ŠOLA ZA ČASTNIKE
IZREDNA GENERACIJA JANUAR 2012
SPECIALIZACIJA OBVEŠČEVALEC

ZAKLJUČNA NALOGA

VAROVANJE TAJNIH PODATKOV V SV

Kandidat-slušatelj: stotnik Robert Perčič

Mentor: major Jože Grbec

Maribor, maj 2012

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

SLOVENSKA VOJSKA
POVELJSTVO ZA DOKTRINO, RAZVOJ, IZOBRAŽEVANJE IN USPOSABLJANJE
Šola za častnike

Številka:
Datum:

ZAKLJUČNA NALOGA

VAROVANJE TAJNIH PODATKOV V SV

Kandidat-slušatelj: stotnik Robert Perčič

Mentor: major Jože Grbec

Maribor, maj 2012

Engelsova ulica 15, 2111 Maribor
Telefon: 02 332 2227, fax: 02 332 1035, e-pošta: pdriu@mors.si

VAROVANJE TAJNIH PODATKOV V SV

POVZETEK

Republika Slovenija in z njo tudi Slovenska vojska ima pravico in dolžnost zavarovati samo sebe. Eden izmed načinov je obstoj tajnih podatkov in omejen dostop do njih. Nepooblaščeno razkritje tajnih podatkov lahko povzroči nepopravljivo škodo ali celo izgubo življenj. S sprejetjem Zakona o tajnih podatkih je bil poenoten nacionalni sistem varovanja tajnih podatkov.

V Slovenski vojski se je po sprejetju zakona in podzakonskih aktov na področju varovanja tajnih podatkov pristopilo k sistematičnemu urejanju tega področja, ki pa je zelo obširno in zahteva ukrepe na fizičnem, tehničnem in organizacijskem področju. Za pravilno delovanje sistema za varovanje tajnih podatkov je pomemben nadzor, ki odkriva pomanjkljivosti, katere se mora odpraviti in s tem pripomoči k učinkovitejšemu varovanju tajnih podatkov.

Navkljub vzorno urejenemu sistemu varovanja tajnih podatkov moramo zagotoviti še, da bodo osebe, ki obravnavajo tajne podatke, ustrezno usposobljene, da bodo upoštevale vsa navodila in predpise ter da bodo v skladu z njimi tudi ravnale.

Ključne besede: Slovenska vojska, varovanje tajnih podatkov, nadzor, usposabljanje

PROTECTION OF CLASSIFIED INFORMATION IN SLOVENIAN ARMED FORCES

SUMMARY

The Republic of Slovenia and Slovenian Armed Forces with it have the right and duty to protect itself. One way of protection is the existence of classified information and restricted access to them. Unauthorized disclosure of classified information can cause irreparable damage or even loss of life. With the adoption of the Classified Information Act national system of protection of classified information was unified.

Following the adoption of the Act and implementing regulations for the protection of classified information Slovenian Armed Forces began with systematic regulation of this area, which is very broad and calls for action on physical, technical and organizational field. For proper operation of the system to protect classified information control that detects defects, which must be eliminated and thus contribute to more effective protection of classified information is very important.

Despite the exemplary regulated system for protection of classified information we must ensure that people who handle classified information are properly trained to follow all the guidelines and regulations and they act accordingly with them.

Keywords: Slovenian Armed Forces, protection of classified information, supervision, training

KAZALO

1 UVOD

Varovanje tajnih podatkov je del sistema nacionalne varnosti. Tajni podatki niso in ne morejo prosto dostopni vsem, ampak se smejo s tako označenimi podatki in informacijami seznaniti samo upravičeni posamezniki.

V skladu z Zakonom o tajnih podatkih je tajni podatek definiran kot 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 s tem zakonom označeno za tajno.

Spremembe v družbi po osamosvojitveni vojni so se odrazile v spremenjenem razumevanju med individualno in državno zasebnostjo. Naenkrat je bila javnost prepričana, da je samoumevno, da je seznanjena z vsemi informacijami in podatki, v nasprotju s prejšnjo državo, kjer je bila tehtnica močno na strani državne zasebnosti. Od demokratične družbe se pričakuje, da določi pravilno razmerje med obema skrajnostma.

V Slovenski vojski, ki je tista organizacijska struktura slovenske države, za katero se zahteva najvišja stopnja povezljivosti z Natom, se jasno zavzemamo zato, da se terminologija čim bolj poenoti in uskladi z ustrezno terminologijo v Natu. To za strokovnjake, ki izvajajo naloge na varnostnem področju pomeni veliko olajšanje saj se aktivnosti na področju varovanja tajnih podatkov tako prepletajo med varovanjem nacionalnih podatkov in tajnih podatkov zveze Nato, da je postopke aktivnosti na tem področju praktično nemogoče ločevati. Največkrat pa se postopki varovanja Nato podatkov navezujejo na postopke, ki so opredeljeni za nacionalne tajne podatke, seveda ob predpogoju, da nacionalno normativno področje ustreza vsem zahtevam Nata. Ustrezno uskladitev terminologije so večkrat predlagali tudi strokovnjaki, ki so prihajali v Slovenijo s strani Urada za varnost v Natu. Vendar se vsi zavedamo, da se temu cilju lahko samo približamo, nikakor pa ne moremo vzpostaviti enake terminološke podlage, saj se v malenkostih razlikujeta celo terminologiji Nata in Evropske unije na področju varovanja tajnih podatkov.

Na obrambnem področju in v vojaški organizaciji kot nosilcu obrambe države je veliko število zaposlenih. Ti se vsak dan srečujejo z izdelavo, distribucijo in varovanjem tajnih podatkov. Zaradi zahtevnosti normativne zakonodaje je treba zaposlene usposabljati. Pri usposabljanju je treba obnoviti in nadgraditi znanje zaposlenih s področja varovanja tajnih podatkov zaradi spremembe zakonodaje in uveljavljanja standardov, ki jih predpisujeta EU in Nato. Z usposabljanji je treba dvigniti tudi raven varnostne kulture ter na zaposlene vplivati do te mere, da varnost postane del njihove vsakodnevne kulture. Varnostna kultura, še posebej pripadnikov SV, je pomemben temelj nacionalne varnosti, saj stopnja razvitosti varnostne kulture pripadnikov oboroženih sil neke države močno vpliva na učinkovitost delovanja sistema nacionalne in kolektivne varnosti.

Varnost in zaščita tajnih podatkov v SV, kot eden od poglavitnih elementov pripravljenosti poveljstev in enot se lahko izvaja samo, če so pri njenem izvajanju zajeti vsi elementi varnostne kulture in izhajajo iz poveljevanja in kontrole. Vloga poveljujočih je pomemben element zaščite tajnih podatkov, ker so nosilci v sistemu poveljevanja in kontrole oziroma imajo vpliv glede na svojo funkcionalno dolžnost. Obveščevalne službe kljub sodobnemu načinu zbiranja podatkov še vedno zbirajo določeno število podatkov z direktnim komuniciranjem s pripadniki Slovenske vojske in zaposlenimi na obrambnem področju.

Za poenotenje nadzora nad tajnimi podatki je ključno leto 2006, ko je Zakon o varovanju tajnih podatkov predpisal dolžnost inšpekcijskega nadzora nad varovanjem tajnih podatkov

po ZTP in predpisih, sprejetih na njegovi podlagi. Na obrambnem področju ta nadzor izvaja Inšpektorat Republike Slovenije za obrambo.

Na prehodu iz 20. v 21. stoletje smo bili priča velikemu razvoju znanosti na vseh področjih življenja. Razvoj novih tehnologij omogoča izdelavo novih komunikacijskih sredstev, s katerimi posamezniki komunicirajo med seboj in družbo. Razvoj interneta in mobilne telefonije spreminja način življenja družbe na globalni ravni. Pri tem postaja komuniciranje med ljudmi vedno bolj neosebno. Hkrati z razvojem novih komunikacijskih sredstev se znova pojavlja tudi potreba po varovanju podatkov s stopnjami tajnosti, saj je še vedno treba ločiti zasebno od javnega.

1.1 IZHODIŠČE ZAKLJUČNE NALOGE

V nalogi se ukvarjam z predpisi, ki urejajo področje varovanja tajnih podatkov v Sloveniji in njihovo praktično uporabo v Slovenski vojski. Izhajam iz predpostavke, da je delo s tajnimi podatki občutljivo področje, ki zahteva popolno normativno ureditev, še bolj pomemben pa je človeški faktor, saj je le strokovno usposobljen, lojalen in odgovoren posameznik garant za preprečitev odtekanja tajnih podatkov v nepooblaščene roke.

Področje varovanja tajnih podatkov zajema širok spekter ukrepov, ki jih je nemogoče vse obdelati v enem delu, zato me poleg normativne ureditve zanima rezultat nadzorov, ki so bili opravljeni v enotah. Na podlagi popisa pomanjkljivosti, ki so bile zaznane, bom predvidel aktivnosti in načine na katere lahko minimiziramo nepravilnosti pri ravnanju s tajnimi podatki.

Naloga je zasnovana na javno dostopni literaturi in vpogledih v dokumente brez stopnje tajnosti s področja varovanja tajnih podatkov.

1.2 NAMEN IN CILJ RAZISKAVE

Namen raziskave je ovrednotiti stanje na področju obravnave tajnih podatkov v Republiki Sloveniji, s poudarkom na Slovenski vojski in skozi nabor nepravilnosti, ki so bile ugotovljene v postopkih izvajanja nadzora prikazati področja znotraj sistema varovanja tajnih podatkov, kjer se nam pojavljajo nepravilnosti in s predpisi neskladna ravnanja.

Naloga proučuje temeljno legislativno podlago in služi nadaljnji obravnavi praktičnega izvajanja posameznih določil Zakona o tajnih podatkih in na njegovi podlagi sprejetih predpisov.

Cilji preučevanja:

- predstaviti regulativno ureditev področja varovanja tajnih podatkov,
- opredeliti posebnosti pri varovanju tajnih podatkov v SV,
- analizirati in opisati nedoslednosti pri izvajanju področnih predpisov,
- poudariti pomen usposabljanja o varovanju tajnih podatkov.

1.3 METODE DELA

Preučevanje tematike varovanja tajnih podatkov in opis neskladnih ravnanj v Slovenski vojski zahtevata uporabo različnih metod, ki so medsebojno prilagojene in usklajene.

Skozi celotno nalogo sem uporabljal deskriptivno metodo, ki je uporabljena skupaj s teoretičnimi koncepti. V nalogi je uporabljena tudi analiza virov: primarnih (zakonov,

pravilnikov, izvedbenih predpisov), sekundarnih (knjig, člankov, raziskovalnih poročil) in tudi terciarnih (internet, diplomske naloge na podobno tematiko). V delu naloge, kjer so podane ugotovitve nadzorov, uporabljam metodo študija primerov.

1.3.1 Hipotezi

Glede na zastavljene cilje bosta preizkušeni dve hipotezi:

- Slovenija ima področje ravnanja s tajnimi podatki pravno dobro urejeno in
- dodatno usposabljanje s področja tajnih podatkov preprečuje nepravilna ravnanja.

1.4 STRUKTURA ZAKLJUČNE NALOGE

Naloga je razdeljena v tri sklope. V prvem delu zaključne naloge opisujem sistemsko ureditev, sprejem krovnega zakona in ostalih področnih predpisov, navajam osebe, ki imajo pravico dostopa do tajnih podatkov ter predstavim vladni urad, ki bdi nad področjem varovanja tajnih podatkov v naši državi.

Drugi del naloge začne pregled ukrepov na področju varovanja tajnih podatkov, zajame področji, ki sta neločljivo povezani s tajnimi podatki, kot sta sistem vrednot in varnostna kultura, ki sta temeljnega pomena pri preprečitvi zlorabe tajnih podatkov s strani zaposlenih.

Tretji, osrednji del naloge zajema nadzor nad varovanjem tajnih podatkov, ki kot nepogrešljiv in pomemben del sistema s svojimi ugotovitvami pokaže, na katerih področjih nadzorovani subjekt ne ravna točno v skladu s predpisi in mora pomanjkljivosti v določenem roku odpraviti. Na koncu zadnjega poglavja se posvečam oblikam in pomenu usposabljanja, ki s je pomembno zato, da so zaposleni na obrambnem področju vseskozi seznanjeni z vsemi predpisi in pravilno ravnajo s tajnimi podatki ter tako preprečijo njihovo odtekanje nepooblaščenim osebam in organizacijam.

V zaključku sledi ovrednotenje hipotez in strnjeno razmišljanje o predelani tematiki.

2 SISTEMSKA UREDITEV VAROVANJA TAJNIH PODATKOV

Pravno urejen sistem varovanja tajnih podatkov je po vključitvi Slovenije v evroatlantske povezave zelo pomemben. Država, ki ustrezno varuje svoje in tuje tajne podatke, je v mednarodni skupnosti sprejeta kot zaupanja vreden partner. Slovenija je to dosegla s sprejetjem Zakona o varovanju tajnih podatkov (ZTP) in zadostila zahtevam pogajalskih izhodišč za vstop v Evropsko unijo v poglavju št. 24, Pravosodje in notranje zadeve.

Zakon je na ravni države združil nekatera področja varovanja tajnih podatkov, ki so sicer že bila delno urejena v posameznih zakonih oziroma podzakonskih aktih. Zakon o tajnih podatkih je v splošnih določbah opredelil temeljne pojme, kot so tajni podatek, dokument, določanje tajnih podatkov, prenehanje tajnosti podatkov, varnostno preverjanje in varnostni zadržek.

2.1 RAZMERJE MED INDIVIDUALNO IN DRŽAVNO ZASEBNOSTJO

Že v uvodu sem omenil občutljivo vprašanje razmerja med individualno in državno zasebnostjo. V demokratični družbi mora ureditev tega področja upoštevati vsa načela, na katerih temeljijo pravice in svoboščine državljanov. Najprej je tu načelo preglednosti delovanja nosilcev oblasti, postopkov, dejanj, ukrepov in odločitev, s katerimi država posega v življenje ljudi. Pravica dostopa do podatkov ter informacij državnih organov in javnost njihovega dela je splošno načelo vsake moderne družbe. Delovanje države si danes ni mogoče predstavljati brez sodelovanja in podpore javnosti.

39. člen Ustave RS zagotavlja svobodo tiska in drugih oblik javnega obveščanja in pravico vsakogar, da skladno z zakonom dobi informacije javnega značaja. »Zagotovljena je svoboda izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja. Vsakdo ima pravico dobiti informacije javnega značaja, za katere ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon.« Toda to načelo dostopnosti ne more veljati absolutno, javnost dela državnega organa je odvisna od njegovega položaja in značilnosti dela organa. Nekatere podatke in informacije, ki nastajajo v državnih organih, je treba zaradi zavarovanja državnih interesov označiti kot tajne. Ti podatki so nedostopni za nepooblaščene osebe in javnost v celoti, kar je v nasprotju z načelom javnosti (Čaleta 2003: 16).

Nasprotje interesov, ki nastopi ob posebnem režimu varovanja določenih podatkov zahteva pravilno vzpostavitev razmerja med tajnim in javnim in je izziv večine demokratičnih družb. Državni organi bi lahko z nekontroliranim prikrivanem informacij in podatkov vršili nepravilnosti in nezakonitosti, po drugi strani pa preohlapno varovanje podatkov lahko ogrozi interese in varnost države.

2.2 SPREJEM ZAKONA O VAROVANJU TAJNIH PODATKOV

Preden je bil sprejet sistemski zakon o tajnih podatkih je bilo to področje neurejeno in pomembni državni podatki so večkrat nepooblaščeno prišli v javnost. Družba se ni zavedala državne zasebnosti kot vrednote in je ni pravno uredila. Sprejem ustreznega zakona je bila nuja in velik korak naprej v urejanju državne zasebnosti. Ureditev področja varovanja tajnih podatkov je bil eden izmed temeljnih pogojev za vstop Slovenije v EU in Nato. Pred sprejetjem zakona je bilo to področje urejeno le v posameznih organih brez vnaprej znanih kriterijev glede dostopa, določanja, varovanja in prenehanja tajnih podatkov.

V Sloveniji smo do leta 2001 poznali dva načina označevanja tajnih podatkov. V obrambnem sistemu smo tajnost podatku označevali iz vrste tajnosti in stopnje zaupnosti, kot je bilo npr. VOJAŠKA SKRIVNOST - ZAUPNO, na ministrstvu za notranje zadeve pa so te stopnje tajnosti označevali kot URADNA TAJNOST - ZAUPNO.

Zakon o tajnih podatkih je bil sprejet v Državnem zboru novembra 2001. Predpisal je področje varovanja zasebnosti države, določevanje, označevanje in dostop do tajnih podatkov. S tem je bilo urejeno področje dela državnih organov, ki se nanaša na javno varnost, obrambo, zunanje zadeve in obveščevalno in varnostno delo države. Namesto prejšnjih oznak državna ali vojaška skrivnost in strogo zaupno je predpisal stopnje tajnosti interno, zaupno, tajno in strogo tajno, kar je primerljivo s sistemom EU in Nato.

Leta 2003 je Zakon o spremembah in dopolnitvah ZTP (ZTP-A) uvedel spremembe na področju varnostnega preverjanja. Določil je osnovno, dodatno in preverjanje z poizvedovanjem, ki se izvede glede na vrsto dostopa, ki ga bo kandidat imel.

Dopolnitev zakona je sledila leta 2006 (ZTP-B). Spremembe in dopolnitve so bile usmerjene v večjo učinkovitost in varnost nacionalnih in tujih tajnih podatkov. Podrobno je bila opredeljena vloga informacijskega pooblaščenca in postopek, kjer se ugotavlja javni interes glede razkritja tajnih podatkov. Novela je uvedla tudi inšpekcijski nadzor, ki je garant za večjo enotnost pri izvajanju predpisov s področja tajnih podatkov.

V letu 2010 je sledila sprememba zakona (ZTP-C), kjer je pooblastilo za izdajo dovoljenj namesto Policije dobilo ministrstvo, pristojno za notranje zadeve.

Zadnja dopolnitev leta 2011 (ZTP-D) je k upravičencem, ki lahko dostopajo do tajnih podatkov brez dovoljenja, dodala predsednika in člane Državne revizijske komisije.

2.2.1 Predpisi o varovanju tajnih podatkov v Republiki Sloveniji

Predpisi, ki jih Urad Vlade Republike Slovenije za varovanje tajnih podatkov omenja, da urejajo področje varovanja tajnih podatkov v Republiki Sloveniji so:

- Zakon o dopolnitvi Zakona o tajnih podatkih (Ur. l. RS, št. 60/11),
- Zakon o spremembah Zakona o tajnih podatkih (Ur. l. RS, št. 9/10),
- Zakon o tajnih podatkih (Ur. l. RS, št. 50/06-uradno prečiščeno besedilo),
- Uredba o dopolnitvi Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. l. RS, št. 86/11),
- Popravek Uredbe o spremembah Uredbe o varovanju tajnih podatkov (Ur. l. RS, št. 24/11),
- Uredba o spremembah Uredbe o varovanju tajnih podatkov (Ur. l. RS, št. 7/11),
- Uredba o obliki in uporabi znaka Urada Vlade RS za varovanje tajnih podatkov (Ur. l. RS, št. 1/08),
- Uredba o načinu in postopku ugotavljanja pogojev za izdajo varnostnega dovoljenja organizaciji (Ur. l. RS, št. 70/07),
- Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. l. RS, št. 48/07),
- Uredba o spremembah Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Ur. l. RS, št. 138/06),
- Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja (Ur. l. RS, št. 94/06),
- Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Ur. l. RS, št. 71/06),

- Uredba o varovanju tajnih podatkov (Ur. l. RS, št. 74/05),
- Uredba o notranjem nadzoru nad izvajanjem Zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi (Ur. l. RS, št. 106/02),
- Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja (Ur. l. RS, št. 94/06),
- Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Ur. l. RS, št. 6/02).

Poleg naštetih se na obrambnem področju uporabljajo še naslednji predpisi:

- Pravilnik o varovanju tajnih podatkov na Ministrstvu za obrambo (šifra 0070-5/2006-4, z dne 21. 2. 2006);
- Pravilnik o spremembah in dopolnitvah Pravilnika o varovanju tajnih podatkov na Ministrstvu za obrambo (številka 0070-5/2006-30, z dne 31. 8. 2006);
- Pravilnik o spremembah in dopolnitvah Pravilnika o varovanju tajnih podatkov na Ministrstvu za obrambo (številka 0070-22/2008-26, z dne 11. 6. 2008);
- Pravilnik o spremembah in dopolnitvah Pravilnika o varovanju tajnih podatkov na Ministrstvu za obrambo (številka 0070-26/2012-4, z dne 6. 4. 2012);
- Pravilnik o varovanju komunikacijskega in informacijskega sistema MORS (številka 007-161/2008-2, z dne 12. 6.2008);
- Navodilo o označevanju gradnikov in nosilcev elektronskih podatkov v komunikacijskem in informacijskem sistemu Ministrstva za obrambo (številka 0070-18/2007-1, z dne 22. 3. 2007);
- Navodilo o postopkih uničevanja nosilcev podatkov v elektronski obliki (številka 007-71/2008-1, z dne 6. 3. 2008)

V Slovenski vojski so na področju varovanja tajnih podatkov v enotah izdelani standardni operativni postopki (SOP). Ti so akti poveljevanja, s katerimi poveljnik predpisuje način izvedbe rutinskih opravil in aktivnosti, s ciljem usklajenega in učinkovitega delovanja enote. O uporabi SOP-a v sistemu varovanja tajnih podatkov podrobneje pišem v četrtem poglavju.

2.2.2 Dostopanje do nacionalnih tajnih podatkov

3. člen ZTP-ja določa, da v zvezi z opravljanjem svoje funkcije lahko do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov dostopa:

- predsednik republike;
- predsednik vlade;
- poslanec;
- državni svetnik;
- župan in občinski svetnik;
- minister in predstojnik vladne službe, ki je neposredno odgovorna predsedniku
- vlade;
- varuh človekovih pravic in njegov namestnik;
- guverner, namestnik in vice guverner centralne banke;
- član računskega sodišča;
- predsednik in člani Državne revizijske komisije
- sodnik;
- državni tožilec;
- generalni državni pravobranilec in
- informacijski pooblaščenec.

Osebe iz prejšnjega odstavka dobijo dovoljenje z začetkom funkcije oziroma opravljanja dela in podpisom izjave, da so seznanjene z ZTP-jem in drugimi predpisi, ki urejajo varovanje tajnih podatkov, in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi.

Nadalje 4. člen istega zakona določa, da ima dostop do tajnih podatkov brez dovoljenja pri opravljanju svoje funkcije nadzora Komisija Državnega zbora Republike Slovenije za nadzor nad delom varnostnih in obveščevalnih služb.

Vse ostale osebe, ki niso zajete v 3. oziroma 4. členu ZTP-ja lahko dostopajo do tajnih podatkov stopnje tajnosti ZAUPNO ali višje le na podlagi uspešno opravljenega varnostnega preverjanja, s katerim si pridobijo dovoljenje za dostop do tajnih podatkov, in v skladu s potrebo po seznanitvi s tajnimi podatki zaradi opravljanja funkcije ali izvajanja nalog na delovnem mestu v organu.

V skladu z 31. a členom ZTP-ja imajo vse osebe, ki opravljajo funkcijo ali delajo v organu, dostop do tajnih podatkov stopnje tajnosti INTERNO, seveda v skladu s potrebo po seznanitvi in predhodno podpisano izjavo, da so seznanjene z ZTP-jem in drugimi predpisi, ki urejajo varovanje tajnih podatkov. Predstojnik organa mora za te osebe pred podpisom izjave zagotoviti ustrezno usposabljanje s področja obravnavanja in varovanja tajnih podatkov (osnovno usposabljanje) in to izvede v skladu z 21. (program osnovnega usposabljanja), 23. in 24. členom Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov.

V kolikor predstojnik organa meni, da določene osebe v organu ne bodo dostopale niti do tajnih podatkov stopnje tajnosti INTERNO, je v sistemizaciji smiselno opredeliti tudi tista delovna mesta, na katerih se dostopa do tajnih podatkov stopnje tajnosti INTERNO. V praksi so načeloma opredeljena le delovna mesta, na katerih potrebuje oseba dovoljenje za dostop do tajnih podatkov stopnje tajnosti ZAUPNO ali višje. Če torej v sistemizaciji izrecno ni opredeljeno delovno mesto, na katerem ima oseba dostop do tajnih podatkov stopnje tajnosti INTERNO, se določba 31. a člena ZTP-ja smatra dobesedno, to je »vsi, ki opravljajo funkcijo ali delajo v organu«.

2.3 VLOGA URADA VLADE RS ZA VAROVANJE TAJNIH PODATKOV

Urad Vlade Republike Slovenije za varovanje tajnih podatkov (UVTP) je bil ustanovljen 22.01.2002, na podlagi 43. člena ZTP. Urad je vladna služba, ki bdi nad stanjem na področju tajnih podatkov. Uradu so državni organi, organi lokalnih skupnosti, nosilci javnih pooblastil in gospodarske organizacije, ki razpolagajo s tajnimi podatki, dolžni predložiti poročila, ki jih UVTP od njih zahteva. Urad predlaga ukrepe za izboljšanje varovanja tajnih podatkov, skrbi za razvoj in izvajanje ukrepov varovanja, skrbi za izvrševanje mednarodnih pogodb in obveznosti, ki jih je na področju tajnih podatkov sprejela RS. Prav tako usklajuje dejavnosti za zagotavljanje varnosti nacionalnih tajnih podatkov v tujini in tujih tajnih podatkov na domačem teritoriju. Poglavitne naloge urada so:

- izdaja dovoljenja za dostop do tajnih podatkov,
- izdaja varnostna potrdila pravnim osebam,
- izdaja varnostna potrdila za sisteme in naprave za prenos, hranjenje in obdelavo tajnih podatkov,
- potrjuje izpolnjevanje predpisanih pogojev za obravnavanje tajnih podatkov s strani posameznega organa tujim državam in organizacijam,
- predlaga varnostno preverjanje za izdajo dovoljenja za dostop do tajnih podatkov, katerih predlagatelji niso zajeti v 22. členu ZTP-ja in potrebujejo dovoljenje za dostop do tajnih podatkov tuje države ali mednarodne organizacije,

- izdaja navodila za ravnanje s tajnimi podatki tuje države oziroma mednarodne organizacije,
- nadzoruje izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države oziroma mednarodne organizacije in skladno z ugotovitvami nadzora izdaja obvezna navodila za odpravo ugotovljenih pomanjkljivosti, ki so jih organi dolžni nemudoma izvršiti,
- izmenjuje podatke z nacionalnimi varnostnimi organi in mednarodnimi organizacijami,
- pripravlja predloge predpisov, potrebnih za izvajanje ZTP-ja,
- daje mnenje o skladnosti splošnih aktov o določanju, varovanju in dostopu do tajnih podatkov z ZTP-ja,
- koordinira delovanje državnih organov, pristojnih za varnostno preverjanje ter
- predlaga ukrepe za izboljšanje varovanja tajnih podatkov.

Za namen izvrševanja pristojnosti po ZTP, ostalih zakonih in mednarodnih pogodbah urad obdeluje in vodi naslednje evidence:

- dovoljenj za dostop do tajnih podatkov (22. člen ZTP),
- dovoljenj fizičnim osebam za dostop do tujih tajnih podatkov (43b. člen ZTP),
- izdanih varnostnih dovoljenj organizacijam (35. člen ZTP),
- izdanih varnostnih dovoljenj organizacijam za dostop do tujih tajnih podatkov (43b. člen ZTP),
- začasnih dostopov do tajnih podatkov (30. člen ZTP).

UVTP tudi organizira in izvaja usposabljanja s področja varovanja tajnih podatkov in opravlja druge naloge, ki so določene s predpisi, sprejetimi na podlagi ZTP-ja.

3 VAROVANJE TAJNIH PODATKOV NA MORS IN V SV

Zaščita podatkov je sestavni del dnevnega življenja zaposlenih na obrambnem področju. Kljub določenim varnostnim ukrepom in izgrajevanju varnostne kulture ni mogoče vsem osebam popolnoma zaupati. Vedno obstaja določeno tveganje, ki ga lahko omejimo z uvajanjem novih tehničnih oziroma organizacijskih rešitev. Kljub vsemu pa nikoli ni mogoče zagotoviti popolne varnosti, saj večina ljudi ne razume enako pojma varovanja podatkov.

Pri svojem delu morajo zaposleni poznati vse določbe Zakona o tajnih podatkih, podzakonske akte, previdnostne ukrepe, ki so neposredno povezani z nediskretnimi pogovori, previdnostne ukrepe pri stikih s predstavniki tiska in potencialnimi dejavnostmi tujih obveščevalnih in varnostnih služb. Pridobljeno znanje na področju varovanja tajnih podatkov je treba periodično obnavljati. Zaradi navedenega bi morali v vsa organizirana izobraževanja in usposabljanja uvesti navedene vsebine, prilagojene udeležencem izobraževanja. Z izobraževanjem in usposabljanjem bi teoretične osnove s področja varnostne kulture in varovanja podatkov s stopnjami tajnosti dopolnili s praktičnimi izkušnjami in nasveti zaposlenih, ki so izkušnje z obeh obravnavanih področij pridobili v tujini. Le tako lahko omogočimo trajnejše znanje, ki bo služilo namenu, udeleženci pa ga bodo znali uporabiti življenju. Zato znova poudarjamo pomen poznavanja posameznikovih izkušenj in ugotavljanja potreb. Vendar pa izobraževanja ne bi bilo treba izvajati le na najnižji, individualni ravni. Varnostno kulturo bi bilo treba spodbuditi na ravni organov, ki pri svojem delu prihajajo v stik s tajnimi podatki, v ta namen pa bi se morali izobraževati tudi nadrejeni.

Na MORS je bila leta 2007 v sodelovanju s Centrom za politološke raziskave FDV opravljena raziskava o organizacijski in varnostni v upravnem delu MO in v SV. Eden od zaključkov avtorjev raziskave je bil, da je razkrivanje tajnih podatkov zunaj ministrstva v večinoma odziv na nepripravljenost vodilnih oseb v ustanovi, da bi rešili težave znotraj sistema.

3.1 VRSTE UKREPOV PRI VAROVANJU TAJNIH PODATKOV

Ukrepe lahko na podlagi slovenske zakonodaje strnemo v fizične, organizacijske in tehnične ukrepe. Terminologijo, ki jo poznata Nato in Evropska skupnost se nekoliko razlikuje od opredelitve, ki jo za varovanje tajnih podatkov poznamo v Sloveniji. Ukrepi, ki jih izvajajo na področju varovanja tajnih podatkov so razdeljeni v naslednje skupine ukrepov in sicer kadrovska varnost, fizična varnost, varnost informacij, industrijska varnost, varnost informacijskih sistemov in industrijska varnost (Čaleta, 2003: 2). Poudariti je potrebno, da zakon o tajnih podatkih predpisuje minimalne potrebne ukrepe za varovanje tajnih podatkov. To pa pomeni, da se lahko organ glede na pomembnost tajnih podatkov, ki jih varuje, odloči za restriktivnejše ukrepe, če oceni, da je to nujno potrebno.

3.1.1 Kadrovska varnost

Glavni cilj in namen kadrovske varnosti je zagotavljati ustrezen sistem varnostnega preverjanja za vse zaposlene osebe, ki bodo imele v organu dostop do tajnih podatkov stopnje tajnosti ZAUPNO in višje. To varnostno preverjanje se izvede in osebi na podlagi tega izda dovoljenje za dostop do tajnih podatkov ustrezne stopnje. Šele po uspešno končanem postopku varnostnega preverjanja se osebi odobri dostop do tajnih podatkov ustrezne stopnje.

Drugi zelo pomemben ukrep v sistemu varovanja tajnih podatkov na področju kadrovske varnosti je potreba po vedenju. Termin, ki ga pozna Nato in Evropska unija za potrebo po vedenju oz. vpogledu v tajni podatek je »need to know«. To pa pomeni, da ima oseba dostop

do tajnega podatka samo takrat, kadar se mora s tajnim podatkom seznaniti, zaradi opravljanja funkcije ali delovnih nalog. Nobena oseba se ne glede na položaj, čin ali stopnjo dovoljenja za dostop do tajnih podatkov, se ne sme seznaniti z določenim tajnim podatkom, če ne izkaže upravičene potrebe ali interesa za vpogled v tajni podatek.

Tretje pomembno področje kadrovske varnosti je dvig varnostne kulture, oziroma zavedanja o pomembnosti pravilnega rokovanja s tajnimi podatki ter ustrezen sistem usposabljanja zaposlenih s področja varovanja in rokovanja s tajnimi podatki.

Četrto pomembno področje, ki bi ga lahko opredelil na področju kadrovske varnosti je izdelava ustreznih postopkov za dostop do tajnih podatkov v izrednih primerih, kot so enkratni dostopi do tajnih podatkov zaradi nujnih potreb, čeprav oseba nima dovoljenja za dostop do tajnih podatkov ustrezne stopnje.

Kot zadnje področje, pa bi lahko opredelili protiobveščevalno ščitenje oseb in delovnih mest, na katerih se osebe seznanjajo ali obdelujejo najvišje stopnje tajnosti podatkov. Čeravno zakon o tajnih podatkih ne opredeljuje konkretnih ukrepov za navedeno področje. Jasno zakonsko podlago najdemo v 32. členu Zakona o obrambi, kjer so opredeljene protiobveščevalne in varnostne naloge, ki zajemajo tudi zaščito oseb zaposlenih na takih delovnih dolžnostih.

3.1.2 Fizična varnost

Ukrepi fizične varnosti, ki jih predvideva zakon o tajnih podatkih imajo predvsem namen preprečitve nepooblaščenega dostopa do tajnih podatkov. Ti ukrepi predvsem temeljijo na določitvi varnostnih območij ustrezne stopnje v vseh organih, ki obdelujejo in shranjujejo tajne podatke. Zavedati se moramo, da lahko učinkovito varovanje zagotovimo samo v povezavi fizičnega varovanja z vsemi drugimi segmenti in ukrepi varovanja osebja, varnosti informacij in ukrepov za zagotavljanje varnosti informacijskih in komunikacijskih sistemov.

3.1.3 Varnost informacij

V tem delu bom opredelil minimalne varnostne standarde s področja varnosti informacij. Zelo pomembno je zavedanje, da tajni podatki oz. informacije zahtevajo določene varnostne ukrepe, ki se redno izvajajo v sistemu življenjskega ciklusa teh informacij. Zagotoviti je potrebno ukrepe, ki bodo omogočali ustrezne postopke določitve stopnje tajnosti podatkom ali informacijam, njihovo označevanje in jasno prepoznavnost ter čas trajanja tajnosti, dokler mora podatek ali informacija ostati označena z ustrezno stopnjo tajnosti.

Originator je odgovoren za opredelitev stopnje tajnosti podatka, ki ga je izdelal in označil kot tajnega, hkrati pa je odgovoren za posredovanje tega podatka drugim, ki morajo biti po njegovi oceni seznanjeni z določenim tajnim podatkom. Samo originator informaciji ali podatku, ki je zajet v določenem dokumentu, lahko zniža, spremeni ali umakne stopnjo tajnosti. Seveda pa originator že ob nastanku tajnega podatka, določi način znižanja ali prenehanja stopnje tajnosti določenemu podatku (Čaleta, 2003: 5).

Določitev ustrezne stopnje tajnosti določenemu podatku vpliva na nadaljnje postopke zagotavljanja varovanja tajnega podatka in sicer na področju fizične varnosti ob njegovem shranjevanju, posredovanju ali prenosu, kroženju, uničevanju in zahtevah po ustreznih stopnjah dovoljenj za dostop do tajnih podatkov pri njegovem vpogledu. Zaradi navedenega moramo biti v praksi posebej pozorni na določitev previsoke ali prenizke stopnje tajnosti podatka, ki bi lahko vplivala na učinkovitost sistema varovanja tajnih podatkov.

3.1.4 Varnost informacijskih sistemov

Določila varnosti informacijskih sistemov opredeljujejo minimalne standarde za varovanje tajnih podatkov, ki se pošiljajo, obdelujejo ali shranjujejo v komunikacijsko informacijskih sistemih (KIS) ali omrežjih.

Zelo pomembno pri zagotavljanju varnosti informacijskih sistemov je vzpostavitev ustrezne in učinkovite varnostne organizacije za KIS v kateri ima vsak nivo točno opredeljene pristojnosti in dolžnosti v smislu zaupnosti, samostojnosti in uporabnosti tajnih podatkov, ki so shranjeni, procesirani ali obdelani v KIS ali omrežjih. Noben KIS ali omrežje ne sme biti uporabljen za shranjevanje in procesiranje tajnih podatkov ali informacij, če predhodno niso pridobili ustrezne akreditacije s strani ustreznega akreditacijskega organa v državi.

Sodobne obveščevalne službe uspešno izkoriščajo razvoj znanosti in tehnologije. Danes veliki obveščevalni sistemi ne morejo preživeti brez globalnega računalniško podprtega obveščevalno informacijskega okolja (Šaponja, 1999: 13). Z vstopom Slovenije v EU in NATO se je zanimanje tujih obveščevalnih služb okrepilo, hkrati pa sta Slovenija in njen obrambno-varnostni sistem postala predmet nadzorov držav članic EU in NATA. Državni organi bodo tudi v prihodnje morali dokazovati, da so vredni zaupanja in da so z dvigom varnostne kulture zaposlenih poskrbeli za primeren način komuniciranja.

3.1.5 Industrijska varnost

Zakon o varovanju tajnih podatkov določa, da pooblaščene osebe lahko posredujejo tajne podatke dobaviteljem, izvajalcem gradenj ali izvajalcem storitev (v nadaljevanju organizacije), če:

- organizacija izpolnjuje fizične, organizacijske in tehnične pogoje za varovanje tajnih podatkov v skladu s tem zakonom in predpisi, sprejetimi na njegovo podlagi;
- so osebe, ki bodo v organizaciji po službeni dolžnosti imele dostop do tajnih podatkov, varnostno preverjene in imajo dovoljenje za dostop do tajnih podatkov;
- organizacija zagotovi, da bo dostop do tajnih podatkov dovoljen samo tistim osebam, ki morajo imeti vpogled v te podatke po svoji službeni dolžnosti zaradi uresničevanja naročila organa;
- je imenovana oseba, pristojna za nadzor in usmerjanje varnostnih ukrepov v zvezi z izvajanjem naročila, za usposabljanje oseb, ki imajo dostop do tajnih podatkov, poročanje pristojnemu organu o okoliščinah, ki vplivajo na izdajo varnostnega dovoljenja in izvajanje drugih predpisanih ukrepov za varno obravnavanje tajnih podatkov.

Z ukrepi industrijske varnosti zagotovimo ustrezne normative, ki pripomorejo k izvajanju določenih storitev v organu s strani zunanjih izvajalcev, ki bodo za svoje delo potrebovali dostop do tajnih podatkov. Te normativi ali ukrepi pripomorejo v postopku pogajanja s podjetji za sklenitev ustreznih pogodb, ki bodo opredeljevale tudi zahteve in dolžnosti izvajalcev posla pri rokovanju ali dostopu do tajnih podatkov organa, katere bodo nujno potrebovali za izpeljavo storitve za organ.

Šele potem, ko se ugotovi, da je organizacija zadostila vsem kriterijem, se ji posredujejo tajni podatki potrebni za izvedbo storitve. Organ lahko tudi med izvajanjem storitve v organizaciji preverja ukrepe in postopke za varovanje tajnih podatkov, vendar samo v tistem delu, ki se nanaša na izvajanje omenjene storitve.

3.2 POVEZANOST VREDNOT IN VAROVANJA TAJNIH PODATKOV

Vrednote, ki jih imajo zaposleni na obrambnem področju, se razlikujejo od vrednot širše populacije. Temeljna skupna vrednota pripadnikov Slovenske vojske je domoljubje. Domoljubje je zavest pripadnosti domovini Sloveniji in nesebično opravljanje dolžnosti pri uresničevanju skupnih ciljev. Ena izmed vrednot je tudi lojalnost Republiki Sloveniji, Slovenski vojski in enoti ter povezuje pripadnike Slovenske vojske med seboj. Lojalnost Slovenski vojski pripadniku enote narekuje skrb za njeno učinkovitost. Lojalnost slovenski državi mu narekuje skrb za zaščito njenih interesov in krepitev ugleda v svetu. Lojalnost podrejenih do svojih nadrejenih je sestavni del lojalnosti vojaški organizaciji. Podrejeni so lojalni do nadrejenih tako, da izvajajo povelja, ki uresničujejo poslanstvo Slovenske vojske in podpirajo interese Republike Slovenije. Lojalnost se izraža z medsebojnim zaupanjem in spoštovanjem ter discipliniranim in odgovornim opravljanjem dolžnosti (Vojaška doktrina, 2006: 17–19).

Lojalnost kot temeljna vrednota na obrambnem področju in v Slovenski vojski je pomembna predvsem z vidika dostopanja do tajnih podatkov in njihovega obravnavanja. Vrednota je pomembna za zaposlene, ki dostopajo do tajnih podatkov ter morajo zaradi tega biti varnostno preverjeni. Ob izvedbi varnostnega preverjanja zaposlenih je prav lojalnost eden izmed najpomembnejših kriterijev, s pomočjo katerega se omogoča, da lahko zaposleni dostopa do tajnih podatkov oziroma posluje z njimi.

Najpomembnejši faktor je človek, uslužbenec organa javne oziroma državne uprave. Pomembni so odnosi med zaposlenimi, nadrejenim in podrejenimi, stopnja politične, organizacijske in varnostne kulture, občutek pripadnosti organizaciji, lojalnost in ne nazadnje seznanjenost s tem, kako ravnati.

Vrednote se udejanjajo s standardi vedenja v Slovenski vojski, za katere se njeni pripadniki zavzemajo in ki jih cenijo, ter se poučujejo na vseh ravneh izobraževanja in usposabljanja. Vrednote niso le seznam kvalitet, ki jih dosega posameznik, temveč skupna odgovornost Slovenske vojske in vsake enote. Uveljavljajo in krepijo se z voditeljstvom in usposabljanjem. Vsi pripadniki Slovenske vojske z osebnim zgledom in ravnanjem uveljavljajo njene vrednote, nadrejeni pa skrbijo, da jih podrejeni upoštevajo pri svojem delu (Vojaška doktrina, 2006: 18).

3.3 VARNOSTNA KULTURA

Varnostna kultura temelji na pričakovanju, da bodo ljudje, če bodo seznanjeni z nevarnostmi, ki jih pri delu lahko doletijo, in postopki za njihovo preprečevanje, te dosledno upoštevali pri svojem delu. Ob tem je treba poudariti, da je dobra ali slaba varnostna kultura opredeljena kot skupek odgovornih in sprejetih vrednot, zavedanja, načinov vedenja vseh, ki vstopajo v posamezen sistem. Torej je opredeljena z značilnostmi delovnega okolja ter vpliva na zaznavo in ravnanje zaposlenih glede pomembnosti, ki jo organizacija namenja varnosti.

Varnostna kultura v idealni zasnovi je odprta kultura, ki temelji na poštenju, zaupanju, komunikaciji, sodelovanju, gospodarnosti, profesionalnosti, enakosti ter spoštovanju osebne varnosti in varnosti organizacije (Hartman, 2007: 16).

Pojem varnostne kulture opredeljuje Resolucija o strategiji nacionalne varnosti kot zadnji, toda ne nepomemben temelj sistema nacionalne varnosti. V resoluciji je opredeljeno: »Za zagotavljanje nacionalne varnosti Republike Slovenije se organizira sistem nacionalne varnosti, ki temelji na pravnih, političnih, gospodarskih, materialnih, socialnozdravstvenih, informacijskih, infrastrukturnih, znanstvenih, izobraževalnih in drugih zmogljivostih države. Pri tem se ne zanemarja pomena razvitosti varnostne kulture v družbi.« Opredeljuje jo kot varnostno kulturo državljanov, posebej tistih na vodilnih in vodstvenih položajih, ter

pojasnjuje, da stopnja njene razvitosti vpliva na učinkovitost delovanja sistema nacionalne varnosti in njegov razvoj.

V širše pojmovanje varnostne kulture bi lahko umestili vprašanja, kot so, v kakšni vlogi se vidijo posamezniki znotraj sistema nacionalne varnosti, kakšen je njihov odnos do vojaškega poklica, Slovenske vojske in mirovnih gibanj, ali so pripravljeni sodelovati z obveščevalno-varnostnimi službami, kako bi se vedli ob oboroženi agresiji na Slovenijo ipd. (Grizold 1998: 107).

Z varnostno kulturo so tesno povezani tudi vrednote in stališča posameznika do najpomembnejših vprašanj nacionalne varnosti. Varnostna kultura v ožjem pomenu posega na področje organizacijske oziroma politične kulture, je njun del in je tesno povezana z verodostojnostjo, lojalnostjo, pripadnostjo, varovanjem tajnosti ter zanesljivostjo (Črnčec, 2003: 20).

Glede na definicije lahko varnostno kulturo na obrambnem področju in v SV povežemo z varovanjem tajnih podatkov oziroma z doslednim izvajanjem vseh postopkov, ki so namenjeni varovanju podatkov, prostorov in objektov, kjer se tajni podatki hranijo, kakor tudi zaščiti zaposlenih, ki se srečujejo z izdelavo, uporabo ter varovanjem. Torej je zaradi tega lahko logično nadaljevanje tajnosti, ki posameznika sili k spoštovanju vseh pravil in postopkov, ki so namenjeni varovanju tajnosti, hkrati pa mora biti usposobljen zaznati poskuse ogrožanja ter znati izvajati ukrepe za preprečevanje groženj.

Zaposleni na obrambnem področju in v SV se pri vsakodnevnem operativnem delu srečujejo z izdelavo, obravnavanjem, varovanjem, izvajanjem predpisanih ukrepov, torej tudi z varnostno kulturo, ki je temeljni predpogoj, da določeni podatki ostanejo prikriti pred nepooblaščenim dostopom in pred tujimi obveščevalnimi službami.

3.4 DOLOČBE O ZLORABI TAJNEGA PODATKA

Zakon o tajnih podatkih v četrtem odstavku 1. člena določa, da je vsakdo, ki mu je bil zaupan tajni podatek, ali ki se je seznanil z vsebino tajnega podatka, odgovoren za njegovo varovanje in ohranitev njegove varnosti. ZTP in na podlagi tega sprejeti podzakonski akti določajo skupne osnove enotnega sistema določanja, varovanja in dostopa do tajnih podatkov ter prenehanja tajnosti tajnih podatkov. Po tem zakonu 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.

Varovanje tajnih podatkov skladno s predpisi zagotavlja torej vsak organ, ki tajni podatek določi in organ, ki tajni podatek prejme ter posamezniki v teh organih, in sicer z vzpostavitvijo fizičnih, organizacijskih in tehničnih ukrepov varovanja, ki onemogočajo njihovo razkritje nepooblaščenim osebam.

Postopek ob zlorabi tajnega podatka je določen v 35. in 36. členu Uredbe o varovanju tajnih podatkov in predvideva seznanitev pooblaščenih oseb oz. organov ter zagotovitev vseh ukrepov za preprečitev nadaljnje zlorabe tajnega podatka in izsledite odtujenih tajnih podatkov. Za zlorabo se skladno s 35. členom uredbe šteje vsak nepooblaščen dostop, uničenje, odtujitev ali kakršenkoli drug dogodek, ki kaže na zlorabo tajnih podatkov. O takšnem dogodku je treba takoj seznaniti predstojnika organa oziroma osebo, ki jo pooblasti. Predstojnik organa, v katerem je bil tajni podatek zlorabljen, mora o tem obvestiti organ, ki je določil tajni podatek ter nacionalni varnostni organ in v primeru suma storitve kaznivega dejanja tudi policijo. Takoj je treba tudi zagotoviti vse ukrepe za preprečitev nadaljnje zlorabe in izsledite odtujenih tajnih podatkov.

Obvestilo o zlorabi tajnega podatka mora vsebovati (36. člen uredbe):

- podatke za identifikacijo tajnega podatka,
- kratek opis okoliščin,
- ali je bil lastnik podatkov obveščen,
- postopke in ukrepe, ki so bili izvedeni, da se prepreči nadaljnja zloraba tajnih podatkov.

Izgubo ali nepooblaščeno razkritje tajnega podatka obravnava tudi 40. člen ZTP-ja, ki določa, da je o tem treba obvestiti pooblaščeno osebo, ki mora takoj ukreniti vse potrebno, da se ugotovijo okoliščine zaradi katerih je prišlo do izgube ali razkritja nepoklicani osebi, da se odpravijo škodljive posledice in prepreči ponovna izguba oz. nepooblaščeno razkritje tajnega podatka.

ZTP v VI. poglavju (44., 44a in 45. člen) opredeljuje kazenske določbe za prekršek, ki ga stori pravna oseba ali samostojni podjetnik ali posameznik, medtem ko Kazenski zakonik v 260. členu opredeljuje kazenske določbe za izdajo tajnih podatkov.

Pravilnik o varovanju tajnih podatkov na ministrstvu za obrambo v 44. členu določa, da mora oseba ministrstva, ki je ugotovila, da je prišlo do zlorabe tajnega podatka, takoj obvestiti vodjo organizacijske enote ministrstva, ki mora o zlorabi in znanih okoliščinah zlorabe takoj obvestiti vodjo organizacijske enote ministrstva, ki je določila tajni podatek, in odrediti izvedbo dodatnih postopkov in ukrepov, da se prepreči ponovna zloraba teh podatkov.

O zlorabi tajnih podatkov mora oseba iz prejšnjega odstavka takoj obvestiti tudi OVS, ki v skladu s predpisi o zlorabi obvesti nacionalni varnostni organ oziroma policijo ali drug pristojni organ, če zloraba tajnega podatka kaže na sum storitve kaznivega dejanja.

Podrobnejše postopke in ukrepe za primer zlorabe tajnega podatka je treba na podlagi usmeritev, ki jih pripravi OVS, določiti z načrtom varovanja.

Postopki obveščanja v Slovenski vojski potekajo skladno z akti poveljevanja in kontrole. Generalštab Slovenske vojske zagotovi, da je o vseh zlorabah tajnih podatkov obveščena OVS.

3.4.1 Sodna praksa izdaje tajnih podatkov

Kaznivo dejanje izdaje tajnih podatkov je opredeljeno v 260. členu Kazenskega zakonika (KZ-1) kot ravnanje , ki ga izvrši oseba, ki v nasprotju s svojimi dolžnostmi varovanja tajnih podatkov sporoči ali izroči komu tajne podatke ali mu kako drugače omogoči, da pride do njih, ali zbira take podatke, zato da jih izroči nepoklicani osebi. Kateri podatek je tajen ne ureja KZ-1, ampak ZTP in predpisi sprejeti na njegovi podlagi.

Sodne prakse Vrhovnega sodišča na podlagi 260. člena KZ-1 še ni, obstaja le en judikat sodišča na podlagi 266. in 359. člena KZ, ki je odločilo, da ni dovolj, da gre za podatek, ki je označen s stopnjo tajnosti, ampak mora biti dokazana tudi škodljiva posledica za službo, v konkretnem primeru za policijo (Zgaga, 2012: 13).

4 NADZORI IN USPOSABLJANJA S PODROČJA TAJNIH PODATKOV V SV

V tem poglavju bom povzel ugotovitve nadzorov na področju varovanja tajnih podatkov v enotah SV v naključno izbranem letu. Namenoma ne bom navajal izvajalcev nadzora in nazivov nadzorovanih subjektov, bom pa predstavil konkretne primere, kjer je prišlo do razhajanj med ravnanji, predpisanimi v aktih, ki urejajo področje varovanja tajnih podatkov in zatečenim stanjem v enotah SV.

4.1 INŠPEKCIJSKI IN NOTRANJI NADZOR

Vlada RS je sprejela uredbi, ki opredeljujeta nadzor. To sta Uredba o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisov izdanih na njegovi podlagi in inšpekcijski nadzor, ki ga predpisuje Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja. ZTP je v dopolnitvi leta 2006 (ZTP-B) uvedel inšpekcijski nadzor na področju tajnih podatkov. Na obrambnem področju nadzor izvaja Inšpektorat Republike Slovenije za obrambo (IRSO). Z vzpostavitvijo inšpekcijskega nadzora je dosežena večja enotnost pri izvajanju predpisov s področja tajnih podatkov. Notranji nadzor, ki ga izvaja predstojnik le znotraj »svojega« organa, ni zagotavljal enotne prakse na tem področju. Prek inšpekcijskega nadzora pomembne informacije pridobiva tudi nacionalni varnostni organ, ki je pristojen za spremljanje stanja ter razvoj in izvajanja standardov varovanja tajnih podatkov. Delo inšpektorata na področju tajnih podatkov opredeljujejo členi od 42a do 42d ZTP. V postopku izvajanja nadzora ZTP in prekrškovnega postopka, so inšpektorji zavezani subsidiarni uporabi ZUP in Kazenskega zakonika.

Inšpektorat opravlja nadzor v enotah na podlagi 86. in 87. člena Zakona o obrambi, Pravilnika o inšpekcijskem nadzoru na obrambnem področju in Načrta dela Inšpektorata Republike Slovenije za obrambo za tekoče leto. Za odpravo morebitnih nepravilnosti, ugotovljenih z nadzorom, se določijo ukrepi in roki za njihovo odpravo.

4.2 PREGLED UGOTOVLJENIH POMANJKLJIVOSTI

4.2.1 Izvajanje notranjega nadzora

Notranji nadzor se izvaja v skladu z Uredbo o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisi, izdanimi na njegovi podlagi.

Notranji nadzor na področju varovanja tajnih podatkov se opravlja v obliki splošnega ali tematskega nadzora. S splošnim nadzorom se preverjajo vse dejavnosti organa, ki se nanašajo na izvajanje določb zakona in predpisov, izdanih na njegovi podlagi, da se ugotovita zakonitost in strokovnost dela s tajnimi podatki. S tematskim nadzorom se preverjajo posamezne dejavnosti organa, ki se nanašajo na izvajanje določb zakona in predpisov, izdanih na njegovi podlagi. Nadzor se opravlja na podlagi letnega načrta oziroma odločitve predstojnika organa in je lahko napovedan ali nenapovedan. Notranji nadzor v Slovenski vojski se prične na podlagi ukaza načelnika Generalštaba Slovenske vojske.

V odredbi oziroma ukazu morajo biti navedeni vrsta in vsebina nadzora, organizacijska enota, v kateri se bo izvajal nadzor, za nadzor pooblaščeni delavci, čas nadzora,

nadzorovano obdobje in pogoji, ki jih mora izpolniti vodja nadzirane enote ali tisti, ki ga nadomešča, za neovirano izvedbo nadzora.

Za nadzor pooblaščeni delavec oziroma vodja nadzora v sodelovanju z drugimi za nadzor pooblaščenimi delavci pred izvedbo pripravi načrt v skladu z odredbo, v katerem konkretizira vsebino nadzora in naloge posameznih, za nadzor pooblaščenih delavcev. Namesto načrta nadzora se v Slovenski vojski vsebina nadzora in naloge posameznih, za nadzor pooblaščenih delavcev, opredeli v ukazu.

Pred izvedbo nadzora vodja nadzora seznani vodjo organizacijske enote ali osebo, ki ga nadomešča, o odredbi oziroma ukazu o izvedbi nadzora in načrtu oziroma ukazu za nadzor, če o tem še ni bil seznanjen in mu vroči odredbo oziroma ukaz, če mu pred tem še ni bil vročen.

Poročilo o nadzoru se izdela v skladu z 11. členom Uredbe o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisi, izdanih na njegovi podlagi. Izvod poročila se pošlje tudi Inšpektoratu Republike Slovenije za obrambo.

Na področju izvajanja notranjih nadzorov je bilo ugotovljeno, da se le ti v enotah izvajajo, niso pa povsod postopki izvedeni v skladu s Pravilnikom o varovanju tajnih podatkov na ministrstvu za obrambo in Uredbo o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisi, izdanih na njegovi podlagi.

4.2.2 Osnovno in dodatno usposabljanje po ZTP

V enotah SV se izvajajo osnovna in dodatna usposabljanja, ki se načrtujejo z načrti dela. Osnovno usposabljanje zajema seznanitev s predpisi, ki urejajo področje obravnave tajnih podatkov, dodatno usposabljanje pa se izvaja po programu, ki ga je predpisal UVTP. Usposabljanja izvajajo osebe, ki morajo imeti ustrezne certifikate oziroma potrdila za predavatelje zakona o tajnih podatkih.

Do tajnih podatkov stopnje INTERNO lahko dostopajo vse osebe zaposlene v MORS, ko opravijo osnovno usposabljanje s področja ravnanja s tajnimi podatki in podpišejo izjavo, da so seznanjene z Zakonom o tajnih podatkih in predpisi izdanimi na njegovi podlagi ter se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi.

Oseba podpiše izjavo o seznanjenosti z ZTP-jem po opravljenem usposabljanju. Pomanjkljivost, ki je bila ugotovljena v nadzoru se nanaša na podpis izjave pripadnika, ki je podpisal izjavo preden se je udeležil osnovnega usposabljanja.

Dodatnega usposabljanja se morajo enkrat letno udeležiti vsi zaposleni, ki imajo dostop do tajnih podatkov stopnje ZAUPNO in višje. Nadzor je pokazal, da se v nekaterih enotah premalokrat v letu načrtuje usposabljanje, zato ne uspe zajeti vseh zaposlenih. Zaradi specifike dela v SV je, po oceni izvajalca nadzora, smotrno usposabljanja načrtovati najmanj enkrat mesečno.

4.2.3 Ocena možnih škodljivih posledic

Dokumentom se tajnost določeni na podlagi ocene možnih škodljivih posledic, ki bi lahko nastale, če bi tajni podatek prišel v nepooblaščene roke. Zaradi tega morajo biti izdelane skrbno in vsebovati konkretne opise posledic.

Ocena možnih škodljivih posledic je pisna in obvezna za vsak dokument, ki vsebuje tajni podatek. Ocena možnih škodljivih posledic nima stopnje tajnosti in se hrani kot priloga dokumenta pri organu, ki je stopnjo tajnosti določil. Ocena možnih škodljivih posledic je obrazložitev možnih škodljivih posledic v primeru razkritja podatka nepooblaščeni osebi. V oceno tudi zapišemo način prenehanja tajnosti skladno z 18. členom Zakona o tajnih podatkih.

Strokovno mnenje UVTP-ja na vprašanje, ali je treba dokument, ki je pravilno označen s stopnjo tajnosti in je evidentiran, ima žig in podpis pooblaščene osebe, ne pa tudi ocene možnih škodljivih posledic, obravnavati kot tajen, je pritrdilno. Ocena možnih škodljivih posledic je priloga arhivskemu izvodu dokumenta, prejemniki z dokumentom ravnajo skladno s predpisi o varovanju tajnih podatkov, čeprav z oceno možnih škodljivih posledic niso seznanjeni in je ne poznajo. Pri dokumentih starejšega datuma, pred uveljavitvijo Zakona o tajnih podatkih v letu 2003, ocene možnih škodljivih posledic ni bilo treba izdelovati, zato jo ob preoznačitvi prav tako ni treba posebej izdelovati. Preoznačitev stopnje tajnosti je izrecno določena v 48. členu ZTP-ja, zato se z dokumentom ravna v skladu z določeno stopnjo tajnosti. Če bi ob ponovni uporabi tovrstnega dokumenta ocenili, da je stopnjo tajnosti treba povišati ali znižati, bi to morali pisno obrazložiti, kar bi štelo za oceno možnih škodljivih posledic.

V nadzoru je bilo ugotovljeno, da pri določenih dokumentih s tajnimi podatki ni priložene ocene možnih škodljivih posledic, pri nekaterih dokumentih pa so škodljive posledice navedene presplošno, kar ne daje zadostne utemeljitve potrebe po dodelitvi stopnje tajnosti vsebovanim podatkom. V nekaterih primerih je ocena samo dikcija iz ZTP-ja, pojavi se tudi ocena, ki je kopirana iz drugega dokumenta in se nanaša na povsem drugo temo, ki jo sicer obravnava stopnjevani dokument.

Ocena možnih škodljivih posledic je eden ključnih dokumentov pri presojanju prevladujočega javnega interesa v zvezi z razkritjem podatkov, ki so določeni kot tajni, zato je pomembno, da je izdelana z vso skrbnostjo osebe, ki je stopnjo tajnosti določila.

4.2.4 Pregled nosilcev tajnih podatkov

Letne preglede tajnih podatkov opravijo osebe, ki so v SV pristojne za določanje, spremembo ali preklic stopnje tajnosti tajnim podatkom ali osebe, ki jih za pregled pisno pooblastijo vodje organizacijskih enot. Vodje organizacijskih enot SV ravni poveljnikov bataljonov, njim enake ali višje enote morajo zagotovit letne preglede tajnih podatkov.

Pri letnem pregledu tajnih podatkov je potrebno zagotoviti, da se tajni podatki označeni s stopnjo tajnosti STROGO TAJNO pregledajo enkrat na leto, oziroma pred njihovo oddajo v stalno zbirko dokumentarnega gradiva, ostale stopnje tajnosti pa vsake tri leta oziroma pred njihovo oddajo v stalno zbirko dokumentarnega gradiva. Za dokumente s tajnimi podatki, ki so v stalni zbirki dokumentarnega gradiva, se pregled potrebe po njihovi tajnosti in ustreznosti stopnje tajnosti oceni ob ponovni uporabi dokumenta.

Pri letnem pregledu tajnih podatkov je potrebno oceniti, ali še obstaja potreba po njihovi tajnosti in ali je stopnja tajnosti še ustrezna. Nosilec tajnega podatka se po pregledu označi z datumom in podpisom osebe, ki je opravila pregled. Na nosilcu tajnih podatkov se vidno označi, da tajnost ostane nespremenjena, se prekliče ali spremeni. Za spremembo stopnje tajnosti podatka je potrebno pripraviti novo pisno oceno možnih škodljivih posledic, ki se priloži predhodni oceni možnih škodljivih posledic.

Ugotovljeni sta bili dve pomanjkljivosti. Prva je ta, da se v enotah se pregled lastnih tajnih podatkov z namenom ugotoviti ali stopnja tajnosti podatkov še ustreza ali ne do dneva

inšpekcije še ni izvajal, so pa enote po ugotovljenem stanju začele aktivnosti za izvedbo pregleda.

Druga ugotovljena nepravilnost govori o mešanju pojmov pri pregledu tajnih podatkov. Pri pregledu moramo upoštevati 15. člen Pravilnika o varovanju tajnih podatkov na ministrstvu za obrambo in 30. člen Uredbe o varovanju tajnih podatkov.

Pravilnik določa,da mora vodja organizacijske enote ministrstva zagotoviti, da se bodo izvajali pregledi tajnih podatkov, ki sodijo v pristojnost organizacijske enote v skladu s predpisi. Pri pregledu je treba oceniti, ali še obstaja potreba po njihovi tajnosti in ali je stopnja tajnosti še ustrezna. Nosilci tajnih podatkov se po pregledu označijo z datumom in podpisom osebe, ki je pregled opravila. Na nosilcu tajnih podatkov se vidno označi, da tajnost:

- ostane nespremenjena,
- se spremeni,
- se prekliče.

Na drugi strani Uredba o varovanju tajnih podatkov v 30. členu govori o uničenju tajnih podatkov v organu. Gre za podatke, ki niso nastali doma, temveč smo jih prejeli informativno. Uničenje mora opraviti najmanj tričlanska komisija, izdelati zapisnik in zadostiti ostalim zahtevam uredbe.

Če povzamem, dokumenta, ki smo ga izdelali v organu, ne moremo komisijsko uničiti, ampak ravnamo po 15. členu pravilnika. Tajnemu podatku, ki smo ga prejeli informativno pa po drugi strani ne moremo spreminjati stopnje tajnosti.

4.2.5 Določanje stopnje tajnosti

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 zaradi razlogov določenih v ZTP potrebno zavarovati pred nepoklicanimi osebami in ki je skladno s tem zakonom določen in označen za tajno. Sem spadajo tudi sistemi, naprave, projekti, načrti, tehnološke, gospodarske, raziskovalni projekti.

14. člen Zakona o tajnih podatkih določa, da mora pooblaščena oseba pri določanju tajnosti podatka določiti najnižjo stopnjo tajnosti, ki še zagotavlja varovanje podatka, potrebno za varstvo interesov ali varnosti države.

Dosledno upoštevanja omenjenega člena omogoča pravilen pregled nad stopnjevanimi dokumenti. Praksa iz devetdesetih let je pokazala, da je nastala poplava dokumentov z različnimi stopnjami tajnosti, do katerih pa večina dokumentov ni bila upravičena. Zato je pri odločanju, katero stopnjo tajnosti določimo dokumentu pomembna kakovostna presoja pri izdelavi ocene možnih škodljivih posledic.

Pregledi stopnjevanih dokumentov in pobude za spremembo stopnje tajnosti pripomorejo k ohranitvi samo tistih tajnih podatkov, ki morajo ostati stopnjevani.

4.2.6 Pobuda za spremembo stopnje tajnosti

Pobudo za spremembo ali preklic stopnje tajnosti podatka lahko skladno s predpisi poda vsak prejemnik tajnega podatka in jo posreduje neposredno nadrejenemu, kar določa 14. člen Pravilnika o varovanju tajnih podatkov na ministrstvu za obrambo. Na podlagi pobude lahko nadrejeni predlagajo spremembo ali preklic tajnosti podatka osebi iz 9. člena

pravilnika, v čigar pristojnost sodi tajni podatek, česar pa nekateri nadzorovani zaposleni niso poznali in posledično niso upoštevali določbe o pobudi za znižanje stopnje tajnosti.

4.2.7 Označevanje delovnega gradiva

Pravilnik o varovanju tajnih podatkov na ministrstvu za obrambo v 13. členu določa, da delovno in pomožno gradivo, ki se uporablja oziroma nastane pri izdelavi dokumentov, ali medijev ki vsebujejo tajne podatke ter ni namenjeno drugim osebam in ga izdelovalec takoj po končanju izdelave dokumenta ali drugega medija, ki vsebuje tajni podatek, uniči, ker presodi, da ga ne bo več potreboval pri izdelavi dokumenta, ki vsebuje tajni podatek, se označi kot tajni podatek vendar se ne evidentira. Uničenje se izvede brez komisijskega zapisnika.

Delovno in pomožno gradivo, ki nastane pri izdelavi dokumenta, ki vsebuje tajen podatek in ki ni takoj uničeno, se v skladu s pisno oceno škodljivih posledic označi z ustrezno stopnjo tajnosti. V primeru posredovanja delovnega gradiva tretjim osebam, se ga evidentira in obravnava po predpisih, ki urejajo poslovanje javne uprave z dokumentarnim gradivom.

V nadzoru je bilo ugotovljeno, da se z delovnim gradivom ni ravnalo v skladu s pravilnikom, prihajalo je do mešanja ravnanj iz prvega in drugega odstavka 13. člena.

4.2.8 Obravnavanje tajnih podatkov izven varnostnih območij

O obravnavanju tajnih podatkov izven varnostnih območij govori Uredba o varovanju tajnih podatkov v 16. členu in Pravilnik o varovanju tajnih podatkov na ministrstvu za obrambo v 23. členu.

Tajni podatki se lahko obravnavajo zunaj varnostnega območja, če je prostor ali območje, v katerem se tajni podatek obravnava, fizično ali tehnično varovan, dostop do prostora pa je nadzorovan. Oseba, ki obdeluje tajni podatek zunaj varnostnega območja, mora imeti tajni podatek ves čas pod nadzorom. Po končani obdelavi tajni podatek vrne v varnostno območje.

Kadar se mora tajni podatek stopnje tajnosti ZAUPNO ali višje stopnje tajnosti zaradi izvedbe točno določene naloge obravnavati zunaj prostorov določenega organa, mora odgovorna oseba izdelati načrt ukrepov in postopkov za varovanje tajnega podatka glede na njegovo stopnjo tajnosti. Ukrepi in postopki morajo biti primerljivi z ukrepi in postopki, ki so predpisani za posamezno varnostno območje.

Vsak iznos ali vnos nosilca tajnega podatka stopnje tajnosti ZAUPNO in višje stopnje zunaj varnostnega območja se evidentira. Oseba, ki prevzame tajni podatek, to potrdi z lastnoročnim podpisom in s tem prevzame skrb za varnost tajnega podatka.

Načelnik Generalštaba SV določi poveljnike, ki smejo dovoliti odnašanje tajnih podatkov iz varnostnih območij v objektih Slovenske vojske. Odnašanje tajnih podatkov stopnje ZAUPNO in višje se evidentira. Evidenca vsebuje podatke o številki dokumenta, stopnji tajnosti, datumu, uri in minuti, ko je bil tajni podatek odnesen ali prinesen (vrnjen), ime osebe, ki je tajni podatek odnesla ali prinesla in podatek o tem, kje se bo tajni podatek nahajal.

Med izvajanjem nadzora se je pokazalo nedosledno spoštovanje zahtev iz predpisov, ki urejajo obravnavanje tajnih podatkov izven varnostnih območij. Prihajalo je do neskladij s predpisi, do odtekanja tajnih podatkov na ta način ni prišlo.

4.2.9 Pooblastilo osebam, ki kopirajo stopnjevane dokumente

Pravilnik o varovanju tajnih podatkov na ministrstvu za obrambo v 1. odstavku 24. člena določa, da morajo biti fotokopirni stroji, telefaksi in druge naprave za razmnoževanje in prenos tajnih podatkov, nameščeni v varnostnem območju, dodatno zavarovani, tako da jih lahko uporabljajo samo osebe, ki so posebej pooblaščene za ravnanje s temi napravami. Pooblastilo izda vodja organizacijske enote ministrstva, v čigar pristojnost sodi varnostno območje.

Med nadzorom je bilo ugotovljeno, da v enoti ni bilo pooblastila osebi, ki upravlja z naštetimi napravami v varnostnem območju.

4.2.10 Urejanje področja tajnih podatkov s SOP-i

V podrejenih enotah izdajajo SOP-e poveljniki enot za svoje enote. Če je vsebina iz istega področja kot ga obravnava SOP nadrejenega, ne sme biti z njim v neskladju. V primeru, ko standardni operativni postopek velja za več ravni poveljevanja, se v originalni obliki posreduje v vse enote in poveljstva. Podrejenim poveljnikom v tem primeru ni potrebno izdajati svojega SOP-a s tega področja (pod pogojem, da SOP z višje ravni opredeljuje vse potrebne postopke).

Splošno urejanje področja varovanja tajnih podatkov s SOP-i, se po besedah izvajalcev nadzora ni izkazalo za učinkovito, saj je bilo odkrito nekaj neskladij s predpisi, ki že sicer dokaj podrobno urejajo področje varovanja tajnih podatkov. V primeru neskladja je nevarnost pojava neenotnega obravnavanja tajnih podatkov.

Izdelava standardnega operativnega postopka je smiselna in priporočljiva v specifičnih primerih varovanja tajnih podatkov, ko se srečamo s sredstvi in pogoji za katere obstoječi predpisi ne definirajo konkretnega ravnanja. Na ta način naj se ureja vzpostavitev varnostnega območja v terenskih pogojih ali ravnanje z oborožitvenimi sistemi ali njihovimi deli, katerim je določena stopnja tajnosti.

4.2.11 Označevanje gradnikov in nosilcev elektronskih podatkov

Navodilo o označevanju gradnikov in nosilcev elektronskih podatkov v komunikacijskem in informacijskem sistemu Ministrstva za obrambo predpisuje da mora biti vsaka naprava, ki predstavlja gradnik KIS MO na vidnem mestu jasno označena s stopnjo tajnosti podatkov, skladno z oznakami iz Zakona o tajnih podatkih.

Navodilo v 3. členu predpisuje, da se za označevanje uporabijo naslednje barvne oznake:

- · za oznako INTERNO se uporabi črn napis INTERNO na rumeni podlagi;
- · za oznako ZAUPNO se uporabi črn napis ZAUPNO na zeleni podlagi;
- · za oznako TAJNO se uporabi črn napis TAJNO na modri podlagi in
- · za oznako STROGO TAJNO se uporabi črn napis TAJNO na rdeči podlagi.

4.3 POMEN USPOSABLJANJA O VAROVANJU TAJNIH PODATKOV

Za vse osebe, ki dostopajo do tajnih podatkov, mora država zagotoviti ustrezne oblike usposabljanja in izpopolnjevanja v obliki seminarjev, delavnic, predavanj, pogovorov na individualni ravni in drugo. Izobraževanje je še posebej pomembno zato, ker je v Kazenskem zakoniku Republike Slovenije za izdajo tajnih podatkov predvidena zaporna kazen. Posameznik, ki podpiše izjavo, da je seznanjen z zakonodajo, ki ureja varovanje tajnih

podatkov, bi moral dejansko biti usposobljen na tem področju. V primeru kršitve varovanja tajnih podatkov bi lahko prišlo do zelo neugodnih scenarijev, saj sta na prvem mestu za varovanje tajnih podatkov odgovorna posameznik in državni organ, ki izda dovoljenja za dostop.

Kot je že omenil Hartman (2007: 78) je usposabljanje odgovornost vseh organov javne uprave, analiza potreb po usposabljanju pa je odgovornost vodilnih javnih uslužbencev. Za doseganje kakovosti dela javnih uslužbencev mora biti v ta namen v javni upravi omogočena ustrezna raven usposabljanja in izpopolnjevanja. Urad vlade Republike Slovenije za varovanje tajnih podatkov je tovrstna izobraževanja začel izvajati konec leta 2005. Kot pravi Korošec, (2006: 57) nam uspešno opravljeno varnostno preverjanje še ne zagotavlja pravilnega ravnanja s tajnimi podatki, ljudi je treba tudi izobraziti. Zavedati se namreč moramo, da še tako dober sistem varovanja tajnih podatkov ne pomeni nič, če nimamo dobro usposobljenih ljudi, ki se z njimi ukvarjajo.

4.4 IZVEDBA USPOSABLJANJA S PODROČJA TAJNIH PODATKOV

Usposabljanje s področja ravnanja s tajnimi podatki je obvezna oblika usposabljanja za vse osebe, katerim je bilo izdano dovoljenje za dostop do tajnih podatkov. Z obvezno obliko usposabljanja je zakonodajalec želel zagotoviti večjo varnost tajnih podatkov, ki se obdelujejo in varujejo pri subjektih zavezanimi Zakonu o tajnih podatkih.

4.4.1 Osnovno in dodatno usposabljanje

Način in izvajanje usposabljanja sta opredeljena v Uredbi o varnostnem preverjanju in izdaji dovoljenja za dostop do tajnih podatkov. Členi 21 do 23 opredeljujejo osnovno in dodatno usposabljanje ter izvajalce usposabljanja. Osnovno usposabljanje se izvede za osebe, preden jih predstojnik predlaga v postopek varnostnega preverjanja ali preden podpišejo izjavo o seznanitvi s predpisi s področja tajnih podatkov. Dodatnega usposabljanja se morajo enkrat letno udeležiti osebe, ki imajo dovoljenje za dostop do tajnih podatkov ZAUPNO ali višje ter določajo stopnje tajnosti, zaradi opravljanja funkcije ali izvajanja nalog na delovnih mestih v ministrstvih. Usposabljanja so se dolžne udeležiti tudi osebe, ki v civilnih organizacijah skrbijo za varno obravnavanje tajnih podatkov, predstojniki organov ali organizacij, ki izvajajo notranji nadzor, ter osebe, ki jih določi predstojnik organa in organizacije. Dodatno usposabljanje mora obsegati skrajšano obliko osnovnega usposabljanja, vključevati mora morebitne nove predpise in vsebine s posameznih področij obravnavanja in varovanja tajnih podatkov, za katere je bilo z notranjim, inšpekcijskim nadzorom in nadzorom Nacionalnega varnostnega organa ugotovljeno, da se izvajajo pomanjkljivo, oziroma druge vsebine, za katere predstojnik meni, da jih je treba vključiti v program dodatnega usposabljanja. Okvirni program izdela nacionalni varnostni organ v sodelovanju s pristojnima inšpektoratoma, ki sta Inšpektorat Republike Slovenije za notranje zadeve in Inšpektorat Republike Slovenije za obrambo. Uredba o varnostnem preverjanju določa tudi, da osnovno in dopolnilno usposabljanje izvajajo pooblaščeni delavci OVS in predavatelji Zakona o tajnih podatkih iz organa S/G/J-2.

Izvedbo dodatnega usposabljanja predlagam na način, kot sem ga uporabil v drugi točki tega poglavja. Iz popisa ugotovljenih pomanjkljivosti, ki jih odkrije nadzor ali kdorkoli, ki se pri svojem delu srečuje s tajnimi podatki sestavimo predavanje, ki ga v načrtovanih terminih podamo vsem, ki morajo dodatno usposabljanje opraviti. S tem bomo zadostili namenu dodatnega usposabljanja in se izognili dolgočasnemu vsakoletnemu ponavljanju istih tem.

4.4.2 Usposabljanje iz varnostne kulture

Poleg naštetih usposabljanj je potrebno izvajati usposabljanja s področja varnostne kulture. Zaposlene moramo usposobiti, kako ukrepati ter katere varnostne ukrepe v določeni situaciji uporabiti, da bo dosežena preventivna prvina varnosti, kar visoko izgrajena varnostna kultura nedvomno je. Glavni cilj izobraževanja zaposlenih je, da se usposobijo za varovanje podatkov s stopnjami tajnosti ter tako dvignejo varnostno kulturo na raven, ki jo pričakuje SV. Hartman (2007: 90) predlaga uvedbo predmeta Varnostna kultura in varovanje podatkov v sistem vojaškega šolstva, ker bi na ta način vsi udeleženci usposabljanja med predavanji in praktičnim delom dojeli pomen varnostne kulture in varovanja tajnih podatkov. Poleg osnovnega in dopolnilnega izobraževanja, ki ga predpisuje novela Zakona o tajnih podatkih in varnostne kulture predlaga še izvajanje izobraževanja in usposabljanja, s katerimi bodo zaposleni pridobili nekatera specialistična znanja s področja varovanja tajnih podatkov. Posameznik bi moral poznati vse določbe Zakona o tajnih podatkih, podzakonske akte in previdnostne ukrepe, ki so neposredno povezani z možnostjo odtekanja tajnih podatkov. Po zaključku usposabljanja bi posameznik pridobil ustrezno potrdilo o udeležbi na usposabljanju.

4.4.3 Usposabljanje v elektronski učilnici

Perspektiven projekt je odsek J-2 GŠSV pripravil za pripadnike Slovenske vojske, ki naj bi v prihodnosti prešli na novo obliko dodatnega usposabljanja s področja ravnanja s tajnimi podatki. Dosedanjo klasično predavanje bo nadomestilo usposabljanje preko e-učilnice, katera se je v organih, ki jo že uporabljajo, izkazala kot učinkovita metoda. S takšnim načinom usposabljanja želijo doseči večjo učinkovitost sprejemanja informacij s področja ravnanja s tajnimi podatki ter hkrati zmanjšati potrebno logistično oskrbo, kajti s to obliko usposabljanja odpadejo potrebne rezervacije predavalnic, prevozi na usposabljanje, odsotnost iz delovnega mesta itd.

Z namenom, da bi usposabljanje v e-učilnici uporabnikom čim bolj približali, bo odprt »Forum ZTP«, kjer lahko postavljamo vprašanja, izpostavljamo morebitne probleme s katerimi se srečujemo pri predelavi gradiva ali preverjanju znanja ter podajamo pobude za izboljšanje izvedbe usposabljanja.

Vsak imetnik veljavnega dovoljenja bo moral enkrat letno predelati učno gradivo v e-učilnici. Gradivo je zbrano v predmetu Dodatno usposabljanje s področja tajnih podatkov, razdeljeno je na 34 sklopov, med katerimi listamo in se hkrati seznanjamo s snovjo, ki jo moramo poznati na področju ravnanja s tajnimi podatki. Ta del ni časovno omejen. Avtor predmeta opozarja, da je dobro preučiti vsebino predmeta in se šele nato lotiti preverjanja znanja, kar pa je normalen in zaželen postopek pri vseh predmetih v elektronski učilnici.

Drugi del predmeta Dodatno usposabljanje s področja tajnih podatkov je preverjanje znanja. Ustvarjen je nabor 70-ih vprašanj, ki zajemajo tematiko iz učnega gradiva. Od teh jih računalnik naključno izbere 30 in ponudi v reševanje testiranemu. Vprašanja že ponujajo najmanj dva možna odgovora, med katerimi iščemo pravilnega. Za preverjanje znanja je na voljo 90 minut. Vprašanja pri preverjanju znanja se točkujejo, pogoj za uspešno zaključeno usposabljanje pa je doseženih vsaj 18. točk (60%). Oseba, ki bo uspešno zaključila usposabljanje bo prejela potrdilo o opravljenem usposabljanju, v nasprotnem primeru pa bo lahko čez teden dni preverjanje znanja ponovila.

Na ta način so usposabljanje s področja ravnanja s tajnimi podatki že opravili pripadniki Slovenske vojske, ki opravljajo delo na mednarodnih vojaških predstavništvih v tujini. Prve izkušnje govorijo v prid zastavljenemu projektu in verjetno razširitev na vse pripadnike SV, ki morajo opravljati letna dodatna usposabljanja.

5 ZAKLJUČEK

Demokratična država mora za vse državljane omogočiti enake pogoje za dostop do tajnih podatkov. Določanje podatkov za tajne je v nasprotju z načelom javnosti, zato je nujno potrebno, da je področje varovanja tajnosti dobro zakonsko urejeno. To je pri nas zagotovljeno z Zakonom o tajnih podatkih, ki je primerljiv z zakonodajo drugih evropskih držav, ki so prav tako morale uskladiti ureditev varovanja tajnih podatkov s politiko Evropske unije. Enotno urejanje tajnih podatkov je zelo pomembno in enotna terminologija je prav gotovo pomemben del varovanja tajnosti. Varovanje tajnih podatkov ni pomembno samo po sebi, temveč je nujno zaradi varovanja vrednot, ki veljajo v družbi. Varovanje tajnih podatkov vzpostavi ravnovesje med tveganjem (ogrožanjem) in obvladovanjem (nadzorom) tega tveganja. To pa sta bistvena naloga in cilj sistemskega varovanja. Prvo fazo sistemskega varovanja predstavlja identifikacija oziroma prepoznava ogrožanj, nato sledi njihova analiza. V tretji fazi se pojavijo dejavnosti, ki so usmerjene v preprečevanje groženj oziroma nevarnosti, ki ogrožajo podatke, ter v odpravljanje morebitnih škodljivih posledic. Strinjam se, da je pri preučevanju tako širokega področja, kot je varovanje tajnih podatkov, smiselno upoštevati izsledke strokovnjakov, ki se ukvarjajo s to tematiko in privzeti delitev varovanja tajnih podatkov na posamezne sklope in ukrepe, saj nam to omogoči podrobnejši vpogled in lažjo obravnavo konkretnih primerov.

Prvo hipotezo, ki trdi, da ima Slovenija pravno urejeno področje varovanja tajnih podatkov lahko potrdim Ugotovil sem, da je področje varovanja tajnih podatkov pravno zelo podrobno in sistematično regulirano. Pravni akti, ki obravnavajo varovanje tajnih podatkov v Republiki Sloveniji omogočajo transparentno in učinkovito varovanje tajnih podatkov. S spremembami, ki so bile izvedene po sprejemu Zakona o tajnih podatkih, smo zadostili predpisom, ki jih opredeljujeta EU in zveza Nato. Spremembe so bile izvedene v smeri doseganja minimalnih standardov. Minimalni standardi varovanja podatkov so zagotovljeni povsod, nekatera določila pa so celo strožja, kot jih predpisujeta organizaciji, katerih članica je tudi Republika Slovenija. Imamo uveljavljeno tristopenjsko varnostno preverjanje, odvisno od stopnje tajnih podatkov, do katerih naj bi posameznik dostopal. Tudi morebitna dopustnost poseganja in zbiranja osebnih podatkov zaposlenega za potrebe varnostnega preverjanja se mi ne zdi sporna z vidika kršenja človekovih pravic. Do zlorabe tajnih podatkov načeloma težje pride zaradi sistemske napake varovanja, ampak zaradi individualne napake ali nelojalnosti posameznika, ki ima dostop do tajnih podatkov. Razkritje tajnosti je sankcionirano v kazenskem zakoniku in aktih o zaposlitvi.

Varovani podatki so bistvenega pomena za državo, zato mora oseba, ki ima dostop do tajnih podatkov imeti določene kvalitete, ki se preverjajo v postopku varnostnega preverjanja. S tem se že preventivno izločijo potencialni storilci kaznivega dejanja izdaje tajnih podatkov. Strog režim izvajanja varnostnega preverjanja in varovanje človekovih pravic se ne izključujeta. Močna država z demokratično ureditvijo je namreč porok za varovanje temeljnih človekovih pravic in svoboščin. Področje dostopa zaposlenih do tajnih podatkov v Slovenski vojski po mojih ugotovitvah ne predstavlja rizika, saj se v zadnjih letih ne pojavljajo večje nepravilnosti.

Druga hipoteza, ki se glasi, da dodatno usposabljanje s področja tajnih podatkov zmanjšuje nepravilna ravnanja vsekakor drži, saj se večina nepravilnosti, ki so bile odkrite v postopkih nadzora nad varovanjem tajnih podatkov v Slovenski vojski, pojavlja zaradi nepopolnega poznavanja in s tem posledično neupoštevanja področnih predpisov. Skozi usposabljanja morajo zaposleni vzdrževati nivo znanja na področju varovanja tajnih podatkov in ga periodično obnavljati. Le tako lahko omogočimo trajnejše znanje, ki bo služilo namenu, udeleženci pa ga bodo znali uporabiti pri svojem delu. Prav tako so na področju varovanja tajnih podatkov pomembne posameznikove izkušnje.

V Slovenski vojski se je z uvedbo inšpekcijskega nadzora poenotilo obravnavanje tajnih podatkov. Odrejeni ukrepi po opravljenem nadzoru poskrbijo za odpravo pomanjkljivosti in vodijo k izboljšanju stanja na nadziranem področju. Poleg tega sem ugotovil, da so rezultati nadzora, ne samo inšpekcijskega, odlična podlaga za izvajalce dodatnih usposabljanj, saj identificirajo nepravilnosti, katerim moramo posvečati več pozornosti in jih zato vključimo v letni nabor tem za usposabljanje.

Na področju varovanja tajnih podatkov poteka v Slovenski vojski več vrst usposabljanj. Temeljni obliki ostajata osnovno in dodatno usposabljanje, ki pa se dopolnjujeta predvsem z usposabljanjem iz varnostne kulture. Zaposleni v Slovenski vojski z različnimi oblikami izobraževanja in usposabljanja sprejemamo nova znanja. Pridobljeno znanje pozneje uporabimo pri svojem strokovnem delu, omogoča pa nam tudi kvalitetnejše opravljanje operativnih nalog, kjer smo zaposleni. Med aktivnosti, ki pripomorejo k uspešnemu varovanju tajnih podatkov in jih lahko pogojno uvrstimo med različne oblike usposabljanj so tudi dejavnosti, ki izgrajujejo lojalnost posameznika in krepijo njegovo pripadnost organizaciji.

LITERATURA IN VIRI

KNJIGE, ČLANKI

1. ČALETA, Denis (2003). Varnostno preverjanje v SV. Bilten SV 2003-5 (1), 9-37.
2. ČRNČEC, Damir (2003). Varnostna kultura in varnostno preverjanje oseb na obrambnem področju. Revija Slovenska vojska, leto XI/21.
3. FURLAN Branimir in ostali (2006). Vojaška doktrina. Ljubljana: PDRIU.
4. GRIZOLD, Anton (1998). Javnost o organiziranju in upravljanju nacionalne varnosti Slovenije. Perspektive sodobne varnosti, Teorija in praksa, str. 99–134. Ljubljana: Fakulteta za družbene vede.
5. HARTMAN, Ervin (2007). Varovanje tajnih podatkov in varnostna kultura na obrambnem področju; protiobveščevalno – varnostni vidik. Specialistično delo. Ljubljana: Fakulteta za družbene vede.
6. KOROŠEC, Sabina (2006). Varnostno preverjanje v Republiki Sloveniji. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.
7. ŠAPONJA, Vladimir (1999). Taktika dela obveščevalno varnostnih služb. Ljubljana: Visoka policijsko-varnostna šola.
8. Urad Vlade Republike Slovenije za varovanje tajnih podatkov. www.uvtp.gov.si. (7.5.2012).
9. ZGAGA, Sabina (2012). Izdaja tajnih podatkov. Pravna praksa 1/2012, 14-15.

PRAVNI VIRI

1. Kazenski zakonik, Uradni list RS, št. 55/08.
2. Navodilo o označevanju gradnikov in nosilcev elektronskih podatkov v komunikacijskem in informacijskem sistemu Ministrstva za obrambo, številka 0070-18/2007-1 z dne 22. 3. 2007.
3. Navodilo o postopkih uničevanja nosilcev podatkov v elektronski obliki, številka 007-71/2008-1 z dne 6. 3. 2008.
4. Popravek Uredbe o spremembah Uredbe o varovanju tajnih podatkov, Ur. l. RS, št. 24/11.
5. Pravilnik o spremembah in dopolnitvah pravilnika o varovanju tajnih podatkov na Ministrstvu za obrambo, šifra 0070-5/2006-30 z dne 31. 8. 2006.
6. Pravilnik o spremembah in dopolnitvah pravilnika o varovanju tajnih podatkov na Ministrstvu za obrambo, šifra 0070-22/2008-26 z dne 11. 6. 2008.
7. Pravilnik o spremembah in dopolnitvah Pravilnika o varovanju tajnih podatkov na Ministrstvu za obrambo, številka 0070-26/2012-4, z dne 6. 4. 2012.
8. Pravilnik o varovanju komunikacijskega in informacijskega sistema MORS, številka 007-161/2008-2 z dne 12. 6.2008.
9. Pravilnik o varovanju tajnih podatkov na Ministrstvu za obrambo, šifra 0070-5/2006-4 z dne 21. 2. 2006.
10. Pravilnik o inšpekcijskem nadzoru na obrambnem področju. Ur. l. RS, številka 88/03.
11. Resolucija o strategiji nacionalne varnosti Republike Slovenije, Uradni list RS, št. 56/01.
12. Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja, Ur. l. RS, št. 94/06.
13. Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov, Ur. l. RS, št. 6/02.
14. SOP ŠČ št. 02 – 006 za oblikovanje in zagovor zaključne naloge kandidatov in slušateljev na šoli za častnike, številka: 804-153/2012-1 z dne 15.3.2012.
15. SOP št. 1000 PSSV: Izdelava SOP v Poveljstvu sil Slovenske vojske in podrejenih enotah, številka 804-193/2009-1 z dne 25. 3. 2009.

16. Uredba o dopolnitvi Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, Ur. l. RS, št. 86/11.
17. Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja, Uradni list RS, št. 94/06.
18. Uredba o načinu in postopku ugotavljanja pogojev za izdajo varnostnega dovoljenja organizaciji, Ur. l. RS, št. 70/07.
19. Uredba o notranjem nadzoru nad izvajanjem Zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi, Ur. l. RS, št. 106/02.
20. Uredba o obliki in uporabi znaka Urada Vlade RS za varovanje tajnih podatkov, Ur. l. RS, št. 1/08.
21. Uredba o spremembah Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov, Ur. l. RS, št. 138/06.
22. Uredba o spremembah Uredbe o varovanju tajnih podatkov, Ur. l. RS, št. 7/11.
23. Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov, Ur. l. RS, št. 71/06.
24. Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, Ur. l. RS, št. 48/07.
25. Uredba o varovanju tajnih podatkov, Ur. l. RS, št. 74/2005.
26. Zakon o dopolnitvi Zakona o tajnih podatkih (ZTP-D). Ur. l. RS, št. 60/11.
27. Zakon o obrambi, Ur.l. RS 82/94.
28. Zakon o spremembah Zakona o tajnih podatkih. Ur. l. RS, št. 9/10.
29. Zakon o tajnih podatkih, Ur. l. RS, št. 50/2006.

PRILOGA

Priloga 1: Dodatno usposabljanje - prezentacija

OBRAVNAVANJE IN VAROVANJE TAJNIH PODATKOV

DODATNO USPOSABLJANJE
(Ugotovitve nadzorov v SV)

1

USPOSABLJANJE IZ ZTP

- osnovno in dodatno usposabljanje
- izvajalci morajo imeti potrdila, da so usposobljeni za predavanja
- podpis izjave o seznanjenosti z ZTP po končanem usposabljanju in ne prej
- načrtovati dovolj terminov za dodatno usposabljanje

3

OCENA MOŽNIH ŠKODLJIVIH POSLEDIC

• pisna in obvezna za vsak dokument, ki vsebuje tajni podatek

• ocena nima stopnje tajnosti in se hrani kot priloga dokumenta pri organu, ki je stopnjo tajnosti določil

• izdelana mora biti skrbno in vsebovati konkretne opise posledic, ne samo dikcije iz ZTP, ali kopirana iz drugega dokumenta

4

PREGLED NOSILCEV TAJNIH PODATKOV

• zagotoviti letni pregled na ravni bataljona, pooblastilo izvajalcem

• mešanje 15. člena Pravilnika o varovanju tajnih podatkov na ministrstvu za obrambo in 30. člena Uredbe o varovanju tajnih podatkov

➢ Pravilnik zahteva, da se pregledajo tajni podatki, ki sodijo v pristojnost enote. Pri pregledu je treba oceniti, ali še obstaja potreba po njihovi tajnosti in ali je stopnja tajnosti še ustrezna

➢ Uredba o varovanju tajnih podatkov v 30. členu govori o uničenju tajnih podatkov. Gre za podatke, ki smo jih prejeli informativno

5

DOLOČANJE STOPNJE TAJNOSTI

• pooblaščena oseba mora pri določanju tajnosti podatka določiti najnižjo stopnjo tajnosti, ki še zagotavlja varovanje podatka

• slaba praksa iz devetdesetih let, ko je nastala poplava dokumentov z različnimi stopnjami tajnosti, do katerih pa večina ni bila upravičena

POBUDA ZA SPREMEMBO STOPNJE TAJNOSTI

• lahko jo poda vsak prejemnik tajnega podatka in jo posreduje neposredno nadrejenemu

• na podlagi pobude lahko nadrejeni predlagajo spremembo ali preklic tajnosti podatka osebi iz 9. člena pravilnika, v čigar pristojnost sodi tajni podatek

6

OZNAČEVANJE DELOVNEGA GRADIVA

• delovno gradivo, ki se uporablja pri izdelavi dokumenta, ki vsebuje tajen podatek ter ni namenjeno drugim osebam in ga izdelovalec takoj po končanju izdelave dokumenta uniči, se označi kot tajni podatek vendar se ne evidentira. Uničenje se izvede brez komisijskega zapisnika

• delovno gradivo, ki nastane pri izdelavi dokumenta, ki vsebuje tajen podatek in ki ni takoj uničeno, se v skladu s pisno oceno škodljivih posledic označi z ustrezno stopnjo tajnosti. V primeru posredovanja delovnega gradiva tretjim osebam, se ga evidentira

7

OBRAVNAVANJE TP IZVEN VARNOSTNIH OBMOČIJ

• tajni podatki se lahko obravnavajo zunaj varnostnega območja, če je prostor ali območje, v katerem se tajni podatek obravnava, fizično ali tehnično varovan, dostop do prostora pa je nadzorovan

• kadar se mora tajni podatek stopnje tajnosti ZAUPNO ali višje stopnje tajnosti obravnavati zunaj prostorov, mora odgovorna oseba izdelati načrt ukrepov in postopkov za varovanje tajnega podatka

• vsak iznos ali vnos nosilca tajnega podatka stopnje tajnosti ZAUPNO in višje stopnje zunaj varnostnega območja se evidentira

8

POOBLASTILO ZA KOPIRANJE TP

• fotokopirni stroji, telefaksi in druge naprave za razmnoževanje in prenos tajnih podatkov, nameščeni v varnostnem območju morajo biti dodatno zavarovani

• uporabljajo jih lahko samo osebe, ki so posebej pooblaščene za ravnanje s temi napravami

• pooblastilo izda vodja organizacijske enote ministrstva, v čigar pristojnost sodi varnostno območje

9

UREJANJE PODROČJA TP S SOP-i

• urejanje splošnega področja varovanja tajnih podatkov s SOP-i ni potrebno, saj ga predpisi podrobno urejajo

• če je SOP v neskladju s predpisi obstaja nevarnost neenotnega varovanja tajnih podatkov

• smiselno je v specifičnih primerih varovanja tajnih podatkov, ko obstoječi predpisi ne definirajo konkretnega ravnanja (varnostno območje v terenskih pogojih ali ravnanje z oborožitvenimi sistemi ali njihovimi deli, katerim je določena stopnja tajnosti)

10

OZNAČEVANJE GRADNIKOV IN NOSILCEV ELEKTRONSKIH PODATKOV

• vsaka naprava, ki predstavlja gradnik KIS MO, mora biti na vidnem mestu jasno označena s stopnjo tajnosti podatkov, skladno z oznakami iz Zakona o tajnih podatkih

- za oznako INTERNO se uporabi črn napis INTERNO na rumeni podlagi;
- za oznako ZAUPNO se uporabi črn napis ZAUPNO na zeleni podlagi
- za oznako TAJNO se uporabi črn napis TAJNO na modri podlagi in
- za oznako STROGO TAJNO se uporabi črn napis TAJNO na rdeči podlagi.

11

IZJAVA O AVTORSTVU ZAKLJUČNE NALOGE

Slušatelj stotnik Robert Perčič izjavljam, da sem avtor zaključne naloge z naslovom Varovanje tajnih podatkov v SV, ki sem jo napisal pod mentorstvom majorja Jožeta Grbca.

S svojim podpisom zagotavljam da:

- je zaključna naloga izključno rezultat mojega lastnega dela,
- so vsa dela in mnenja drugih avtorjev, ki jih uporabljam v zaključni nalogi, navedena oziroma citirana v skladu s SOP ŠČ št. 02 – 006 za oblikovanje in zagovor zaključne naloge kandidatov in slušateljev na šoli za častnike, dokument ŠČ, številka 804-153/2012-1 z dne 15. 3. 2012.
- se zavedam, da je plagiatorstvo kaznivo po Zakon-u o avtorskih in sorodnih pravicah, (uradno prečiščeno besedilo – ZASP UPB3, Uradni list RS, št. 16/2007, z dne 23. 2. 2007), prekršek pa podleže tudi ukrepom disciplinske odgovornosti v skladu z Zakonom o obrambi in Pravili službe v Slovenski vojski,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo zaključno nalogo in moj status v Slovenski vojski.

S podpisom se odrekam vsem materialnim pravicam v zvezi z zaključno nalogo in dovoljujem uporabo zaključne naloge v študijske namene.

Maribor, 25. maj 2012 Podpis:_____