Pravilnik o varovanju tajnih podatkov na Ministrstvu za obrambo je interni dokument, ki ga podpiše minister za obrambo.

4.5 Pravilnik o varovanju tajnih podatkov v MO

Iz sprememb zakona o TP iz leta 2003 je izhajalo, da se mora na nivoju ministrstva in njenih NOE določiti organizacijsko enoto ali osebo, ki bo skrbela za varovanje tajnih podatkov tako na nivoju MO kot tudi v nižjih organizacijskih enotah. Prvi pravilnik je bil sprejet na Ministrstvu za obrambo dne 21. 2. 2006. Ker se je junija istega leta spremenil zakon, je bilo potrebno ponovno spremeniti tudi pravilnik, kar je bilo storjeno dne 31. 8. 2006. Po uveljavitvi varnostnih območij (VO) so se na ministrstvu pojavile težave z zagotavljanjem sredstev za VO, zato se je pravilnik leta 2008 popravil in nato še leta 2010. Zaradi sprememb pri upravljanju in delu z dokumentarnim gradivom in uvajanjem elektronskega poslovanja tudi s tajnimi podatki, se je pravilnik zadnjič spremenil leta 2012.

Glavni razlog, zakaj se je pravilnik o varovanju tajnih podatkov leta 2008 spremenil, je bil v tem, da ni bilo povsem jasno, katera organizacijska enota v MO bo zagotavlja finančna sredstva za urejanje varnostnih območij in nakup blagajn za shranjevanje TP. Ravno tako so se pojavljale dileme in vprašanja, katere osebe v MO sploh lahko sprožijo postopek varnostnega preverjanja za osebe v ministrstvu in za osebe v podjetjih, ki delajo za potrebe ministrstva in potrebujejo varnostna dovoljenja.

Pravilnik je sprejet na podlagi Zakona o državni upravi, Zakona o tajnih podatkih in Uredbe o varovanju tajnih podatkov. Glavni namen pravilnika je, da se z enotno ureditvijo splošnih in posebnih postopkov ter ukrepov varovanja zagotovi učinkovit sistem varovanja tajnih podatkov na ministrstvu.

Kot je že bilo povedano, se je minister odločil, da bo **OVS skrbela za enoten sistem varovanja tajnih podatkov v ministrstvu** in ji je s pravilnikom naložil naslednje naloge:

- opravlja postopke varnostnega preverjanja za izdajo dovoljenj za dostop do tajnih podatkov,
- opravlja postopke izdaje varnostnega dovoljenja organizacijam iz 1. člena zakona,
- izdaja usmeritve za pripravo načrtov varovanja tajnih podatkov,
- opravlja proti prisluškovalne preglede za ministrstvo in organizacije, ki izvajajo naročila s področja obrambe,
- na intranet straneh MO objavlja obrazce, vzorce in druge oblike zapisov tajnih podatkov, ki se uporabljajo pri obravnavanju tajnih podatkov,
- na podlagi predloga pristojnega predlagatelja posreduje predloge Nacionalnem varnostnem organu za izdajo varnostnega dovoljenja za dostop do tajnih podatkov NATO in EU, izdajo overjenih kopij EU in NATO dovoljenj ter najavo posameznih dogodkov v skladu z Uredbo o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov,
- v sodelovanju z organizacijsko enoto ministrstva, pristojno za upravljanje človeških virov, izvaja usposabljanje zaposlenih v organizacijskih enotah ministrstva, razen Generalštaba, ter sodeluje pri načrtovanju vsebin za usposabljanje, ki ga v SV organizira Generalštab,
- pripravlja predloge predpisov in splošnih aktov s področja tajnih podatkov, razen za področje varovanja tajnih podatkov na informacijskem in komunikacijskem področju,
- izvaja **notranji nadzor** v skladu z 41. členom zakona, **razen Generalštaba, kjer notranji nadzor izvajajo pristojni štabno varnostni organi, ki o ugotovitvah nadzorov obveščajo Obveščevalno varnostno službo,**
- v skladu s prepisi, internimi akti ministrstva ter navodili ministra in generalnega direktorja Obveščevalno varnostne službe opravlja druge naloge s področja varovanja tajnih podatkov.

Ima pa služba še eno pomembno nalogo. Vsako leto mora do konca meseca marca izdelati oceno ogroženosti MO, v katero mora vključiti oceno ogroženosti na področju vohunjenja, sabotaž, terorizma in drugih oblik ogrožanja sistema. S to oceno morajo biti seznanjene vse organizacijske enote ministrstva.

V pravilniku je jasno zapisano, da so se vsi zaposleni dolžni usposabljati s področja tajnih podatkov. Za vse organizacijske enote ministrstva to izvaja OVS, razen za Generalštab, ki to izvaja za svoje potrebe. Prepisano je, da se potrdila o usposabljanjih izdajajo v COU Poljče in v okviru SV v Centru za doktrino, razvoj in usposabljanje.

Eno izmed pomembnih poglavij v pravilniku je poglavje o določanju stopenj tajnosti. V 9. členu pravilnika je dokaj natančno določeno, kdo lahko določa tajnosti tajnim podatkom najvišje stopnje.

Najvišjo stopnjo tajnosti podatkom STROGO TAJNO lahko v ministrstvu za obrambo določijo minister kot predstojnik organa, načelnik GŠ SV, glavni inšpektor IRSO, direktor URSZR in glavni inšpektor IRSVNDN ter določeni vojaški poveljniki, ki jih za to posebej pooblasti predstojnik organa.

Stopnje INTERNO, ZAUPNO in TAJNO lahko v skladu s pravilnikom določijo naslednje osebe: državni sekretar, generalni direktorji direktoratskih uradov, generalni direktor OVS, generalni sekretar, vodja Kabineta ministra, direktorji uradov, sektorjev, centrov, služb, uprav za obrambo, izpostav URSZR, izpostav IRSVNDN, vodja obrambnega oddelka v stalni misiji pri NATO, višji obrambni predstavnik v OVSE, obrambni predstavnik v OVSE, obrambni atašeji ali njihovi namestniki oziroma osebe, ki jih nadomeščajo na podlagi sklepa o nadomeščanju, delavci, ki so na predlog generalnega direktorja OVS določeni s posebnim sklepom ministra, inšpektor višji svetnik, inšpektor svetnik in inšpektor v Inšpektoratu Republike Slovenije za obrambo in osebe, ki jih za to individualno pooblasti minister.

Vodje uprav za obrambo lahko določajo stopnje tajnosti INTERNO in ZAUPNO.

Hkrati s tem, ko vse zgoraj navedene osebe določijo posameznemu podatku stopnjo tajnosti, morajo poleg določitve tajnosti izdelati še posebno oceno škodljivih posledic. Ta ocena je pisna in je sestavni del dokumenta (šteje se, da je priloga dokumenta), ki mu je bila določena stopnja tajnosti. V tej oceni se mora pisno oceniti, kakšne bi bile škodljive posledice razkritja tajnega podatka, če bi se z njim seznanila nepooblaščenca oseba ali če to pride v javnost.

V praksi je največ težav ravno s pisanjem ocen možnih škodljivih posledic razkritja, saj pooblašcene osebe za to še vedno niso dovolj usposobljene. V teh ocenah je namreč potrebno vnaprej predvideti, kakšne posledice bi nastale, če bi nek tajni podatek bil razkrit oz. če bi se z njim seznanila nepooblašчена oseba. Največkrat pa se zgodi, da oseba, ki ima pooblastilo za določanje stopnje tajnosti, sploh ne napiše ocene, temveč mora to storiti njemu podrejeni sodelavec. Največkrat se zgodi, da ta oseba ne pozna vseh okoliščin, v katerih je podatek nastal in bil določen za tajnega, ali pa sploh nima delovnih izkušenj na tistem delovnem mestu.

Se pa morajo pooblašcene osebe za določanje stopnje tajnosti dobro zavedati še nečesa. Če bodo njihove ocene škodljivih posledic slabo zapisane in ne dovolj utemeljene in tehtne, se lahko zgodi, da bodo morali razkriti tajni podatek zaradi določil Zakona o dostopu do informacij javnega značaja.

Po Zakonu o dostopu do informacij javnega ¹²značaja je namreč omogočen prost dostop do vseh informacij javnega značaja, s katerimi razpolagajo državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb (1. člen).

Vse informacije javnega značaja so enako dostopne tako posameznikom kot pravnim osebam. In če posameznik želi biti seznanjen z dokumentom, ki je označen kot tajni podatek, mora predstojnik organa, kjer je bila takšna zahteva vložena, zahtevo posredovati na vlado RS. O upravičenosti prevladujočega javnega interesa za razkritje tajnega podatka odloča vlada na podlagi predhodnega mnenja komisije.

Komisija, ki presoja o upravičenosti javnega interesa, je sestavljena iz predstavnikov ministrstva za obrambo, ministrstva za notranje zadeve, ministrstva za zunanje zadeve, SOVA in nacionalnega varnostnega urada. Naloga komisije je, da na podlagi pisne ocene možnih škodljivih posledic oceni, ali je prevladujoč javni interes po dostopu do tega dokumenta močnejši, kot pa je interes za omejitev dostopa do tajnega

¹² Po Zakon o dostopu do informacij javnega značaja lahko vsaka oseba zahteva dostop do tajnih podatkov stopnje interno in zaupno. O vsaki zahtevi za dostop odloča posebna vladna komisija, ki deluje pri UVTP-ju in jo vodi direktor.

podatka. Vse pa je odvisno, kako je pooblaščen oseba ocenila, kakšne škodljive posledice bi nastale za organ ali pa Republiko Slovenijo.

Če Vlada RS na podlagi mnenja komisije oceni, da je javni interes glede razkritja močnejši od javnega interesa za omejitev dostopa do podatka ali dokumenta, potem naloži organu, v katerem je bila zahteva vložena, da prekliče stopnjo tajnosti. Najkasneje v 15 dneh mora organ preklicati stopnjo tajnosti in prosilca za dostop do informacije seznaniti z zahtevanim dokumentom.

Ne more pa posameznik ali organizacija zahtevati dostopa do vseh vrst informacij.

Omejitve so zlasti pri dostopanju do naslednjih vrst informacij:

- tajni in strogo tajni podatki s področja javne varnosti, obrambe države, mednarodnih odnosov, obveščevalne ali varnostne dejavnosti državnih organov,
- poslovne skrivnosti v gospodarskih družbah,
- osebni podatek, katerega razkritje bi pomenilo kršitev varstva osebnih podatkov,
- podatek, katerega razkritje bi pomenilo kršenje zaupnosti individualnih podatkov v dejavnosti državne statistike,
- podatek, ki se nahaja v javnem arhivskem gradivu, ki je v skladu z zakonom, ki ureja arhivsko gradivo in arhive, opredeljen kot zaupen,
- podatek, katerega razkritje bi pomenilo kršitev zaupnosti davčnega postopka,
- podatek, ki je bil pridobljen ali sestavljen zaradi kazenskega pregona ali v zvezi z njim, ali postopka s prekrški in bi njegovo razkritje škodovalo njegovi izvedbi,
- podatek, ki je bil pridobljen ali sestavljen zaradi upravnega postopka,
- podatek, ki je bil pridobljen ali sestavljen zaradi pravnega, nepravdnega ali drugega sodnega postopka,
- podatek iz dokumenta, ki je v postopku izdelave, in je še predmet posvetovanj v organu, njegovo razkritje pa bi povzročilo napačno razumevanje njegove vsebine,
- podatek o naravni vrednoti,

- podatek iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organov in bi njegovo razkritje povzročilo motnje pri delovanju oziroma dejavnosti organa (6. člen zakona).

Pravilnik o varovanju tajnih podatkov na MO določa (15. člen), da mora vodja NOE zagotoviti, da se vsi tajni podatki, katerim je določil stopnjo tajnosti, vsake tri leta pregledajo. Ob tem pregledu morajo oceniti, ali še obstaja potreba po tajnosti in stopnji tajnosti ali pa se z dokumenta umakne oznaka stopnje tajnosti. V primeru spremembe stopnje tajnosti je potrebno pripraviti novo pisno oceno škodljivih posledic.

Vodja NOE ima dve možnosti:

- da spremeni stopnjo tajnosti, torej zniža stopnjo tajnosti,
- da prekliče stopnjo tajnosti.

Vsakega od prejemnikov tajnega podatka mora obvestiti o znižanju stopnje tajnosti ali o umiku stopnje tajnosti. Vsi prejemniki takšnega obvestila morajo nemudoma spremeniti stopnjo tajnosti na prejetem tajnem podatku in poleg njega pripeti obvestilo originatorja.

Pravilnik o varovanju TP v MO natančno določa, katere osebe lahko sprožijo postopek preverjanja za osebe ali podjetja, ki želijo dostopati do TP. Predlagatelji postopka so vodja kadrovske službe v upravnem delu in oseba, ki ga nadomešča, v Slovenski vojski pa je to oseba, ki je pristojna za upravljanje človeških virov ali druge osebe, ki jih za to pooblasti načelnik Generalštaba.

4.5.1 Osnovno in dodatno usposabljanje za ravnanje s tajnimi podatki

Na podlagi sprememb Zakona o TP v letu 2006 je zakonodajalec v Uredbi o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov v 21. členu dodatno zapisal, da so se osnovnega varnostnega usposabljanja dolžne udeležiti vse osebe, ki bodo prvič zaprosile za izdajo varnostnega dovoljenja. Na ta način se sedaj morajo tega usposabljanja udeležiti tudi osebe, ki bodo imele dostop samo do internih

tajnih podatkov, ki se sicer po zakonu posebej ne preverjajo. Te osebe morajo poleg potrdila za dostop do tajnih podatkov interno imeti še podpisano izjavo, da so seznanjene s prepisi s tega področja.

Osnovnega usposabljanja so se dolžne udeležiti tudi osebe, ki so v postopku vmesnega varnostnega preverjanja. Gre za tiste osebe, ki sicer imajo veljavno varnostno dovoljenje, pa so bile zaradi daljše bolniške odsotnosti ali porodniške iz delovnega okolja odsotne več kot eno leto in v tem času niso dostopale do tajnih podatkov. V postopku vmesnega varnostnega preverjanja te osebe ne smejo dostopati do tajnih podatkov. Predhodno se morajo udeležiti osnovnega usposabljanja (da se osveži njihovo znanje s tega področja), nato pa ponovno izpolnijo vprašalnik za dostop do tajnih podatkov za dovoljenja, ki ga imajo.

Za ostale kandidate, ki so v postopku varnostnega preverjanja za dostop do zaupnih, tajnih ali strogo tajnih podatkov, pa velja, da poleg izpolnjenega vprašalnika svoji vlogi za izdajo dovoljenja priložijo še kopijo potrdila o udeležbi na osnovnem usposabljanju.

V Pravilniku o varovanju tajnih podatkov na MO iz leta 2006 je bilo zapisano, da se usposabljanja s področja tajnih podatkov izvajajo v Centru za obrambno usposabljanje v Poljčah, kjer tudi vodijo evidenco o izdanih potrdilih.

Ker je bilo veliko nejasnosti, kateri organ v SV izdaja ta potrdila, se je v spremembe Pravilnika o varovanju tajnih podatkov na MO, ki so bile sprejete junija 2008, zapisalo, da potrdila za SV izdaja takratno Poveljstvo za doktrino, razvoj in usposabljanje, danes je to Center vojaških šol.

Na tem mestu naj poudarim, da bi po mojem mnenju morala biti funkcija izobraževanja in usposabljanja v Ministrstvu za obrambo, enotna in nedeljiva ter v eni sami organizacijski enoti za celotni obrambni sistem.

Za osnovno usposabljanje je na podlagi Pravilnika predpisana vsebina osnovnega usposabljanja. Usposabljanje traja najmanj 4 šolske ure. Slušatelji se na osnovnem usposabljanju seznajajo z naslednjimi vsebinami:

- prepisi s področja varovanja tajnih podatkov,

- tajni podatki - splošno,
- določitev stopnje tajnosti,
- označitev tajnih podatkov,
- evidentiranje in uničenje tajnih podatkov,
- prenos tajnih podatkov,
- razmnoževanje tajnih podatkov,
- osebe, pooblašene za določanje stopenj tajnosti,
- varnostno preverjanje za dostop do tajnih podatkov,
- vloga in naloge nacionalnega varnostnega organa,
- industrijska varnost,
- informacijska varnost,
- izvajanje nadzora nad zakonom.

Število oseb, ki se udeležuje osnovnega usposabljanja, je različno po letih. Odvisno je od tega, koliko oseb prvič prosi za izdajo dovoljenja za dostop do tajnih podatkov, ter števila oseb, ki se vračajo na svoje delovno mesto po dolgotrajni bolniški odsotnosti ali po porodniškem dopustu.

Dodatno usposabljanje je namenjeno osebam, ki imajo že izdano veljavno dovoljenje za dostop do tajnih podatkov zaupno ali višje. V 22. členu Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov je zapisano, da se morajo tega enkrat letno obvezno udeležiti vse tiste osebe, ki tajnim podatkom določajo stopnje tajnosti (ZTP 10. člen), osebe, ki so pooblašene za izdajo dovoljenj (ZTP 22. člen), osebe, ki so pooblašene za izvajanje nadzora in usmerjanje varnostnih ukrepov v organizacijah in podjetjih (ZTP, 4. točka 35. člena), osebe, ki opravljajo nadzor v organih in organizacijah (ZTP, tretji odstavek 38. člena in drugi odstavek 41. člena). Z udeležbo na dodatnem usposabljanju osebe, naštet iz posameznih členov zakona, svoje že izdano dovoljenje za dostop do tajnih podatkov potrdijo za tekoče leto.

V Ministrstvu za obrambo se je dodatnega usposabljanja leta 2006, ko se je pričelo z izvajanjem dodatnega usposabljanja, udeležilo 226 zaposlenih, leta 2007 pa že preko 900 zaposlenih. Od leta 2008 pa do leta 2014 je bilo udeležencev 850, leta 2013 pa jih je bilo okoli 1100.

Zaradi velike obremenjenosti predavateljev in težnje po sodobnejših oblikah usposabljanja so leta 2015 prešli na sodobnejšo obliko usposabljanja, na daljavo. V okviru SV so v CVS-u strokovnjaki pripravili t. i. e-učilnico. Zaposleni lahko tako preko interneta, na daljavo, opravijo svoje letne obveznosti glede usposabljanja iz 22. člena Uredbe o varnostnem preverjanju. Vsebina e-učilnice je prilagojena prejšnjemu dodatnemu usposabljanju. Seveda sedaj slušatelji predavatelja ne morejo spraševati o konkretni problematiki, kar je prejšnja oblika omogočala. Na vsako posamezno vprašanje imajo neomejeno število poizkusov, da poiščejo in najdejo pravilen odgovor.

4.5.2 Tematski nadzori nad tajnimi podatki v MO in SV

Varovanje tajnih podatkov v Ministrstvu za obrambo se lahko učinkovito zagotavlja samo preko nadzora nad usposobljenostjo zaposlenih za varovanje in ravnanje s tajnimi podatki. »Za učinkovitost delovanja sistema varovanja tajnih podatkov je ključen inšpekcijski nadzor, ki ugotavlja odklone od predvidene zaščite in nalaga popravke kot sistemski korekcijski mehanizem« (Prezelj in Tarman, 2015,: 690).

Tovrstni nadzori se v MO izvajajo od leta 2008 dalje, ko je bil sprejet prvi Pravilnik o varovanju tajnih podatkov na MO in SV. V ministrstvu so iskali najoptimalnejšo rešitev, kako preveriti, ali sistem varovanja tajnih podatkov deluje. Za sistem varovanja TP je zelo pomembno, da so zaposleni kot bistveni element tega sistema pravilno in pravočasno usposobljeni.

Osnova za uvrstitev izvajanja tematskih nadzorov v Pravilnik je namreč v Zakonu o tajnih podatkih, kjer je zapisano, da so »za notranji nadzor nad izvajanjem tega zakona in predpisov, sprejetih na njegovi podlagi, odgovorni predstojniki organov«. Ker se v OVS izvajajo vse ostale naloge iz zakona, je bilo povsem logično, da se naloge notranjega nadzora – tematskih nadzorov dodelijo v OVS.

Na podlagi pravilnika, OVS skrbi za »enoten sistema varovanja nacionalnih tajnih podatkov na ministrstvu ter za usklajevanje in sodelovanje z nacionalnim varnostnim organom ter drugimi organi in organizacijami zunaj ministrstva«. ¹³

Pri zagotavljanju enotnega sistema varovanja tajnih podatkov na MO se pojavlja problem. OVS lahko na podlagi določil pravilnika opravlja izvajanje tematskih nadzorov na področju tajnih podatkov samo v upravnem delu ministrstva. Tematske nadzore v SV opravljajo pripadniki štabno varnostnega organa. Pri tem se resno zastavlja vprašanje, na kakšen način ter kdo je pripadnike štabno varnostnega organa usposobil za izvajanje teh nadzorov. Kot mi je poznano, so bili nekateri poizkusi, da se izvajajo tematski nadzori s strani OVS tudi v SV. Temu so se pripadniki štabno varnostnega organa močno uprli in so grozili z umikom soglasja za spremembe pravilnika, če bi se takšen člen vnesel v pravilnik.

S tako veljavnim pravilnikom in takšnim določilom glede izvajanja tematskih nadzorov ne moremo govoriti o »enotnem sistemu varovanja tajnih podatkov na ministrstvu«. In če ne obstaja enoten sistem nadzora varovanja in kontrole nad tajnimi podatki, so tudi možnosti za pomanjkljivosti v sistemu varovanja toliko večje.

Bistvo izvajanja tematskih nadzorov v MO ni iskanje napak v sistemu varovanja tajnih podatkov v NOE ministrstva, temveč predvsem kot pomoč vodjem organizacijskih enot, kako še izboljšati sistem varovanja tajnih podatkov v organizacijskih enotah.

Tematske nadzore izvajajo najbolj izkušeni delavci OVS, ki vrsto let delajo na področju varovanja TP, nekateri so sodelovali pri izdajanju dovoljenj za dostop do TP za osebe, organizacije ali pa so sodelovali pri pisanju predlogov zakona ali uredb s področja TP.

Tematski nadzor se odredi z odredbo generalnega direktorja OVS. Določila tematskega nadzora se izvajajo v skladu z določili Zakona o splošnem upravnem postopku, enako kot se opravlja preverjanje za dostop do tajnih podatkov. Z odredbo

¹³ V pravilniku je določeno, kateri organ na ministrstvu je zadolžen za varovanje enotnega sistema tajnih podatkov na ministrstvu.

se določi obseg in časovno obdobje, za katero se bo tematski nadzor izvedel. Tematski nadzor izvedejo običajno trije delavci, strokovnjaki s svojega področja. Praviloma je eden od njih strokovnjak s področja osebne varnosti (izdaja dovoljenj za dostop do TP, vmesno varnostno preverjanje, usposabljanje s področja TP), strokovnjak za dokumentarno gradivo (označevanje dokumentov s TP, pošiljanje teh dokumentov, uničevanje, arhiviranje dokumentov) ter strokovnjak s področja tehničnega varovanja (varnost TP v KIS, določanje varnostnega območja, video nadzorni sistemi).

Praviloma so letno izvedli pet do šest tematskih nadzorov v ministrstvu. Končno poročilo o izvedenem nadzoru je vedno prejel tudi minister za obrambo.

4.5.3 Bistvene ugotovitve po tematskih nadzorih v upravnem delu MO

Pri izvedenih tematskih nadzorih so bile v upravnem delu ministrstva ugotovljene številna napake, ki imajo v svojem bistvu vzrok v dveh dejavnikih:

- Vodje NOE so šele prišli na vodilno mesto in se še niso uspeli seznaniti z vsemi predpisi na tem področju ter niso bili na nobenem dodatnem usposabljanju.
- Zaposleni v upravnem delu so bili pri svojem delu s tajnimi podatki nepazljivi, so jih pomotoma založili ali pa uničili.

Najpogostejše napake, ki so jih naredili vodilni delavci v posameznih delih ministrstva, so naslednje: niso se udeležili dodatnega usposabljanja o tajnih podatkih, svojih sodelavcev niso predlagali pravočasno v vmesno varnostno preverjanje, ko so prišli

po daljši odsotnosti nazaj na delovno mesto, pozabili so spremeniti stopnjo tajnosti po obvestilu o spremembi tajnosti dokumenta.

Zaposleni, ki so imeli dostopa do tajnih podatkov, so na podlagi rezultatov tematskih nadzorov tajne podatke – dokumente – pomotoma uničili. Ne da bi o tem naredili uradni zaznamek ali zapisnik, so tajne podatke poslali po informacijskem sistemu, ki ni bil akreditiran za tisto stopnjo tajnosti, kot jo je imel tajen dokument. Velikokrat se je zgodilo, da so zaposleni dokumente pomotoma založili in so jih šele čez nekaj mesecev ponovno našli.

4.6 Varnostna območja v ministrstvu za obrambo

S spremembo Uredbe o varovanju tajnih podatkov (Ur. l. RS št. 74/2005) je bil določen končni rok, in sicer 31. 12. 2005, do katerega so morali vsi državni organi uskladiti ukrepe na področju varovanja tajnih podatkov z njihovimi načrti varovanj. V uredbi, v njenem 10. členu, je prišlo tudi do pomembne spremembe pri obravnavanju območij, kjer se lahko hranijo tajni podatki.

Po Uredbi o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov (Ur. l. RS, št 70/02) smo imeli tri varnostna območja glede na tajne podatke, ki so se v njih shranjevali.

Varnostna območja:

- III. varnostno območje za interne dokumente,
- II. varnostno območje za zaupne dokumente in
- I. varnostno območje za tajne in strogo tajne dokumente.

S spremembo uredbe v letu 2006 pa se je III. VO preimenovalo v upravno območje, še naprej pa sta ostali v veljavi II. in I. varnostno območje. S spremembo Uredbe so se spremenili tudi pogoji hranjenja najvišjih stopenj tajnosti, kot so npr. strogo tajni podatki. Ti se sedaj lahko hranijo tudi v II. VO, kar po prejšnji uredbi ni bilo mogoče, seveda pa morajo biti tajni podatki, shranjeni v varnostnih vsebnikih – blagajnah z ustrežno stopnjo varnosti.

Varnostno območje določi predstojnik organa ali organizacije (12. člen Uredbe). Po veljavnem Pravilniku o varovanju tajnih podatkov v MO in SV je do meseca junija 2008 ta sklep o vzpostavitvi VO podpisal minister za obrambo. S spremembami pravilnika leta 2008 je bilo tovrstno pooblastilo preneseno s strani ministra na generalnega direktorja Obveščevalno varnostne službe.

Pri tem so sledili ideji, da minister kot predstojnik organa s preverjanjem pogojev za vzpostavitev varnostnega območja nima neposredne povezave. Če pa bi se na primer zgodilo, da bi bilo z varovanjem tajnih podatkov v nekem varnostnem območju karkoli narobe, bi bil posredno za to pomanjkljivost odgovoren ravno minister. S spremembo pravilnika, ko sklep o vzpostavitvi varnostnega območja podpiše generalni direktor OVS, pa ima direktor odločilno vlogo pri vzpostavljanju varnostnega območja, ki mora izpolnjevati določene standarde za varno obravnavo tajnih podatkov.

4.6.1 Načrti za varovanje tajnih podatkov

V skladu z Uredbo o varovanju tajnih podatkov (10. člen) se morajo tajni podatki stopnje interno obvezno nahajati v upravnem območju. Tajni podatki od stopnje zaupno navzgor pa se lahko obravnavajo in hranijo samo v točno določenem varnostnem območju - prostoru, ki je vidno označen. Glede na to, kateri tajni podatki se v posameznem območju hranijo, ločimo II. in I. varnostno območje (VO).

4.6.2 Splošni del načrta varovanja

Načrtovanje varnostnega območja se dejansko prične z oceno ogroženosti nekega objekta ali prostora, v katerem bodo tajni podatki nastajali, se obdelovali ali hranili. Pri načrtovanju vzpostavitve varnostnega območja pa je najprej potrebno realno oceniti, koliko TP se bo nekje hranilo oz. koliko jih v določenem času v neko NOE dobijo oz. pri njih sploh nastanejo. Na MO se pogosto dogaja, da vodje NOE tega ne znajo oceniti in potem so se porabljala velika finančna sredstva za vzpostavitev ustreznega VO, v

katerem se potem hrani malo število tajnih podatkov. Od ocene ogroženosti so potem odvisni tudi tehnični in drugi ukrepi za varovanje TP.

Načrt varovanja tajnih podatkov v varnostnem območju vsebuje naslednje elemente:

- opis glavnega in pomožnih objektov,
- osnovni podatki o varnostnem območju,
- dostopne poti,
- podatki o varnostno tehnični opreми,
- opis varnostno tehnične opreme, ki se uporablja za varovanje,
- tehnično varovanje,
- fizično varovanje,
- načrt blokadnih mest,
- podatki o nosilcu načrta varovanja.

Pri izdelavi načrta varovanja sodelujejo vse osebe v NOE, kjer se hranijo in obdelujejo tajni podatki in morajo z njim biti tudi natančno seznanjeni. Za to, da so vsi seznanjeni z načrtom varovanja, je zadolžen nosilec načrta varovanja, ki mora v načrt varovanja zapisati svoje podatke ter kje in na katerih mobilnih številkah je dosegljiv 24 ur na dan in 7 dni na teden.

Med splošne ukrepe je na začetku načrta potrebno zapisati, da do tajnih podatkov lahko dostopajo samo tiste osebe, ki pred prvim dostopom do tajnih podatkov, že posedujejo veljavno dovoljenje. Potrebno je tudi zapisati, da se bodo vse osebe, ki bodo dostopale do tajnih podatkov, najprej udeležile osnovnega usposabljanja ter da se bodo tudi potem, ko bodo že imele ustrezno dovoljenje, še naprej usposabljele. Sem spada tudi obveza vodilnih v državnih organih in podjetjih, da bodo poskrbeli, da se s tajnimi podatki seznanijo samo osebe, ki imajo potrebo po vedenju, ter da poskrbijo, da so s tajnimi podatki seznane samo v obsegu, ki je nujen za opravljanje funkcije ali delovnih nalog.

Vse osebe, ki se bodo seznani s tajnimi podatki, morajo predhodno podpisati izjavo o seznanjenosti z Zakonom o tajnih podatkih.

4.6.3 Posebni del načrta varovanja

V posebnem delu načrta varovanja so zapisani fizični in tehnični ukrepi za varovanje TP v VO.

Ukrepi fizičnega varovanja

V načrt varovanja je v tem delu potrebno zapisati, kateri ukrepi fizičnega varovanja so izvedeni za varovanje objekta in varnostnega območja. S temi ukrepi se zagotavlja varovanje in nadzor prostorov, kjer se sprejemajo, obdelujejo, shranjujejo in uničujejo tajni podatki.

Zunanje fizično varovanje

V tem delu se opiše, na kakšen način se objekt varuje zunaj in s kakšnimi ukrepi se preprečuje dostop do območja, kjer se hranijo tajni podatki. Med te ukrepe nedvomno sodijo varnostne rešetke, ki morajo biti nameščene na oknih do višine 5 m. Izdelane morajo biti iz železnih elementov debeline 20 mm. Med elementi rešetk pa ne sme biti večjega razmaka kot 150 mm. Dostop do objekta, vhodi in morebitni drugi izhodi morajo biti osvetljeni z najmanj 40 luxov svetlobe. Če pa gre še za kombinacijo z video nadzornim sistemom, morajo visoko resolucijske kamere zagotavljati najmanj 460 linij horizontalne resolucije.

Med **notranje fizično varovanje** spadajo ukrepi, ki varujejo tajne podatke v zgradbi. Med te ukrepe nedvomno spada zahteva, da morajo biti zidovi VO debeline najmanj 100 mm iz armiranega betona ali iz materiala enake mehanske trdnosti. Vrata v VO pa morajo biti po standardu SIST ENV 1627 razreda 4, ki so vgrajena z vsaj tritočkovnim zapiranjem. Zunanji del protivlomnih vrat mora biti opremljen s slepo kljuko in protivlomno zaščito ključavnice. Cilindrični vložek mora ustrezati standardu SIST EN 1303, ki zagotavlja mehansko odpornost stopnje 2.

Tehnično varovanje

Namen tehničnega varovanja je, da se onemogoči dostop nepooblaščenim osebam do objekta, varnostnega območja in ne nazadnje do tajnih podatkov. Ukrepe tehničnega varovanja je vedno potrebno kombinirati s fizičnim varovanjem in s tem se zagotavlja nadzor nad vstopom v objekt oziroma v varnostno območje.

Sistem tehničnega varovanja obsega:

- sistem videonadzora,
- sistem protivlomnega varovanja,
- sistem mehanske zaščite.

Sistem video nadzora

V načrtu varovanja se v delu, kjer se opisuje sistem video nadzora, zapiše, kolikšen del zunanosti objekta je pokrit z video nadzorom, kako so pokrite dostopne poti do VO in tudi samo varnostno območje. Zelo pomembno je, da se opiše, ali se uporabljajo fiksne ali vrteče kamere ter kje se spremlja signal iz kamer in kdo jih servisira. Pomembno je, da je snemalna naprava, kjer se shranjujejo video posnetki v varnostnem ali upravnem območju, do kamor imajo dostop samo pooblaščen osebe. Zahteva je, da se posnetki video nadzora shranjujejo vsaj 60 dni in da je gostota posnetkov na vsaki kameri en posnetek na sekundo.

Sistem protivlomnega varovanja

V tem delu načrta se podrobneje opiše, kje in kako je sistem protivlomnega varovanja nameščen. Opiše se, na kakšen način je sistem nameščen, kdo ga upravlja, kdo ga nadzoruje in kam je speljan alarmni signal v primeru sprožitve alarma. Zelo pomembno je, da se alarmni sistem večkrat tudi dejansko preizkusi, kar mora biti zapisano tudi v načrtu. Najbolje je, da je sistem takšen, ki omogoča avtomatsko detekcijo gibanja in da je skladen s standardom SIST EN 50131, razreda 3, ki je vključen vedno, ko v varnostnem območju ni pooblaščenih oseb.

Kadar gre za varovanje VO, v katerih se nahajajo NATO ali EU tajni podatki, se temu delu varovanja namenja posebna pozornost. Inšpektorji, ki obiščejo državo članico pred vzpostavitvijo in ustrezno akreditacijo VO, v katerem so shranjeni NATO tajni podatki, skorajda vedno tudi sprožijo vlomni in požarni alarm in se tako v realnih razmerah prepričajo, ali sistem deluje in ali je odzivni čas za varnostno enoto dovolj hiter. Trenutno velja standard, da mora biti odzivni čas v obeh primerih 7 minut.

Sistem mehanske zaščite objekta

Namen sistema mehanske zaščite objekta, kjer se nahajajo tajni podatki, je v tem, da se prepreči dostop do objekta nepooblaščenim osebam. Vzpostavitev sistema pomeni, da se na dostopih do objekta izvede montaža:

- ograje,
- varnostnih rešetk na okna ali vrata,
- protivlomnih vrat na vseh vhodih in izhodih v objekt,
- varnostne ključavnice s protivlomnimi vložki in protivlomna zaščita ključavnic,
- blagajne,
- protivlomne folije na oknih.

V tem delu načrta je potrebno podrobneje opredeliti, kako ta sistem mehanske zaščite deluje ter kdo in na kakšen način pokliče serviserja, ki lahko napake hitro odpravi.

4.6.7 Smernice tehničnega varovanja in objektov ministrstva

S smernicami, ki so bile izdelane in objavljene leta 2007, se je želelo standardizirati načine zagotavljanja fizičnega in tehničnega varovanja prostorov in objektov na MO in v SV. To je že drugi poizkus, da se na MO na tem področju naredi red in da se to področje poenoti. Že leta 2001 se je namreč oblikovala posebna delovna skupina na MO, ki jo je vodil bivši državni sekretar Dušan Mikuž z namenom, da se uredi tehnično varovanje na ministrstvu kot celota. Delovna skupina je svoje delo končala leta 2004 s sprejetjem smernic, ki pa jih na žalost na ministrstvu nikoli nismo uspeli sprejeti v obliki ustreznega pravilnika.

5 UGOTAVLJANJE VZROKOV ZA RAZKRIVANJE TAJNIH PODATKOV MO

Zaradi pogostih primerov razkrivanja tajnih podatkov Ministrstva za obrambo v javnosti bodisi v tiskanih ali elektronskih medijih se je vodstvo ministrstva v letu 2007 odločilo, da se s pomočjo Ciljnega raziskovalnega projekta poizkuša ugotoviti, kateri so tisti vzroki, ki vodijo zaposlene k razkrivanju tajnih podatkov izven obrambnega sistema.

Podatki, ki so predstavljeni v nadaljevanju, so povzeti na podlagi dveh opravljenih anketiranj zaposlenih. Prvi anketni vprašalnik je bil razdeljen med zaposlene leta 2007 in naslednji leta 2009. Namen anketiranja je bil ugotoviti, kakšen odnos imajo zaposleni do tajnih podatkov, kakšen je njihov odnos do usposabljanj s področja tajnih podatkov ter kakšen odnos imajo zaposleni do oseb, ki razkrivajo podatke v javnosti, pišejo anonimke ter ali lahko govorimo, da imajo zaposleni izgrajen pravi odnos do varnega obravnavanja tajnih podatkov. Prva raziskava z naslovom »Organizacijska in varnostna kultura v MORS in SV« je bila izvedena v organizaciji Centra za politološke raziskave FDV iz Ljubljane.

Leta 2009 je bilo opravljeno ponovno anketiranje zaposlenih v okviru raziskave »Varnostna kultura in ravnanje s tajnimi podatki v MORS in SV«, ki sta jo opravila Fakulteta za varnostne vede Univerze v Mariboru in Center za politološke raziskave FDV Ljubljana.

V raziskavo leta 2007 je bilo zajetih 260 pripadnikov SV in 136 delavcev upravnega dela MO. Načrtovano je bilo, da bi bil vzorec v upravnem delu enak, torej 260, vendar je bilo za potrebe raziskave izpolnjenih in vrnjenih samo 136 vprašalnikov. Realizacija vzorca je bila torej samo 52,3 % anketirane populacije, kar nekako lahko štejemo, da vzorec še vedno zadostuje reprezentativnosti vzorca.

Leta 2009 je anketne vprašalnike izpolnilo 240 pripadnikov SV in samo 124 delavcev upravnega dela ministrstva. Težave so bile namreč pri vračanju vprašalnikov in nezainteresiranosti zaposlenih v upravnem delu MO.

V glavnem delu vprašalnika nas je zanimalo stališče zaposlenih v upravnem delu MO kot v SV glede varnostne kulture, osveščenosti zaposlenih do varovanja njim zaupanih podatkov kot tudi do ravnanja s tajnimi podatki.

O končnih rezultatih opravljene raziskave se je vedno obveščalo vodstvo ministrstva z vsemi zaključki in priporočili, kako stanje na tem področju izboljšati.

Velika večina anketirancev meni (Tabela 5), da so novo zaposleni, ki prihajajo v MO, dovolj varnostno osveščeni oz. da imajo dovolj visok nivo varnostne kulture (60 % v upravnem delu in 55 % v SV), zaskrbljuje pa ocena zaposlenih, da ta nivo ni dovolj visok, posebej je to izrazito v SV (45 %).

Tabela 2.1. Varnostna osveščenost novo sprejetih delavcev v MO (v %)

Ali so novo sprejeti delavci v vaši organizaciji po vašem mnenju dovolj varnostno osveščeni?	UPRAVNI DEL MO (N=134)	SV (N=254)
DA	59,0	54,7
NE	41,0	45,3
... če ne... zakaj (možnih več odgovorov)	(N=105)	(N=118)
a) ker ni v organizaciji nobenega varnostnega usposabljanja	28,2	28,0
b) ker ni v organizaciji nobenega usposabljanja glede ravnanja s tajnimi podatki	9,9	11,0
c) ker so v varnostnem sistemu pomanjkljivosti	43,7	50,0
d) ker varnostni organi niso dovolj usposobljeni	22,5	16,1
e) drugo	22,5	20,3

V naslednjem sklopu vprašanj je bilo anketirancem postavljeno vprašanje, kakšno stališče imajo zaposleni do svojih sodelavcev, ki zunaj ministrstva in SV razkrivajo tajne podatke.

Velika večina anketirancev tovrstna dejanja obsoja (75,6 % v MO in 70,6 % v SV), prepričljiva večina tovrstnih dejanj tudi ne razume. Pri tem vprašanju večjih razlik v stališčih zaposlenih med obema v anketo vključenima deloma Ministrstva za obrambo ni zaznati.

Tabela 5.2. Odnos anketirancev do sodelavcev, ki zunaj MO razkrivajo tajne podatke (v %)

	UPRAVNI DEL MORS	VOJAŠKI DEL MORS
(N=)	(172)	(252)
a) takšna dejanja obsojam in jih ne razumem	75,6	70,6
b) takšna dejanja obsojam, a jih razumem	19,2	21,4
c) takšnih dejanj ne obsojam in jih razumem	1,2	2,8
d) takšnih dejanj ne obsojam, a jih tudi ne razumem	4,1	5,2

Vprašanje: »Kakšen je vaš odnos do vaših sodelavcev, ki zunaj vaše organizacije razkrivajo tajne podatke?«

Zelo nas je zanimalo, kakšni so razlogi za razkrivanje tajnih podatkov izven Ministrstva za obrambo. Tudi pri tem vprašanju pomembnejših razlik med vojaškim in upravnim delom MO ni bilo zaznati; večina anketirancev meni, da je razkrivanje tajnih podatkov zunaj obrambnega sistema predvsem način izražanja nezadovoljstva posameznikov s sistemom, v katerem delajo, in njegovim delovanjem. Pet različnih vzrokov je bilo že podanih naprej.

Pri tem je mogoče ugotoviti, da reševanje problemov znotraj ministrstva in Slovenske vojske ni najbolj učinkovito, kar lepo razkriva tudi sklop vprašanj v razdelku o organizacijski kulturi.

Tabela 5.3. Razlogi za razkrivanje tajnih podatkov in zaupnih podatkov zunaj MO (v %)

	UPRAVNI DEL MORS	VOJAŠKI DEL MORS
(N=)	(174)	(257)
a) na ta način posamezniki izražajo nezadovoljstvo z organizacijo in njenim delovanjem	52,9	53,3
b) na ta način posamezniki izražajo nezadovoljstvo z načinom reševanja problemov znotraj organizacije	40,2	40,1
c) na ta način se posamezniki skušajo maščevati lastni organizaciji zaradi občutka krivice, ki da se jim je zgodila	40,8	39,3
d) na ta način skušajo posamezniki javnost opozoriti na nepravilnosti znotraj organizacije	42,0	38,9
e) na ta način želijo posamezniki pridobiti zase različne materialne koristi	27,6	16,0
f) drugo	7,5	9,3

Vprašanje: »Kakšni so po vašem mnenju razlogi, da nekateri zaposleni v vaši organizaciji zunaj organizacije razkrivajo tajne in zaupne podatke?«

Sklop vprašanj o razkrivanju tajnih podatkov Ministrstva za obrambo je bil zaključen s vprašanjem o anonimkah, ki so se v javnosti zelo pojavljala v obdobju od 2003 do 2008. V veliki večini so bile anonimke usmerjene bolj zoper posameznike znotraj obrambnega sistema kot pa zoper sam sistem.

Večina zaposlenih v obeh delih Ministrstva za obrambo meni, da reševanje notranjih težav in problemov preko anonimk za samo ministrstvo ni dobro; morda nekoliko preseneča »samo« **69,6 oziroma 74,6 % delež anketirancev, ki so izrazili jasno in nedvoumno stališče proti anonimkam kot orodju za reševanje notranjih težav v organizaciji.**

Splošno vprašanje glede stališča o anonimkah kot načina reševanja problemov v organizaciji je bil nato nadgrajeno še s podrobnejših vprašanjem glede razlogov, zaradi katerih se anonimke po mnenju anketirancev sploh pojavljajo.

V tem delu so odgovori zaposlenih uslužbencev in pripadnikov SV precej bolj diverzificirani; opazimo lahko tudi manjše razlike med vojaškim in upravnim delom MO. Zanimivo je, da si največji delež zaposlenih v obeh delih ministrstva razlaga anonimke kot sredstvo za izražanja nezadovoljstva z organizacijo in njenim delovanjem (46,8 %, oz. 52,7 %) in kot način **(legitimni) izražanja nezadovoljstva z načinom reševanja njihovih problemov znotraj ministrstva (42,2 % oz. 53,9 %)**. Nekoliko manjši pa je odstotek tistih zaposlenih, ki si anonimke razlagajo kot sredstvo, s katerim želijo posamezniki javnost opozoriti na nepravilnosti znotraj obrambnega sistema (36,4 oziroma 44,5 odstotka).

Tabela 5.4. Stališča posameznikov glede anonimk kot sredstva za reševanje notranjih težav in problemov v MO (v %)

Ali menite, da je reševanje notranjih težav in problemov v vaši organizaciji preko anonimk za vašo organizacijo dobro?	UPRAVNI MORS (N=173)	DEL	VOJAŠKI MORS (N=256)	DEL
DA	12,9		11,3	
NE	69,6		74,6	
NE VEM	17,5		14,1	
Zakaj se v vaši organizaciji po vašem mnenju pojavljajo anonimke?	UPRAVNI MORS (N=173)	DEL	VOJAŠKI MORS (N=256)	DEL
1. na ta način posamezniki izražajo nezadovoljstvo z organizacijo in njenim delovanjem	46,8		52,7	
2. na ta način posamezniki izražajo nezadovoljstvo z načinom reševanja problemov znotraj organizacije	42,2		53,9	

3. na ta način se posamezniki skušajo maščevati lastni organizaciji zaradi občutka krivice, ki da se jim je zgodila	29,5	40,6
4. na ta način skušajo posamezniki javnost opozoriti na nepravilnosti znotraj organizacije	36,4	44,5
5. na ta način skušajo posamezniki prikriti nekatera druga sporna dejanja v organizaciji	12,1	12,1
6. na ta način želijo posamezniki pridobiti zase različne materialne koristi	9,2	10,2
7. drugo	15,0	14,1

Pri drugem delu vprašanja so lahko anketiranci izbrali poljubno število ponujenih odgovorov, za katere so bili mnenja, da najbolje izražajo njihovo stališče.

Naslednji del vprašalnika o varnostni kulturi znotraj MO se je nanašal na ravnanje in usposabljanje z zaupnimi oziroma tajnimi podatki (Glej tabelo 10). Najprej je bilo zastavljeno splošno vprašanje glede njihove ocene ravnanja z zaupnimi dokumenti in podatki v varnostnem smislu v MO in SV.

Kot dobro oziroma odlično je omenjeno ravnanje ocenilo 65,1 % anketirancev iz upravnega dela MO in 69,9 % anketirancev iz Slovenske vojske. Gre za prepričljivo večino, seveda pa se ob tem postavlja resno vprašanje, ali je takšen odstotek za sistem, kot je MO, kjer se tajni dokumenti dnevno »proizvajajo«, obdelujejo in shranjujejo ter pošiljajo izven MO, res dober. Prej bi lahko ocenili, **da je to zaskrbljujoče.**

Tabela 5.5. Ocena ravnanja z zaupnimi dokumenti in podatki v varnostnem smislu v MO s strani zaposlenih (v %)

	UPRAVNI MORS	DEL	VOJAŠKI MORS	DEL
(N=)	(175)		(256)	

Nezadovoljivo	3,4	3,9
Zadovoljivo	26,3	21,5
Dobro	52,0	55,1
Odlično	13,1	14,8
Ne vem	5,1	4,7

Anketiranci so odgovarjali na vprašanje: »Kako ocenjujete ravnanje z zaupnimi dokumenti in podatki v varnostnem smislu v vaši organizaciji?«

Ob tem je bilo zaposlenim v MO zastavljeno še manjše podvprašanje, in sicer, ali menijo, da je neko temeljno znanje s področja varnostne kulture nujno potrebno vsem uslužbencem v celotni državni upravi. Zanimivo je, da so skoraj vsi vključeni uslužbenci upravnega dela MO (98,8 odstotka) na to vprašanje odgovorili pozitivno, enako pa meni tudi 92,6 odstotka anketirancev iz SV.

Po moji oceni pa je zaskrbljujoč podatek, da kar 7,4 odstotka anketirancev iz SV meni, da neko temeljno znanje s področja varnostne kulture ni nujno potrebno vsem uslužbencem v celotni državni upravi oz. v SV.

Tabela 5.6. Stališča glede usposabljanja glede ravnanja s tajnimi podatki (v %)

Ali ste vi osebno bili v času vašega delovanja v organizaciji vključeni v kakršnekoli oblike usposabljanja glede ravnanja s tajnimi podatki?	UPRAVNI DEL MORS (N=175)	VOJAŠKI DEL MORS (N=255)
DA	89,7	82,4
NE	8,6	15,3
NE VEM	1,7	2,4
Menite, da je tako izobraževanje za zaposlene v vaši organizaciji potrebno?	UPRAVNI DEL MORS (N=173)	VOJAŠKI DEL MORS (N=256)
DA	95,4	87,9
NE	1,7	8,2
NE VEM	2,9	3,9

Zanimalo nas je, ali so anketiranci že bili kdaj v času njihove kariere na MO udeleženi na katerem koli izobraževanju iz katerih koli vsebin varnostne kulture.

Velika večina (84,4 % anketirancev iz upravnega dela in 85,6 % anketirancev iz vojaškega dela MO) je na to vprašanje odgovorila pozitivno.

Večina anketirancev ima do usposabljanja s področja tajnih podatkov pozitivno mnenje in meni, da je tovrstno izobraževanje za zaposlene v MO tudi potrebno in nujno. Tudi tukaj pa se ponovno pojavlja majhna, a opazna manjšina znotraj vojske, saj 8,2 % anketiranih pripadnikov celo meni, da usposabljanje glede ravnanja s tajnimi podatki v MO in SV ni potrebno.

Zadnji del vprašanj o varnostni kulturi v MO pa se je nanašal na vprašanje nadzora in varovanja tajnih podatkov.

Najprej je bilo postavljeno vprašanje, ali obstaja v njihovi NOE nadzor nad ravnanjem s tajnimi in zaupnimi podatki; prepričljiva večina (89,3 % anketirancev iz upravnega in 86,9 % anketirancev iz vojske) pritrdi, da tovrsten nadzor obstaja. Manj prepričljivi pa so bili anketiranci pri odgovoru na vprašanje, kdo je pa v njihovi organizaciji resnično odgovoren za varovanje tajnih podatkov. Pri teh odgovorih pa je padel odstotek na 75,3 % anketirancev iz upravnega dela in 73,9 % anketirancev iz vojske.

Podobno je bilo pri vprašanju, ali je v njihovi organizacijski enoti izdelan načrt varovanja tajnih podatkov. Večina anketirancev je na omenjeno vprašanje sicer odgovorila, dejstvo, da več kot tretjina, **37,2 % anketirancev** v upravnem delu in še zlasti **32,4 % anketirancev iz vojske**, z obstojem načrta varovanja tajnih podatkov sploh ni seznanjena, kar pa je več kot zaskrbljujoče.

Na podlagi tega je mogoče oceniti, da v sistemu varovanja tajnih podatkov, tako v upravnem delu kot v vojski, precej stvari manjka. Gre za to, da načrti varovanj tajnih podatkov v vseh sredinah v MO niso dobro izdelani, bodisi zaposleni niso seznanjeni z določili o varovanju podatkov v njihovih sredinah. Če bi bili seznanjeni, bi moral biti odstotek odgovorov precej višji. Ocenjujem, da na podlagi tega zaposleni v obeh delih ministrstva sploh ne vedo, kdo je načrt varovanja v njihovi NOE pripravil, niti kaj je v njem zapisano. V skladu s predpisi pa bi morali biti načrti za varovanje TP narejeni najkasneje do junija 2006.

Tabela 5.7. Stališča glede načrta varovanja tajnih podatkov I. (v %)

Ali je v vaši organizacijski enoti izdelan načrt varovanja tajnih podatkov?	UPRAVNI MORS (N=172)	DEL VOJAŠKI DEL MORS (N=250)
DA	59,3	64,4
NE	3,5	3,2
NE VEM, NISEM SEZNANJEN	37,2	32,4

...če da... Ali ste tudi vi osebno sodelovali pri izdelavi oz. pripravi tega načrta?	UPRAVNI DEL MORS (N=101)	VOJAŠKI DEL MORS (N=163)
DA	17,8	10,4
NE	82,2	89,6

Na drugi del vprašanja so odgovarjali samo anketiranci, ki so na prvi del vprašanja odgovorili z »da«.

Pri pripravi vprašanja na tem področju smo nekako tovrstne odgovore že predvidevali oziroma smo se jih bali. Zato se je v vprašalniku anketirancem zastavilo še eno vprašanje, ki pa ni merilo njihovih stališč, pač pa njihovo znanje s tega področja.

Vprašani so bili glede tega, kaj vse vsebuje načrt varovanja tajnih podatkov (glej Tabelo 12). Ponujeno jim je bilo šest možnih sestavnih delov, od katerih štirje dejansko odražajo elemente načrta varovanja tajnih podatkov, dva odgovora pa smo si izmislili in sta torej nepravilna (odgovora 3 in 5 v Tabeli 12).

Kot vidimo iz podatkov v spodnji razpredelnici, 28,9 odstotka anketirancev iz upravnega in 20,6 odstotka anketirancev iz SV ne pozna oziroma ni seznanjenih z načrtom varovanja tajnih podatkov in na vprašanje niso odgovarjali.

Ugotovimo lahko, da je zaskrbljujoč delež zaposlenih v MO, ki ne poznajo sestavnih delov načrta varovanja tajnih podatkov, kar ob prej navedenih dejstvih in deležu tistih, ki z načrtom že v osnovi sploh niso seznanjeni, ni tako presenetljivo, je pa zaskrbljujoče.

Pri tem vprašanju lahko opazimo tudi nekoliko bolj opazno razliko med upravnim delom in SV. Dejstvo je, da je poznavanje tematike s področja tajnih podatkov v upravnem delu slabše kot v Slovenski vojski, kjer prav tako obstajajo dobre štiri desetine anketirancev, ki načrta varovanja tajnih podatkov oziroma povedano bolj natančno, njegove vsebine, sploh ne poznajo.

Tabela 5.8. Stališča glede načrta varovanja tajnih podatkov II. (v %)

Načrt varovanja tajnih podatkov v organizacijski enoti vsebuje ...	UPRAVNI DEL MORS (N=125)	VOJAŠKI DEL MORS (N=253)
1. oceno ogroženosti objekta	47,2	57,4
2. ukrepe tehničnega varovanja ob sprožitvi alarma v objektu	51,2	53,9
3. izdelavo načrta varovanja, kar je naloga predstojnika organa (ki je tudi nosilec načrta varovanja)	52,0	45,1
4. posebni del ukrepov za zaščito tajnih podatkov	53,6	55,4
5. pravno osnovo za izdelavo načrta varovanja (ki je v Zakonu o obrambi)	40,0	37,3
6. ukrep, da se z ukrepi in postopki varovanja tajnih podatkov morajo seznaniti vsi zaposleni v organu ali enoti	60,8	64,2
7. ne poznam, ne vem	28,9	20,6

Pri tem vprašanju so lahko anketiranci izbrali poljubno število ponujenih odgovorov, za katere so bili mnenja, da so pravilni.

Na koncu tega dela vprašalnika pa so bili anketiranci vprašani, ali morda osebno vedo za kakšen primer sankcioniranja v primeru kršitev varovanja podatkov v njihovi organizaciji.

Na to vprašanje je pozitivno odgovorilo 13,5 odstotka anketirancev iz vojaškega in prav tolikšen delež anketirancev iz upravnega dela MO.

5.1 Anketiranje zaposlenih v ministrstvu leta 2013

Na podlagi predhodno izvedenih anket med zaposlenimi v upravnem delu ministrstva in v SV v letih 2007 in 2009 se je leta 2013 ponovno preučevalo nekatere vidike varnostne kulture in varovanja tajnih podatkov v ministrstvu. Glede na predhodne anketne vprašalnike je bilo več kot 85 % vprašanj v anketnem vprašalniku leta 2013 enakih kot leta 2007 in 2009. Leta 2013 so bila med vprašanja dodana še vprašanja o zaščiti kritične infrastrukture v R Sloveniji, predvsem, kako jo zaposleni v MO in SV dojemajo in razumejo.

Pri izvedbi anketiranja zaposlenih leta 2013 je potrebno omeniti še eno omejitev. Kljub temu, da je ministrstvo zagotovilo finančna sredstva za izvedbo anketiranja, je prišlo v fazi razdeljevanja in izpolnjevanja vprašalnikov v SV do težav. Posamezni visoki častniki na Generalštabu SV so se kljub ukazu načelnika uprli in vprašalnikov niso želeli razdeliti med pripadnike SV, da bi jih izpolnili. Z veliko prepričevanja in dogovarjanji je bilo nato od skupaj 200 vprašalnikov vrnjenih komaj 67. Zaradi tega nekaterih odgovorov iz SV ni mogoče primerjati z odgovori iz let 2007 in 2009.

Podatki iz let 2007 in 2009 so pokazali, da je obstajalo razkrivanje tajnih podatkov v javnosti, predvsem način izražanja nezadovoljstva posameznikov z organizacijo - ministrstvom in načinom funkcioniranja in delovanja. Pri podatkih iz vprašalnikov leta 2013 pa so v ospredje prišli povsem novi razlogi za odtekanje tajnih podatkov v javnost. Na podlagi podatkov je mogoče ugotoviti, da sta se pokazala dva nova vzroka razkrivanja tajnosti v javnosti: opozoriti javnost na nepravilnosti znotraj ministrstva ter maščevanje vodstvu ministrstva zaradi občutka krivice, ki ga je ministrstvo kot sistem povzročilo posamezniku.

Podatki iz leta 2013 kažejo, da je mogoče zaznati močno nezadovoljstvo, predvsem zaradi politike zategovanja pasu. Plača kot zunanji motivacijski dejavnik je zamrznjena, torej zaposleni v ministrstvu iščejo uteho v drugih motivacijskih dejavnikih. Pri izvedbi predhodnih dveh anketnih vprašalnikov je bilo veliko poudarka namenjenega sistemu napredovanj v ministrstvu kot zunanjemu motivacijskemu faktorju zaposlenih.

Podatki iz anketnega vprašalnika so še pokazali, da so zaposleni na ministrstvu dobro varnostno osveščeni, zavedajo se pomembnosti varovanja tajnih podatkov ter

pomembnosti nenehnega izobraževanja na tem področju, saj se na ta način dviguje nivo varnostne kulture pri vsakem zaposlenem v ministrstvu.

6 VREDNOTENJE PODATKOV IZ ANKETNIH VPRAŠALNIKOV

Kot je že bilo zapisano v enem od predhodnih poglavij, je bil namen anketiranja zaposlenih v upravnem delu ministrstva in v Slovenski vojski ugotavljati osveščenost zaposlenih za pravilno in varno ravnanje s tajnimi podatki, poizkušati ugotoviti vzroke za odtekanje in razkrivanje tajnih podatkov v javnosti, ugotavljati stopnjo varnostne kulture pri zaposlenih in ugotavljati, ali so zaposleni zadovoljni z izobraževanji, ki jim ga ministrstvo omogoča na področju varovanja tajnih podatkov.

Gotovo je, da mora vsakokratna vodilna ekipa na ministrstvu nameniti precej naporov, da se izboljša varnostna osveščenost in usposobljenost vseh novo zaposlenih delavcev v ministrstvu. Posebej zaskrbljujoča je ta osveščenost v vojaškem delu oz. v Slovenski vojski. Ob tem bi veljalo razmisliti, da se ponovno uvedejo t. i. uvajalni seminarji za vse novo zaposlene, kar se je v ministrstvu že izvajalo predvsem v začetnem obdobju, od leta 1992 do 1997.

Vodstvo ministrstva se mora dobro zavedati, da je razkrivanje tajnih oziroma zaupnih podatkov izven ministrstva, v javnosti, odraz oziroma reakcija zaposlenih na nesposobnost oziroma nepripravljenost vodstva ministrstva, da bi rešilo probleme, ki nastajajo v obrambnem sistemu.

Na podlagi podatkov, pridobljenih iz anketnih vprašalnikov, je mogoče ugotoviti, da ravnanje s tajnimi podatki v ministrstvu v obdobju od 2007 do 2013 ni bilo na ustreznem nivoju. Ugotoviti je mogoče vrsto pomanjkljivosti, od izvajanja usposabljanja za ravnanje s tajnimi podatki do izvajanja nadzora nad določanjem, obravnavanjem in hranjenjem tajnih podatkov. Po mojem mnenju se bo moralo razmisliti o spremembah na organizacijskem nivoju, kot tudi pri številu pooblaščenih oseb za določanje stopenj tajnosti podatkov in obdelovanju tajnih podatkov. Kljub dejstvu, da je bila večina zaposlenih že na kakšnem usposabljanju s področja TP, se stanje ne izboljšuje, nasprotno, mesečno pojavljanje tajnih podatkov ministrstva v javnosti kaže na to, da se stanje ne izboljšuje.

Da bi se zagotovila večja kontrola nad številom oseb, ki imajo pooblastilo za določanje tajnih podatkov, bi bilo potrebno resno razmisliti, ali je tako širok krog oseb, ki imajo sedaj to pooblastilo, res najboljši. Po trenutno veljavnem predpisu (Pravilniku) je po moji oceni teh oseb v ministrstvu in SV preko 50. Vsaka od teh oseb ima različno prakso in pristop k določanju stopenj tajnosti, vsaka od teh oseb je šla skozi različne faze usposabljanja na področju TP. Zaradi tega še toliko bolj prihaja do izraza subjektivna ocena vsakega posameznika, ko se odloča, ali bo nek podatek, informacijo določil kot INTERNI ali ZAUPNI tajni podatek.

Na tem področju vsekakor manjka jasno navodilo za določanje stopenj tajnosti oz. kriteriji, po katerih bi lahko vsak posameznik – originator tajnih podatkov – lažje določal stopnje tajnosti podatkom oz. informacijam.

7 SKLEP

Zadnje poglavje magistrskega dela je namenjeno sklepu, ki na podlagi uvodnih dveh raziskovalnih vprašanj nakazuje odgovore na vprašanje, ali je visoka stopnje varnostne kulture zaposlenih zagotovilo za dobro varovanje tajnih podatkov s katerimi delajo ter ali se lahko z enotnim sistemom usposabljanja zagotovi višji novo stopnje varovanja tajnih podatkov.

S svojim delom sem želel preko analize nacionalnovarnostnega sistema varovanja tajnih podatkov ter preko analize podsistema varovanja tajnih podatkov na Ministrstvu za obrambo ugotoviti, ali se razkrivanje teh podatkov v javnosti dogaja zaradi nizke stopnje varnostne kulture ali zaradi nezadostnega usposabljanja zaposlenih za varovanje tajnih podatkov.

Pri analizi nacionalnovarnostnega sistema ni bilo ugotovljenih posebnosti, ki bi kazale, da naš zakonski in podzakonski okvir varnostnega preverjanja in dostopanja do tajnih podatkov, odstopa od rešitev drugih držav v NATO in EU. Ugotovljeno je bilo, da je naš sistem glede varovanja človekovih pravic, bolj temeljit in v primerjavi z drugimi sistemi v Evropi, zagotavlja visoko stopnjo varovanja človekovih pravic. Vsi zaposleni, ki želijo dobiti dovoljenje za dostop do tajnih podatkov imajo v postopku izdaje dovoljenja veliko možnosti, da preverijo ali so njihove pravice zavarovane in ali organi, ki jih preverjajo ravnaajo ustrezno z njihovimi podatki. Ne nazadnje imajo možnost sprožiti postopke na sodišču, če menijo, da je bila njihova zahteva za izdajo dovoljenja, neupravičeno zavrnjena.

V sojem delu sem posebej izpostavil vlogo in pomen nacionalnega varnostnega organa – UVTP. Menim, da se v okviru nacionalnovarnostnega sistema preverjanja za dostop do tajnih podatkov ne upoštevajo dovolj naloge, ki jih ima UVTP v skladu z zakonom. Menim, da je UVTP-ju potrebno dati bistveno večjo vlogo in pomen, kot jo ima sedaj. Za večji pomen in vlogo UVTP-ja lahko veliko naredi tudi samo vodstvo urada z večjim proaktivnim delovanjem med vsemi organi, ki izvajajo varnostno preverjanje v R Sloveniji. V delovanju urada je trenutno vse preveč »birokratskega« delovanja.

Pri analizi delovanja podsistem nacionalnega sistema varovanja tajnih podatkov na ministrstvu sem ugotovil, da pravilnik o varovanju tajnih podatkov, dovolj dobro povzema krovni zakon o tajnih podatkih in podzakonske predpise. Bistvo pravilnika je v določitvi organa - OVS, ki izvaja varnostno preverjanje in odgovornost za varovanje enotnega sistema tajnih podatkov na ministrstvu. Kot eno od bistvenih sestavin tega enotnega sistema varovanja podatkov so določbe glede osnovnega in dodatnega usposabljanja zaposlenih na ministrstvu. Korektivni element vodstva ministrstva na tem področju so tematski nadzori na področju tajnih podatkov, ki pa se lahko, po trenutnih določbah pravilnika opravljajo, samo v upravnem delu ministrstva. To je po moji oceni nevzdržno, ker se na ta način ruši enoten sistem varovanja tajnih podatkov na celotnem ministrstvu. Če ne obstaja enoten način usposabljanja in nadzora nad tajnimi podatki (določanjem, dostopanjem, varovanjem, uničevanjem), potem lahko v sistemu prihaja do »razpok«, katere so lahko manifestirajo tudi v odtekanju oz. razkrivanju podatkov ministrstva v javnosti.

V zadnjem delu svojega magistrskega dela so podrobneje predstavljenim rezultate anketnih vprašalnikov, ki so jih o tajnih podatkih, anonimkah in varnostni kulturi zaposleni v upravnem delu in SV izpolnjevali v letih 2007, 2009 in 2013.

Podatki analize vprašalnikov kažejo zanimive odgovore zaposlenih v upravnem delu in SV, posebej glede razkrivanja tajnih podatkov ministrstva v javnosti. Posebej zanimivi so odgovori glede vzrokov razkrivanja tajnih podatkov v javnosti, ki so pojasnjeni v nadaljevanju. Ugotavljam, da varnostna kultura in usposabljanje za varovanje tajnih podatkov nimata veliko vpliva na odtekanje podatkov izven ministrstva. Vzroki za takšna »deviantna« ravnanja zaposlenih, so na podlagi podatkov iz vprašalnikov, drugje. Podatki kažejo, da gre pri razkrivanju podatkov za neko vrsto maščevanje zaposlenih do obrambnega sistema.

7.1. Verifikacija raziskovalnih vprašanj

Prvo raziskovalno vprašanje magistrskega dela je: **»Visoka stopnja varnostne kulture pri zaposlenih pozitivno vpliva na varovanje tajnih podatkov«.**

V teoretičnem delu magistrskega dela sem opredelil teoretična izhodišča o varnostni kulturi. Dejstvo je, da varnostne kulture ni mogoče enoznačno oceniti samo z ocenami od 1 do 10. Lahko pa rečemo, da ima neka oseba nizko ali visoko stopnjo varnostne kulture, predvsem glede na to, kako ravna s tajnimi podatki, ki so ji zaupani. Na podlagi teoretičnih spoznanj in mnenj različnih avtorjev je varnostno kulturo mogoče razumeti kot skupen nabor različnih idej, norm in praks, ki služijo za povečanje varnosti države.

Da bi potrdil ali ovrgel raziskovalno vprašanje, ki sem ga postavil na pričetku tega magistrskega dela, sem si pomagal s podatki iz anketnih vprašalnikov.

Zaposlenim v MO in SV je bilo zastavljeno vprašanje, kako ocenjujejo, ali so novo zaposleni delavci in pripadniki dovolj varnostno osveščeni in imajo dovolj visok nivo varnostne kulture. Zaposleni v MO so pozitivno odgovorili s 60 %, medtem ko je bilo takšnih odgovorov v SV 47 %. Kar 41 % v MO in 45 % v SV pa jih je odgovorilo, da niso dovolj usposobljeni oz. nimajo dovolj varnostne kulture. Ko pa so zaposleni in pripadniki SV odgovarjali, zakaj delavci niso dovolj varnostno osveščeni in nimajo varnostne kulture, pa je kar 50 % pripadnikov SV in 43 % zaposlenih v MO odgovorilo, da so v varnostnem sistemu pomanjkljivosti. Zanimivo je, da so zaposleni v MO in pripadniki SV navedli še, da varnostni organi, ki so odgovorni za varnost sistema tajnih podatkov, niso dovolj usposobljeni. O tem je prepričanih 22 % zaposlenih v MO in 16 % pripadnikov SV.

Problematika razkrivanja tajnih podatkov ministrstva v javnosti je bila zajeta v vprašanju o razlogih za razkrivanje tajnih podatkov izven organizacije. Pri tem je pomembno poudariti, da so bili v tem delu odgovori zaposlenih v MO in pripadnikov SV, skoraj enaki. Kar 53 % odgovorov v MO in SV je bilo, da na ta način posamezniki izražajo nezadovoljstvo z ministrstvom in njenim delom. Dobrih 40 % anketirancev v MO in SV je odgovorilo, da na ta način posamezniki izražajo nezadovoljstvo z načinom reševanja problemov znotraj organizacije. Enak odstotek anketirancev pa je menil,

tako v MO kot v SV, da se na ta način posamezniki maščujejo ministrstvu, ker so se jim znotraj sistema zgodile krivice.

Na podlagi teoretičnih spoznanj in rezultatov, pridobljenih na podlagi izvedenih anketnih vprašalnikov, ugotavljam, da ni vzročne povezave med visoko stopnjo varnostne kulture in visoko stopnja varovanja tajnih podatkov v ministrstvu. Podatki iz vprašalnikov so namreč pokazali, da se tajni podatki razkrivajo zaradi povsem drugih razlogov in varnostna kultura posameznika pri problemu razkrivanja podatkov v javnosti, ne igra pomembne vloge.

Drugo raziskovalno vprašanje je bilo: **»Samo enoten sistem usposabljanja, nadzora in kontrole nad tajnimi podatki v organizaciji lahko zagotovi višji nivo stopnje varovanja tajnih podatkov«.**

Na podlagi Zakona o tajnih podatkih in uredbe o varovanju tajnih podatkov je v ministrstvu sprejet pravilnika o varovanju tajnih podatkov na MO. Ocenilo se je, da se lahko učinkovitost sistema varovanja tajnih podatkov zagotavlja samo preko nadzora nad usposobljenostjo zaposlenih za varovanje in ravnanje s tajnimi podatki.

Ali kot sta zapisala Prezelj in Tarman »za učinkovitost delovanja sistema varovanja tajnih podatkov je ključen inšpekcijski nadzor, ki ugotavlja odklone od predvidene zaščite in nalaga popravke kot sistemski korekcijski mehanizem.«

Za izvajanje inšpekcijskega nadzora nad tajnimi podatki v Ministrstvu za obrambo je zadolžen Inšpektorat Republike Slovenije za obrambo – IRSO. Za tematske nadzore nad tajnimi podatki je zadolžena OVS, ki te tematske nadzore izvaja od leta 2008 dalje, ko je bil sprejet prvi pravilnik.

Vendar pa se na podlagi določil 5. člena pravilnika tematski nadzori opravljajo samo v upravnem delu. Tematske nadzore v SV opravljajo pripadniki štabno-varnostnega organa. Pri tem se resno zastavlja vprašanje, na kakšen način so pripadniki štabno-varnostnega organa pridobili potrebne izkušnje za izvajanje tematskih nadzorov. Če pa že izvajajo nadzori, ni poznano, kakšni so rezultati nadzorov.

Pri izvajanju anketnih vprašalnikov med zaposlenimi v MO in SV sem želel ugotoviti, kakšna so stališča zaposlenih glede usposabljanja za ravnanje s tajnimi podatki. Velike razlike med odgovori zaposlenih v MO in SV ni. Da je to usposabljanje potrebno, je odgovorilo kar 90 % anketirancev v MO in 83 % v SV. Na dodatno vprašanje, ali ocenjujejo, da je to izobraževanje potrebno, se jih je 95 % v MO s tem strinjalo, v SV pa 88 %. Se pa pojavlja zaskrbljujoč podatek, da kar 8 % zaposlenih v SV ocenjuje, da tovrstno izobraževanje zanje ni potrebno.

Tudi glede ocene, ali se v obrambnem sistemu dobro ravna z zaupnimi dokumenti in podatki, se ne pojavljajo večje razlike. Tako se s trditvijo, da se s tajnimi podatki ravna dobro oz. odlično, strinja 65 % anketirancev v MO in 69 % v SV. Da je stanje na tem področju zadovoljivo, je ocenilo 26 % anketirancev v MO in 21 % v SV. Zanimivo pa je, da je odstotek anketirancev, ki ocenjujejo, da je stanje nezadovoljivo, v SV večji, 4 %, kot pa v MO, 3 %.

Na podlagi analize pravilnika o varovanju tajnih podatkov, ugotavljam da na ministrstvu ne moremo govoriti o enotnem sistemu izvajanja osnovnega in dodatnega usposabljanja zaposlenih na področju tajnih podatkov. OVS izvaja tovrstna usposabljanja samo za zaposlene v upravnem delu, medtem ko tovrstna usposabljanja v SV izvajajo štabno-varnostni organi. Na podlagi lastnih izkušenj, lahko zatrdim, da se v SV izvajajo samo osnovna usposabljanja, dodatnih usposabljanj na področju tajnih podatkov ne izvajajo.

Na podlagi vseh teoretičnih spoznanj in podatkov iz opravljenih anketnih vprašalnikov ocenjujem, da je za sistem varovanja tajnih podatkov na ministrstvu najpomembneje, da so zaposleni, kot bistveni element tega sistema, enotno usposobljeni. Samo dobro in na enak način usposobljeni zaposleni, tako v upravnem kot vojaškem delu so zagotovilo za učinkovit sistem varovanja tajnih podatkov na ministrstvu. Za preverjanje, kako učinkovit in zanesljiv je ta sistem pa je bistveno, da se nad njim izvaja enoten nadzor, bodisi inšpekcijski ali nadzori v obliki tematskih nadzorov.

Zato ocenjujem, da se na podlagi podatkov z vprašalnikov lahko strinjam, da samo enoten sistem usposabljanja, zagotavlja višji nivo varovanja tajnih podatkov. K temu

lahko veliko pripomore tudi enoten nadzor. Na ta način ugotavljam, da je drugo raziskovalno vprašanje potrjeno.

Na koncu želim posebej poudariti, da na podlagi preučitev teoretičnih spoznaj, veljavnih normativnih aktov in na podlagi lastnih izkušenj, v Ministrstvu za obrambo ne obstaja enoten sistem varovanja tajnih podatkov, ter da je mogoče v tem potrebno verjetno iskati vzroke, da tajni podatki ministrstva odtekajo v javnost. Na ta način se celotnemu sistemu varovanja tajnih podatkov, povzroča velika škoda. V mednarodnem okolju pa zaradi tega verjetno izgubljam verodostojnost in kredibilnost. Pa ne samo Ministrstvo za obrambo, tudi R Slovenija.

8 LITERATURA

Almond, G. in Sigmund V. 1963. *The Civic Culture: Political Attitudes and Democracy in Five nations*, Princeton.

Anžič, A. 2002. *Mednarodni terorizem - varnostni izziv in dileme. Teorija in praksa*, 39 (2): 454.

Ambrož, M. 1999. *Varnostna kultura*. Ljubljana. Visoka policijsko varnostna šola.

Antončič, M. 2003. *Dostop do informacij javnega značaja in tajni podatki. Kaj prinaša novi zakon o dostopu do informacij javnega značaja*. Ljubljana. Inštitut za javno upravo, Ministrstvo za informacijsko družbo, Ministrstvo za notranje zadeve.

Baylis, Smith and Owens 2008. *The Globalization of World Politics*, Oxford Univessity Press.

Brezovšek, M. in Haček, M. 2003. *Globalizacija in državna uprava*. Ljubljana. Fakulteta za družbene vede.

Brezovšek, M. Črnčec, D. 2007. *Demokratska uprava in tajnost podatkov*. Ljubljana. Fakulteta za družbene vede.

----- 2010. *Demokratska uprava in tajnost podatkov*. Druga dopolnjena izdaja. Ljubljana. Fakulteta za družbene vede.

Brezovšek, M., Haček, M., Zver, M. 2007. *Democratic praxis in Slovenia*; Vydavetelstvi a nakladatelstvi . Aleš černek, s.r.o. Plzen.

Brown, A. 1998. *Organizational culture*. Prentice Hall, London.

Caporaso, J. 1988. *The Elusive State*. Sage, Newbury Park.

Čaleta, D. 2004. *Sistem varovanja tajnih podatkov*. Magistrsko delo. Ljubljana. FPDEŠ.

----- 2004. *Dileme varovanja tajnosti v demokratični družbi*. Dignitas 21/22-

----- 2008. *Varovanje tajnih podatkov v demokratični družbi*. Dignitas. 37/38.

Dimitrovski, M. 2016. *Omejitve zaposlovanja v javni upravi na primeru sodelovanja v ekstremističnih skupinah*. (magistrsko delo) Ljubljana. Fakulteta za upravo.

Dravec, A. 2009. *Varovanje tajnih podatkov v Republiki Sloveniji: formalni vidiki vs praksa*. Ljubljana. Fakulteta za družbene vede.

Dunivin, K.O. 1994. *Military culture. Change and Continuity*. Armed Forces and Society 30 (4).

English, A.D. 2004. *Understanding military culture: A Canadian perspective*. McGill-Queen s University Press Montreal.

Franz, H.J. 1995. *Med organizacijska ureditev in koordinacija na ravni politike*. ur. E. Pusić, E. Zagreb. Naprijed. *Upravna znanost: izbor del*.

Grizold, A. ur. 1992. *Razpotja nacionalne varnosti*. Ljubljana. Fakulteta za družbene vede.

----- ur. 1998. *Perspektive sodobne varnosti*. Ljubljana. Fakulteta za družbene vede.

----- 2001. *Nekaj izzivov v izgradnji varnostne arhitekture v Evropi danes*. 38, (1): 786-797.

Grizold, A. in Andrej, A. 1997. *Varnostni sistem Republike Slovenije*. Ljubljana. Uradni list Republike Slovenije.

Haacke, J. 2003. *ASEAN s diplomatic and security culture*. Routledge Curzon, London and New York.

Harrison, L. in Huntington, S.P. ur. *Culture matters . how values shape human progres*. New York. Basic books.

Jelušič, L. 1992. *Legitimnost vojaštva v sodobni družbi*. Doktorska disertacija. Ljubljana. Fakulteta za družbene vede.

Ji Yon. 2004. *Nationalism, the Cinese defence culture and the PLA*. V: Nationalism, democracy and national intergration in China (ur) Shaoguang Liew, Leong H. in Wang, Routled Curzon, London and New York. 247-261.

Kotnik-Dvojmoč, I. 2000. *Preoblikovanje oboroženih sil sodobnih evropskih držav: (študija primera Slovenije)*. Doktorska disertacija. Ljubljana. Fakulteta za družbene vede.

Kovačević, A. 2013. *Princip »need to know«*. Diplomsko delo. Maribor. Fakulteta za varnostne vede.

Krause, K. ur. 1998. *Culture and security: multilateralism, arms control, and security building*. Portland. Frank Cass.

Luhmann, Niklas 1998. *Teorija sistema*. Beograd..Platon.

Martin, J. 2002. *Organizational culture*. Mapping the Terrain. San Francisco. Sage Publications inc.

Mesarec, B. 2012. *Varnost in policijsko delo, Varovanje tajnih podatkov*. Maribor. Fakulteta za varnostne vede.

Mesner-Andolšek, D. 1995a. *Organizacijska kultura*. Ljubljana. Gospodarski vestnik.

Mitar, M. in Sotlar, A. ur. 1998. *Nacionalna varnost in med etični konflikti v Republiki Sloveniji*. Zbornik raziskovalnega projekta. Ljubljana. Visoka policijsko-varnostna šola,

Pravilnik o varovanju tajnih podatkov na Ministrstvu za obrambo, (šifra 0070-5/2006-4 z dne 21.2. 2006, šifra 0070-5/2006-30 z dne 31.8.2006, šifra 0070-22/2008-26 z dne 11.6.2008, šifra 0070-10/2010-10 z dne 19.8.2011, šifra 0070-26/2012-4 z dne 6.4. 2012).

Prezelj, I. in Grizold, A. 2015. *Razmerje med tajnostjo in javnostjo nacionalno varnostnih podatkov v sodobni demokratični družbi*, *Teorija in praksa* 4(15) Ljubljana. Fakulteta za družbene vede.

Prezelj, I. Tarman, M. 2015. *Sistem varovanja tajnih podatkov v Republiki Sloveniji v luči demokratičnega zagotavljanja nacionalne varnost*, *Teorija in praksa* 4(15) Ljubljana. Fakulteta za družbene vede.

Rančigaj, K.. 2010. *Informacijska varnostna kultura v državni upravi*. Magistrsko delo. Ljubljana. Fakulteta za družbene vede.

Raziskava »Organizacijska in varnostna kultura v MORS in SV« 2007. Ljubljana. Fakulteta za družbene vede, Center za politološke raziskave.

Raziskava »Varnostna kultura in ravnanje s tajnimi podatki v MORS in SV«, 2009. Ljubljana. Fakulteta za družbene vede, Center za politološke raziskave in Univerza v Mariboru, Fakulteta za varnostne vede.

Raziskava: »Varnostna kultura, varovanje tajnih podatkov in zaščita kritične infrastrukture v MO in SV« 2013. Nova gorica. Fakulteta za uporabne družbene študije.

Rizman, R. 2000. *Nacionalna država, suverenost in identiteta v času globalizacije*. *Revija 200*, št. 127/128, str. 177-189.

Robertson, R. 1992. *Globalization*, London..Sage.

Schein, E.H. 1994. *Organizational culture*. Illinois. Inc. Burr Ridge.

Schein, E.H. 1995. *Organizational culture and leadership*. San Francisco. Joshep bass.

Sklep o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja, Ur. I. RS 94/2006.

Slovar Slovenskega Knjižnega jezika, dostopno na www.sskj.si.

Trbovšek F. 2001. *Varnostno preverjanje oseb – omejitev dostopa do tajnih podatkov*. Ljubljana. Varstvoslovje 1-2.

Vah, I. 2003. *Vrednotenje evropske varnostne in obrambne politike*. Magistrsko delo. Ljubljana. Fakulteta za družbene vede.

Uredba o varovanju tajnih podatkov, Ur. I. RS 74/2005 in Spremembe uredbe o varovanju tajnih podatkov, Ur. I. RS 7/2011 in 24/2011.

Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov: Ur. I. RS 71/2006 in 138/2006.

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih: Ur. I. RS 48/2007.

Uredba o načinu in postopku ugotavljanja pogojev za izdajo varnostnega dovoljenja organizaciji: Ur. I. RS 70/2007.

Uredba o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisov izdanih na njegovi podlagi: Ur. list št. 94/2006.

Wallce, A.F.C. 1968. *Culture and personality*. New York. Random House.

Weber, M. 1987. Birokracija. V: Durić, M., Sociologija Maxa Webra, Naprijed, Zagreb.

Zakon o obrambi (ZObr-UPB2) Ur. l. RS. 103/2004, 23.9.2004.

Zakon o medijih (Zmed-UPB1) Ur. l. RS 110/2006, 26.10.2006.

Zakon o tajnih podatkih (ZTP-UPB1) Ur. l. RS 50/2006, 16.5.2006.

Zakon o dostopu do informacij javnega značaja, (ZDIJZ-UPB2), Ur. l. RS 51/2002, 18.5.2006.

Navodilo za delo s tajnimi podatki NATO in EU, izdal UVTP št. 02239-3/2009/28 z dne 4.6.2009.

PRILOGE

ANKETNI VPRAŠALNIK

9 PRILOGA 1 - VPRAŠALNIK ZA UPRAVNI / VOJAŠKI DEL MORS

ORGANIZACIJSKA IN VARNOSTNA KULTURA V MINISTRSTVU ZA OBRAMBO RS / SLOVENSKI VOJSKI

VPRAŠALNIK ZA UPRAVNI / VOJAŠKI DEL MORS

Vprašalnik, ki ga imate pred seboj, je razdeljen na štiri dele. **Prvi del in drugi del vprašalnika (A in B)** sestavljajo trditve in stališča, ki se nanašajo na **Vašo organizacijo** in organizacijsko kulturo v Vaši organizaciji. Prosim Vas, da se glede vsake trditve posamično opredelite, v kolikšni meri ta trditev drži oziroma ne drži za Vašo organizacijo in zaposlene v Vaši organizaciji. **Tretji del vprašalnika (C)** vsebuje različna vprašanja, ki so povezana s področjem varnostne kulture tako v upravnem kot tudi v vojaškem delu Ministrstva za obrambo RS. **Četrty del vprašalnika (D)** sestavljajo nekateri osebni podatki, ki jih potrebujemo v nadaljnjih analizah in ki ne bodo razkriti.

Prosim Vas, da preberete vsa vprašanja in odgovore, ter se odločite za tisti odgovor, ki bo najbolje predstavljal Vaše osebno mnenje ali najbolje opisoval stanje v organizaciji, v kateri ste zaposleni. Če niste povsem prepričani, izberite odgovor, za katerega mislite, da je najustreznejši, ter nadaljujte z naslednjim vprašanjem.

Zahvaljujemo se Vam za Vaš trud, ki ga boste vložili v izpolnjevanje tega vprašalnika.

RAZDELEK A: DIAGNOSTICIRANJE ORGANIZACIJSKE KULTURE
(STRUKTURIRANI VPRAŠALNIK)

Št.	Usmeritve in stališča	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
1	Kreativnost in inovacije				
1-1	Zaposleni v naši organizaciji so večinoma iznajdljivi pri opravljanju svojega dela	3	2	1	0
1-2	V naši organizaciji so nove ideje vedno dobrodošle	3	2	1	0
1-3	Inovativni ljudje so v naši organizaciji vedno dobrodošli in cenjeni	3	2	1	0
1-4	Ljudi, ki ne zmorejo razmišljati kreativno, naša organizacija ne trpi	3	2	1	0
1-5	Večina zaposlenih dobi potreben čas, da dodelajo nove ideje	3	2	1	0
1-6	Ljudje v naši organizaciji ponavadi izrazijo lastne ideje, saj jih ostali zaposleni v organizaciji k temu spodbujajo in poslušajo	3	2	1	0
1-7	Naša organizacija hitro privzame nove ideje	3	2	1	0
2	Moč in konflikti				
2-1	V naši organizaciji vlada atmosfera zaupanja	3	2	1	0
2-2	Vodilne v naši organizaciji vedno naslavljamo spoštljivo, z uradnim nazivom	3	2	1	0
2-3	Pristopi in prakse ravnanja so deležni veliko kritik	3	2	1	0
2-4	Zaposleni v organizaciji situacije pogosto izkoristijo v osebno korist	3	2	1	0
2-5	Mnogo je skupin, ki skrbijo predvsem za lasten interes	3	2	1	0
2-6	Politika je način življenja za mnogo zaposlenih v organizaciji	3	2	1	0
2-7	Napredovanje je bolj posledica tega, koga poznaš kot tega, koliko znaš in koliko si sposoben	3	2	1	0
3	Informacije in komunikacije				
3-1	Naša organizacija z zaposlenimi komunicira učinkovito	3	2	1	0
3-2	Različni oddelki ponavadi prenašajo pravilne delovne informacije v rednih časovnih intervalih	3	2	1	0
3-3	Posamezniki velikokrat zadržijo informacije zase	3	2	1	0

3-4	Organizacija je poskrbela za sprejemljiv informacijski sistem	3	2	1	0
3-5	Vodilni spodbujajo dvosmerni dialog s podrejenimi	3	2	1	0
3-6	Pomembne informacije ponavadi najdejo pot do tistih, ki morajo biti z njimi seznanjeni	3	2	1	0
Št.	Usmeritve in stališča	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
3-7	Opravljanje in špekulacije so v naši organizaciji zelo razširjena praksa	3	2	1	0
4	Pravila				
4-1	Od zaposlenih se pričakuje, da bodo kršitve pravil prijavili	3	2	1	0
4-2	Delo je dobro organizirano in sistematično napreduje	3	2	1	0
4-3	Večina zaposlenih razume in spoštuje pravila	3	2	1	0
4-4	Naša organizacija je zelo fleksibilna	3	2	1	0
4-5	Politike in procedure v organizaciji se spreminjajo zelo počasi	3	2	1	0
4-6	Glede interpretacije pravil je pogosto veliko nejasnosti	3	2	1	0
4-7	Sistemi nadzora nad delom zaposlenih so ponavadi učinkoviti	3	2	1	0
5	Izobraževanje				
5-1	Zaposleni v naši organizaciji se ponavadi učijo iz svojih napak	3	2	1	0
5-2	Ko pri delu se zgodijo napake, se o tem pogovorimo in se iz napak skušamo nekaj naučiti	3	2	1	0
5-3	Organizacijski sistemi in politike v organizaciji ponavadi spodbujajo učenje na podlagi izkušenj	3	2	1	0
5-4	Ko nek sektor znotraj organizacije pride do novih spoznanj, so le-ta hitro posredovana še drugim sektorjem v organizaciji	3	2	1	0
5-5	V naši organizaciji se stare napake ponavljajo vedno znova in znova	3	2	1	0
5-6	Ljudje v naši organizaciji so pogosto preveč zaposleni, da bi lahko učinkovito pridobivali nova znanja	3	2	1	0
5-7	Vodilni ne spodbujajo toliko »izobraževalne« orientacije med zaposlenimi, ampak predvsem »delovno« orientacijo	3	2	1	0
6	Individualnost				
6-1	Naša organizacija spodbuja zaposlene, da na delovnem mestu	3	2	1	0

	oblikujejo svoje lastne osebnosti				
6-2	Naša organizacija je obzirna do posebnosti	3	2	1	0
6-3	Zaposleni v naši organizaciji lahko zadržijo (kanček) lastne individualnosti	3	2	1	0
6-4	V naši organizaciji je nekaj takšnih, ki jim služba predstavlja tudi vse življenje	3	2	1	0
Št.	Usmeritve in stališča	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
6-5	Organizacija spodbuja zaposlene k razvoju in dozorevanju	3	2	1	0
6-6	Zaposleni niso grajeni zaradi osebnega stila	3	2	1	0
6-7	V naši organizaciji je videz manj pomemben kot vsebina	3	2	1	0
7	Sodelovanje				
7-1	Ljudje v organizaciji so ponavadi pripravljeni pomagati drug drugemu (in so obzirni do drugih)	3	2	1	0
7-2	Formalna pravila in procedure organizacije spodbujajo sodelovanje	3	2	1	0
7-3	Večina zaposlenih v organizaciji je dobrih »moštvenih igralcev«	3	2	1	0
7-4	Individualci ponavadi ne napredujejo	3	2	1	0
7-5	Ljudje, ki dobro delajo, zlasti v skupinah, so ponavadi nagrajeni	3	2	1	0
7-6	»Ponudi roko v pomoč« je dober opis delovanja naše organizacije	3	2	1	0
7-7	Zaposleni v naši organizaciji imajo močan občutek skupinske pripadnosti	3	2	1	0
8	Zaupanje				
8-1	Zaposleni v naši organizaciji ponavadi zaupajo sodelavcem	3	2	1	0
8-2	Zaposleni v naši organizaciji ne skušajo izkoriščati sodelavcev	3	2	1	0
8-3	Pravila naše organizacije spodbujajo vzajemnost	3	2	1	0
8-4	Ljudje, ki imajo težave z zaupanjem, v naši organizaciji težko preživijo	3	2	1	0
8-5	Zaposleni v naši organizaciji drug drugemu zaupajo	3	2	1	0
8-6	Zaposleni ponavadi ne pobirajo zaslug za delo, ki so ga opravili drugi	3	2	1	0
8-7	V delovnem vzdušju prevladujeta ljubosumnost in zavist	3	2	1	0

9	Nasprotovanja in konflikti				
9-1	V organizaciji je veliko majhnih konfliktov	3	2	1	0
9-2	Oddelki v organizaciji med seboj sodelujejo brez zavisti	3	2	1	0
9-3	Kritike so pogosto razumljene kot osebni napad	3	2	1	0
9-4	Zaposleni v organizaciji vedno skušajo prevladati v konfliktih	3	2	1	0
9-5	V organizaciji obstajajo močne in povezane skupine, ki skrbijo le zase	3	2	1	0
9-6	Od sodelavcev se le redko doživi osebno nasprotovanje	3	2	1	0
9-7	Konflikt je v naši organizaciji pogosto viden kot pozitivna značilnost	3	2	1	0
Št.	Usmeritve in stališča	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
10	Usmeritve v prihodnost				
10-1	Zaposleni v naši organizaciji razmišljajo in načrtujejo vnaprej	3	2	1	0
10-2	Naša organizacija je usmerjena v prihodnost	3	2	1	0
10-3	Večino zaposlenih v organizaciji bolj zanima, kaj se bo zgodilo jutri kot kaj se je zgodilo včeraj	3	2	1	0
10-4	Strategija organizacije za prihodnost je znana večini zaposlenim	3	2	1	0
10-5	Živahne razprave glede prihodnosti organizacije so zelo pogoste	3	2	1	0
10-6	Zaposleni v organizaciji so cenjeni in spoštovani v smislu njihovega delovnega potenciala	3	2	1	0
10-7	Zaposleni v organizaciji imajo ponavadi dolgoročne poglede na zadeve, ki se tičejo organizacije	3	2	1	0
11	Lojalnost in obveza				
11-1	V naši organizaciji je veliko ljudi, ki so tu že celo kariero	3	2	1	0
11-2	Večina zaposlenih se smatra za lojalne člane organizacije	3	2	1	0
11-3	Malo zaposlenih je zavezanih življenjski karieri v naši organizaciji	3	2	1	0
11-4	Organizacija je zavezana svojim zaposlenim	3	2	1	0
11-5	Zaposleni z dolgim delovnim stažem so deležni prednostne obravnave	3	2	1	0
11-6	Trdno verjamem, da je moja dolgoročna prihodnost vezana na to	3	2	1	0

	organizacijo				
11-7	Ko se pričnejo težave, postane lojalnost organizacije zaposlenim vprašljiva	3	2	1	0
12	Delovna usmeritev				
12-1	Zaposleni na splošno uživajo v svojem delu	3	2	1	0
12-2	Zaposleni v naši organizaciji so vedno pripravljeni na odmor	3	2	1	0
12-3	Zaposleni v naši organizaciji raje živijo za delo kot delajo za življenje	3	2	1	0
12-4	Motivacija v naši organizaciji ni sporna zadeva	3	2	1	0
12-5	Vodilni v organizaciji delajo enako pridno (ali še bolj) kot ostali zaposleni	3	2	1	0
12-6	Zaposleni sledijo geslu »delo pred užitkom«	3	2	1	0
12-7	Vsakodnevne aktivnosti ne zahtevajo trajnega in intenzivnega truda	3	2	1	0

RAZDELEK B: STALIŠČA DO POSAMEZNIH ELEMENTOV ORGANIZACIJSKE KULTURE

V nadaljevanju navajamo trditve, do katerih se je potrebno opredeliti. Prosimo, da se do vsake posamezne trditve opredelite tako, da pri vsaki posamezni trditvi v vsakem stolpcu izberete kvadrček, ki najbolje opisuje vašo izbiro, pri tem pa upoštevate, da ocena 3 pomeni, da trditev vsekakor drži za Vašo organizacijo, ocena 0 pa, da trditev za Vašo organizacijo vsekakor ne drži.

1.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
Od zaposlenih v organizaciji se pričakuje, da pripisujejo največjo pomembnost...	3	2	1	0
(B1-1) ... izpolnjevanju zahtev in pričakovanj nadrejenih in drugih zaposlenih, ki so v organizaciji višje na hierarhični lestvici.	☐	☐	☐	☐
(B1-2) ... izpolnjevanju nalog na njihovem delovnem mestu v skladu s postopki in navodili.	☐	☐	☐	☐
(B1-3) ... iskanju izzivov, ki jih ponujajo naloge in najboljših poti za njihovo reševanje.	☐	☐	☐	☐
(B1-4) ... sodelovanju z ostalimi zaposlenimi	☐	☐	☐	☐

z namenom reševanja tako delovnih, kot osebnih problemov.				
---	--	--	--	--

2.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
V naši organizaciji gre dobro tistim, ki ...	3	2	1	0
(B2-1) ... vedo, kako ugoditi nadrejenim.	☐	☐	☐	☐
(B2-2) ... igrajo po pravilih in si prizadevajo korektno delati.	☐	☐	☐	☐
(B2-3) ... so učinkoviti in dobro podkovani.	☐	☐	☐	☐
(B2-4) ... tesno sodelujejo s sodelavci, so skrbni in odprti za njihova mnenja.	☐	☐	☐	☐

3.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
Organizacija ravna s posameznikom kot ...	3	2	1	0
(B3-1) ... s »parom rok«, katerih čas in energija morata biti na voljo tistim, ki so višje na hierarhični lestvici.	☐	☐	☐	☐
(B3-2) ... z »zaposlenim«, katerega čas in energija sta pridobljena s pogodbenimi pravicami in obveznostmi za obe strani.	☐	☐	☐	☐
(B3-3) ... z »družabnikom« ali enakovrednim članom, s katerim skupaj poskuša doseči skupne cilje.	☐	☐	☐	☐
(B3-4) ... z »družino« ali »prijatelji«, ki so radi skupaj in skrbijo ter podpirajo drug drugega.	☐	☐	☐	☐

4.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
Zaposlene vodijo oziroma jim ukazujejo ...	3	2	1	0

(B4-1) ... ljudje na položajih, ki svojo oblast kažejo z uporabo kazni in nagrad.	☐	☐	☐	☐
(B4-2) ... sistem, pravila in postopki, ki so v naprej določeni.	☐	☐	☐	☐
(B4-3) ... njihove lastne motivacije in doseganje lastnih ciljev.	☐	☐	☐	☐
(B4-4) ... njihova želja, da bi jih sodelavci čim bolj sprejeli.	☐	☐	☐	☐

5.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
Za proces odločanja v organizaciji je značilno, da ...	3	2	1	0
(B5-1) ... usmeritve, ukazi in navodila prihajajo navzdol iz višjih nivojev.	☐	☐	☐	☐
(B5-2) ... vlada privrženost formalnim kanalom in zanašanje na utečene postopke odločanja.	☐	☐	☐	☐
(B5-3) ... so odločitve sprejete tik pred zdajci, sprejmejo pa jih izvajalci odločitev.	☐	☐	☐	☐
(B5-4) ... so odločitve sprejete soglasno in z večinsko podporo članov organizacije.	☐	☐	☐	☐

6.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
Dodeljevanje delovnih nalog posameznikom temelji na ...	3	2	1	0
(B6-1) ... osebnih ocenah in željah tistih, ki imajo v organizaciji moč in oblast.	☐	☐	☐	☐
(B6-2) ... potrebah in načrtih organizacije ter pravilih sistema (izobrazba, delovno mesto, izkušnje).	☐	☐	☐	☐
(B6-3) ... ujetanju zahtev naloge z interesi in sposobnostmi posameznika.	☐	☐	☐	☐
(B6-4) ... željah posameznika in njegovi potrebi po rasti in razvoju.	☐	☐	☐	☐

7.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
V organizaciji prevladuje mnenje, da naj	3	2	1	0

bodo zaposleni ...				
(B7-1) ... ubogljivi, ustrežljivi in lojalni svojemu nadrejenemu.	☐	☐	☐	☐
(B7-2) ... odgovorni in vredni zaupanja.	☐	☐	☐	☐
(B7-3) ... samomotivirani, sposobni ter pripravljeni za doseganje dobrih rezultatov tudi oporekati nadrejenim.	☐	☐	☐	☐
(B7-4) ... dobri člani tima, ki naj bodo v oporo ostalim članom.	☐	☐	☐	☐

8.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
V naši organizaciji je oseba upravičena dati nalogo nekomu, če ...	3	2	1	0
(B8-1) ... ima več moči, oblasti in je na višjem položaju.	☐	☐	☐	☐
(B8-2) ... je za nalogo odgovorna na podlagi njenega opisa del in nalog.	☐	☐	☐	☐
(B8-3) ... ima več znanja in izkušenj, ki jih uporablja z namenom, da bi drugega naučila izvesti nalogo.	☐	☐	☐	☐
(B8-4) ... jo le-ta prosi za pomoč, usmerjanje in nasvet.	☐	☐	☐	☐

9.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
Širše okolje zunaj organizacije si zaposleni predstavljamo kot ...	3	2	1	0
(B9-1) ... džunglo, kjer se bije boj za obstanek.	☐	☐	☐	☐
(B9-2) ... urejen in racionalni sistem, kjer so odnosi določeni s strukturo in pravili in vsakdo ravna v skladu s pravili.	☐	☐	☐	☐
(B9-3) ... tekmovanje v odličnosti, kjer produktivnost, kvaliteta in inovacija prinašajo uspeh.	☐	☐	☐	☐
(B9-4) ... kompleksen sistem, kjer je skupni interes najbolj pomemben.	☐	☐	☐	☐

10.	VSEKAKOR	VEČINOMA	VEČINOMA	VSEKAKOR
------------	-----------------	-----------------	-----------------	-----------------

	DRŽI	DRŽI	NE DRŽI	NE DRŽI
Če so pravila in predpisani postopki »v napoto«, jih člani naše organizacije ...	3	2	1	0
(B10-1) ... prekršijo, če so prepričani, da jih ne bodo zalotili.	☐	☐	☐	☐
(B10-2) ... vseeno upoštevajo.	☐	☐	☐	☐
(B10-3) ... ignorirajo ali obidejo, da lahko svojo nalogo bolje opravijo.	☐	☐	☐	☐
(B10-4) ... s splošno podporo prekršijo, sploh če menijo, da niso dobra.	☐	☐	☐	☐

11.	VSEKAKOR DRŽI	VEČINOMA DRŽI	VEČINOMA NE DRŽI	VSEKAKOR NE DRŽI
Novo zaposleni se mora v naši organizaciji naučiti ...	3	2	1	0
(B11-1) ... kdo je »glavni«, kdo mu lahko pomaga ali škodi ter nenapisanih pravil, ki naj jih upošteva, če noče zaiti v težave.	☐	☐	☐	☐
(B11-2) ... formalnih pravil in postopkov ter upoštevanja le-teh, predvsem pa ne sme delati tistega, česar ni v njegovem opisu del in nalog.	☐	☐	☐	☐
(B11-3) ... kaj vse mu je na voljo in v pomoč, da bi svoje delo dobro opravljal.	☐	☐	☐	☐
(B11-4) ... kako sodelovati z drugimi, kako postati dober član tima.	☐	☐	☐	☐

B12. Sledi nekaj trditev – paradoksov, na podlagi analize katerih lahko ocenimo stopnjo organizacijske kulture v organizaciji. Za vsak paradoks posebej ocenite, ali se z njim strinjate ter svoje (ne)strinjanje izrazite na lestvici od 1 do 5, pri čemer 1 pomeni, da se s posameznim paradoksom sploh ne strinjate, 5 pa, da se s posameznim paradoksom močno strinjate.

ŠT.	PARADOKS	se sploh ne strinjam				se močno strinjam
B12-1	Zaposleni v naši organizaciji imamo jasno predstavo, kaj se od nas pričakuje, VENDAR pooblastila, pristojnosti in odgovornosti niso uravnotežene na vseh nivojih.	1	2	3	4	5
B12-2	Politika in cilji organizacije so jasni vsem zaposlenim, VENDAR pri postavljanju ciljev vsi zaposleni ne sodelujemo.	1	2	3	4	5
B12-3	Uspešnost se praviloma vrednoti po dogovorjenih ciljih in standardih, VENDAR zaposleni ne prejemo plače, ki bi bila	1	2	3	4	5

	enakovredna ravni plač na trgu.					
B12-4	Zaposleni zunaj organizacije pozitivno govorimo o njej, VENDAR bi organizacijo zapustili, če bi se nam zaradi poslovnih težav zmanjšala plača, (zaposlenim pa tudi nismo pripravljeni prevzeti tveganja za uveljavitev svojih pobud).	1	2	3	4	5
B12-5	Delovni sestanki so redni, vodje posredujejo informacije na razumljiv način, KLJUB TEMU pa ne vemo, kaj se dogaja v drugih enotah, ljudje si med seboj ne zaupajo.	1	2	3	4	5
B12-6	Kriteriji napredovanja so jasni vsem zaposlenim in smo načeloma zadovoljni z dosežanim osebnim razvojem, VENDAR nimamo sistema, ki bi omogočal napredovanje res najboljšim.	1	2	3	4	5

RAZDELEK C: STALIŠČA DO VARNOSTNE KULTURE

C1. Ali so novo sprejeti delavci v vaši organizaciji po vašem mnenju dovolj varnostno osveščeni?

- 1) da
- 2) ne

C1-1 ... Če ne ... Zakaj? (možnih je več odgovorov)

- a) ker ni v organizaciji nobenega varnostnega usposabljanja
- b) ker ni v organizaciji nobenega usposabljanja glede ravnanja s tajnimi podatki
- c) ker so v varnostnem sistemu pomanjkljivosti
- d) ker varnostni organi niso dovolj usposobljeni
- e) drugo: _____

C2. Kakšen je vaš odnos do vaših sodelavcev, ki zunaj vaše organizacije razkrivajo tajne podatke?

(en odgovor)

- 1) takšna dejanja obstojam in jih ne razumem
- 2) takšna dejanja obsojam, a jih razumem
- 3) takšnih dejanj ne obsojam in jih razumem
- 4) takšnih dejanj ne obsojam, a jih tudi ne razumem

C3. Kakšni so po vašem mnenju razlogi, da nekateri zaposleni v vaši organizaciji zunaj organizacije razkrivajo tajne in zaupne podatke? (možnih več odgovorov)

- 1) na ta način posamezniki izražajo nezadovoljstvo z organizacijo in njenim delovanjem
- 2) na ta način posamezniki izražajo nezadovoljstvo z načinom reševanja problemov znotraj organizacije
- 3) na ta način se posamezniki skušajo maščevati lastni organizaciji zaradi občutka krivice, ki da se jim je zgodila
- 4) na ta način skušajo posamezniki javnost opozoriti na nepravilnosti znotraj organizacije
- 5) na ta način želijo posamezniki pridobiti zase različne materialne koristi
- 6) drugo: _____

C4. Kako ocenjujete ravnanje z zaupnimi dokumenti in podatki v varnostnem smislu v vaši organizaciji? (en odgovor)

- 1) nezadovoljivo
- 2) zadovoljivo
- 3) dobro
- 4) odlično
- 5) ne vem

C5. Ali menite, da je neko temeljno znanje s področja varnostne kulture nujno potrebno vsem uslužbencem v celotni državni upravi?

- 1) da
- 2) ne

C6. Ali ste vi osebno bili v času vašega delovanja v organizaciji vključeni v kakršnekoli oblike usposabljanja glede ravnanja s tajnimi podatki?

- 1) da
- 2) ne
- 3) ne vem

C7. Menite, da je tako izobraževanje za zaposlene v vaši organizaciji potrebno?

- 1) da
- 2) ne
- 3) ne vem

C8. Ali v vaši organizaciji obstaja nadzor nad ravnanjem s tajnimi oz. zaupnimi podatki?

- 1) da
- 2) ne

C8-1 ... če da ... Kdo ta nadzor izvaja? _____

C9. Ali menite, da je reševanje notranjih težav in problemov v vaši organizaciji preko anonimk za vašo organizacijo dobro?

- 1) da
- 2) ne
- 3) ne vem

C10. Zakaj se v vaši organizaciji po vašem mnenju pojavljajo anonimke? *(možnih več odgovorov)*

- 1) na ta način posamezniki izražajo nezadovoljstvo z organizacijo in njenim delovanjem
- 2) na ta način posamezniki izražajo nezadovoljstvo z načinom reševanja problemov znotraj organizacije
- 3) na ta način se posamezniki skušajo maščevati lastni organizaciji zaradi občutka krivice, ki da se jim je zgodila
- 4) na ta način skušajo posamezniki javnost opozoriti na nepravilnosti znotraj organizacije
- 5) na ta način skušajo posamezniki prikriti nekatera druga sporna dejanja v organizaciji
- 6) na ta način želijo posamezniki pridobiti zase različne materialne koristi
- 7) drugo: _____

C11. Ali vi osebno veste za kakšen primer sankcioniranja v primeru kršitev varovanja podatkov v vaši organizaciji?

- 1) da
- 2) ne

RAZDELEK D: DEMOGRAFSKI PODATKI

D1. Spol

- 1) moški
- 2) ženski

D2. Starost: ____ let

D3. Vaš osebni karierni razred po ZJU (odgovarjajo le zaposleni v upravnem delu MORS): _____

D4. Koliko let ste že zaposleni v slovenski vojski/MORS-u

- a) 1 ali manj
- b) med 2 in 5 let
- c) med 5 in 10 let
- d) več kot 10 let

D5. Dokončana izobrazba

- a) manj kot srednja
- b) srednja
- c) višja
- d) visoka strokovna
- e) univerzitetna
- f) magisterij ali doktorat