UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Specialistično delo

ORGANIZIRANOST IN DELOVANJE SLUŽBE ZA TAJNE PODATKE NA STALNEM PREDSTAVNIŠTVU REPUBLIKE SLOVENIJE PRI EVROPSKI UNIJI

Sven Engelsberger

Ljubljana, november 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Specialistično delo

ORGANIZIRANOST IN DELOVANJE SLUŽBE ZA TAJNE PODATKE NA STALNEM PREDSTAVNIŠTVU REPUBLIKE SLOVENIJE PRI EVROPSKI UNIJI

Kandidat: Sven Engelsberger
Vpisna št.: 04033314
Študijski program: Podiplomski specialistični študijski program Javna uprava
Mentor: Prof. dr. Štefan Ivanko

Ljubljana, november 2009

POVZETEK

Osebe z dovoljenjem za dostop do tajnih podatkov, ki opravljajo delo v organu, bi rade imele hiter dostop do tajnih podatkov, kar pa zaradi ročnega evidentiranja v delovodnike ni mogoče. Osebe bi prejemale tajne podatke v čim večjem obsegu, posledica tega pa je prekomerno kopiranje in distribucija tajnih podatkov ter polnjenje arhivov v službah za tajne podatke.

V specialističnem delu je prikazana pravna ureditev Republike Slovenije in Evropske unije s področja tajnih podatkov, primerjava teh ureditev in prikaz slabosti slovenskih pravnih predpisov.

Opisana je ustanovitev Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju, težave pri delovanju službe in prikaz izboljšanja poslovanja s tajnimi podatki z uvedbo novega modela organiziranosti službe ter nadgradnja modela organiziranosti z informacijsko tehnološkim sistemom.

Ključne besede: tajni podatek, dovoljenje za dostop do tajnih podatkov, potreba po vedenju, evidentiranje tajnih podatkov, distribucija tajnih podatkov, prenos tajnih podatkov, arhiviranje tajnih podatkov, Stalno predstavništvo Republike Slovenije pri Evropski uniji, Evropska unija.

ABSTRACT

Persons with personal security clearance who carry out their duties would like an instant access to classified information which is impossible to obtain because of physical recording in registry. Persons would like to receive classified information in a large extent which suffers the consequences of excessive copying and distribution of classified information and filling archives in registries for classified information.

In a specialist thesis is described juridical regulation of classified information in the Republic of Slovenia and in the European Union, comparison of regulations and review of debility of Slovenian juridical regulation.

In the thesis is represented the Registry for Classified Information in the Permanent Representation of the Republic of Slovenia to the European Union in Brussels, problems by activity of registry and review of improved operation with classified information with implemention a new model of organization in the registry and construction of information technology system to the model of organization.

Key words: classified information, personal security clearance, need to know, recording of classified information, distribution of classified information, transmission of classified information, storage of classified information, Permanent Representation of the Republic of Slovenia to the European Union, European Union.

KAZALO

1 UVOD

Imeti pomembno informacijo pomeni imeti prednost pred drugimi. Kdor pridobi informacije pred konkurenti oziroma nasprotniki, kar velja tako v politiki, gospodarstvu in tudi vsakdanjem življenju, ima prednost pri uveljavljanju svojih interesov in pri doseganju zastavljenih ciljev.

Da bi oseba z interesom imela prednost pred nasprotno stranko, pa morajo biti določene informacije znane manjšemu številu ljudi in skrbno varovane. Nepooblaščeno razkritje takih informacij bi lahko povzročilo osebi z interesom, organu ali državi težko popravljivo škodo. Za preprečitev eventualne škode je treba določene informacije kvalificirati v tajne podatke ob upoštevanju pravnih predpisov s področja dela in varovanja tajnih podatkov.

Po osamosvojitvi Republike Slovenije je bilo treba nujno sprejeti tudi pravne predpise o tajnih podatkih. Sprejeti so bili le podzakonski predpisi, ki so parcialno urejali področje tajnih podatkov v javni upravi. Bližanje procesa vključevanja Republike Slovenije v Evropsko unijo in v zvezo Nato pa je pomenilo potreben sprejem zakona, ki bi celovito uredil področje tajnih podatkov.

Leta 2001 je pričel veljati Zakon o tajnih podatkih, ki predstavlja normativni okvir in osnovo pri delu s tajnimi podatki. Na podlagi zakona je bilo sprejetih več podzakonskih predpisov o tajnih podatkih, ki skupaj celovito zaokrožujejo celoto obravnavanja tajnih podatkov od njihovega nastanka pa do uničenja.

Od leta 2004 je Republika Slovenija dolžna spoštovati predpise o varovanju in delu s tajnimi podatki Evropske unije in zveze Nato.

V času predsedovanja Republike Slovenije Svetu Evropske unije v prvi polovici leta 2008 so se na Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju (v nadaljevanju stalno predstavništvo) v Službi za tajne podatke pričele pojavljati težave pri delu s tajnimi podatki, hkrati pa so se kazale rešitve, ki bi lahko izboljšale delo s tajnimi podatki ob implementaciji nacionalnih pravnih predpisov in pravnih predpisov Evropske unije (Svet Evropske unije in Evropska komisija) s področja tajnih podatkov v praktično delo v službi. V tem času je bila potrebna hitra distribucija tajnih podatkov na relaciji Bruselj-Ljubljana in v obratno smer, kar pa vedno ni bilo mogoče, bi pa lahko bilo ob ustrezni podpori pristojnih služb v Sloveniji in zaposlenih na stalnem predstavništvu v Bruslju.

V specialističnem delu sem predstavil organiziranost in delovanje Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji, katero sem

vodil v času predsedovanja Republike Slovenije Svetu Evropske unije, od same ustanovitve službe pa do novih metod in postopkov pri delu s tajnimi podatki z upoštevanjem varovanja tajnosti dela in opreme v službi.

Problemi, katerih rešitev sem prikazal, predstavljajo:

- pomanjkanje strokovno-tehnične pomoči službam, ki skrbijo za ravnanje s tajnimi podatki, s strani službe za informatiko, varnostno tehnične službe, finančne službe, in pomanjkanje koordinacije podpornih služb;
- tajnim podatkom se določi previsoka stopnja tajnosti ali pa se jim ta sploh ne določi, kar lahko privede do upočasnitve dela oziroma do nastanka težko popravljive škode;
- določeni prejemniki tajnih podatkov ravnajo z njimi neodgovorno in protipravno (fotokopiranje tajnih podatkov, neustrezno hranjenje tajnih podatkov, uničevanje tajnih podatkov, posredovanje tajnih podatkov nepooblaščenim osebam, obdelava tajnih podatkov po nezaščitenih informacijsko-tehnoloških poteh (telefaks, elektronska pošta, shranjevanje na trdi disk delovne postaje), izguba tajnih podatkov, nevračilo tajnih podatkov pristojni službi);
- nesankcioniranje kršiteljev pravnih predpisov s področja varovanja tajnih podatkov kljub opozorilu predstojniku organa oziroma pooblaščencu predstojnika s strani uradne osebe, ki dela v službi za tajne podatke;
- povečanje sledljivosti tajnih podatkov ni doseženo kljub možnosti povečanja;
- notranje organizacijske enote v državnih organih, ki so pristojne za delo s tajnimi podatki, imajo premalo avtonomije in so podvržene aktualni politični oblasti (Urad Vlade Republike Slovenije za varovanje tajnih podatkov, službe za varovanje tajnih podatkov na ministrstvih ipd.);
- evidenca tajnih podatkov se še vedno vodi ročno;
- distribucija tajnih podatkov poteka tudi v papirnati obliki namesto v elektronski obliki (velika poraba papirja, težave pri arhiviranju, izguba delovnega časa pri uničevanju tajnih podatkov (komisijsko uničenje tajnih podatkov, kateri morajo biti navedeni v zapisniku komisije));
- pri prejemu tajnih podatkov v papirnati obliki, se pri distribuciji uporablja tiskanje podatkov namesto optičnega branja in vnosa v bazo podatkov (baza niti ni zgrajena);
- pri prejemu tajnih podatkov na arhivskih medijih (zgoščenka ipd.) se za distribucijo izdela kopija arhivskega medija, namesto da bi se vsebina medija kot datoteka vnesla v bazo podatkov.

Predmet raziskovanja je prikaz problemov in predloga izboljšav pri poslovanju s tajnimi podatki v službah za tajne podatke ob upoštevanju nacionalnih predpisov s področja tajnih podatkov in predpisov Evropske unije. Prikazani so vsi navedeni predpisi s področja tajnih podatkov (poslovanje s tajnimi podatki, varnostnotehnična oprema, komunikacijsko-informacijski sistemi v službah).

Opisan je postopek ustanovitve službe za poslovanje s tajnimi podatki v notranji organizacijski enoti organa državne uprave, t. j. od vzpostavitve varnostnih območij, nabave opreme (blagajne, rezalnik papirja idr.), priprave potrebnih postopkov, navodil in metod dela v skladu s pravnimi predpisi. Izpostavljene so težave, ki se pojavljajo v delovanju službe (organizacijske znotraj organa in pri sodelovanju z drugimi službami (služba za informatiko, varnostno tehnična služba in finančna služba)).

V času pred predsedovanjem Republike Slovenije Svetu Evropske Unije in v času predsedovanja je bilo v Službi za tajne podatke na stalnem predstavništvu v Bruslju potrebno sprejemati hitre in pravno sprejemljive odločitve pri delu s tajnimi podatki. V tem času so se pokazale pri vsakodnevnem delu tudi možne rešitve, ki bi lahko izboljšale poslovanje s tajnimi podatki. Za realizacijo izboljšanja poslovanja s tajnimi podatki sem imel več sestankov s pristojnimi službami in osebami, vendar je bil za izboljšanje poslovanja s strani pristojnih oseb negativen odziv (nedovzetnost za spremembe kljub argumentiranim predlogom, ki so bili finančno sprejemljivi). Ko se je predsedovanje pričelo, so se prejemniki tajnih podatkov pritoževali, zakaj imajo druge evropske države bolj odprt in za prejemnike tajnih podatkov bolj prijazen sistem. Pristojne osebe v Sloveniji niso hotele niti slišati, kakšen sistem ravnanja s tajnimi podatki imajo druge države članice Evropske unije (na primer Francija, Finska). V specialističnem delu so prikazane vse rešitve, katere bi lahko imeli v Službi za tajne podatke in ki bi prihranile čas in denar (ažuren prenos tajnih podatkov in obvestilo prejemniku o prispetju tajnega podatka, zmanjšanje fotokopiranja, ukinitev prihodov kurirjev na relaciji Ljubljana-Bruselj-Ljubljana) pri poslovanju s tajnimi podatki (zasnova modela organiziranosti, podprtega z informacijsko tehnologijo).

Natančno so pojasnjeni pojmi tajni podatek, določanje tajnih podatkov, označevanje tajnih podatkov, evidentiranje tajnih podatkov, obdelava tajnih podatkov, razmnoževanje tajnih podatkov, arhiviranje, načrti varovanja, postopek ob zlorabi tajnega podatka, dostop do tajnih podatkov in njihovo varovanje, varnostno območje, upravno območje, varnostno preverjanje, dovoljenje za dostop do tajnih podatkov, prenos tajnih podatkov, uničenje tajnih podatkov, protiprisluškovalni pregled prostorov, nadzor, sankcije.

Ob opredeljenemu problemu in predmetu raziskovanja sem v specialističnem delu preveril naslednje hipoteze (nepreverjene trditve):

- **Prva hipoteza:**

Obstoječa organiziranost Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju predstavlja težave pri poslovanju s tajnimi podatki.

- **Druga hipoteza:**

Adekvatna informacijska podpora Službi za tajne podatke bi izboljšala poslovanje s tajnimi podatki.

- **Tretja hipoteza:**

Pravni predpisi Republike Slovenije s področja varovanja tajnih podatkov otežujejo dostop do tajnih podatkov in delo s tajnimi podatki.

Namen raziskovanja je analiza obstoječih pravnih predpisov s področja varovanja tajnih podatkov, vzpostavitev službe za poslovanje s tajnimi podatki in začetek dela s tajnimi podatki. Namen je prikaz vseh težav, s katerimi se soočajo službe za tajne podatke in prejemniki tajnih podatkov, kateri v izrednih situacijah potrebujejo tajni podatek takoj, ko za njega zaprosijo, kar pa obstoječi sistem ne omogoča, bi pa lahko. Najslabše je urejen prenos tajnih podatkov med diplomatsko-konzularnimi predstavništvi v tujini in državnimi organi v Republiki Sloveniji.

Zaradi neurejenega sistema dela s tajnimi podatki prihaja tudi do kršitev pri poslovanju s tajnimi podatki (fotokopiranje tajnih podatkov, metanje dokumentov v koš za smeti in drugo protipravno ravnanje), službe za poslovanje s tajnimi podatki pa izgubljajo čas za nepotrebna opravila (prekomerno ročno dokumentiranje, fotokopiranje, arhiviranje in uničevanje tajnih podatkov, priprava kurirske pošte in s tem povezane dejavnosti).

Cilj raziskovanja poda utemeljen odgovor na pomanjkljivosti obstoječega stanja. V nalogi je izdelanih več konceptov pri delu s tajnimi podatki (organizacijski in informacijski koncept), ki bodo lahko za prejemnike tajnih podatkov in za službe za poslovanje s tajnimi podatki pomenili izboljšanje storitev poslovanja s tajnimi podatki.

Zasnoval sem model izboljšanja organiziranosti dela s tajnimi podatki:

- Na tajni podatek se večkrat krepko natisne številka (ali pa črtna koda) prejemnika tajnega podatka (diagonalno in za vsako stopnje tajnosti v drugačni barvi), kar omogoča povečano sledljivost podatka in zmanjša zlorabo podatka (fotokopiranje, založitev ipd.).
- Vsak prejemnik tajnega podatka je dolžan voditi lastno evidenco tajnih podatkov, s čimer se poveča odgovornost prejemnikov pri delu s tajnimi podatki.
- Pri vračilu tajnih podatkov Službi za tajne podatke se podatkom priloži prejemnikov seznam tajnih podatkov, kar omogoča kasnejše hitrejšo komisijsko uničenje tajnih podatkov, s čimer se prepreči prekomerno kopičenje tajnih podatkov v arhivu.
- Prejemniku tajnega podatka, ki ga kljub pozivu Službe za tajne podatke po elektronski pošti ne prevzame (na primer neprevzem tajnega podatka v roku 14 dni), se ukine distribuiranje tajnih podatkov do preklica službe (s tem se zmanjša nepotrebno fotokopiranje tajnih podatkov in arhiviranje).
- Izdela se distribucijska lista prejemnikov tajnih podatkov, ki jo določijo vodja stalnega predstavništva in vodje notranjih organizacijskih enot, s tem da ima Služba za tajne podatke pravico prenehanja distribucije tajnih podatkov

neprevzemnikom (s tem bi se zmanjšalo prekomerno razmnoževanje tajnih podatkov).
- Delovodnike zamenja računalniška evidenca tajnih podatkov in prejemnikov tajnih podatkov (na primer v programu Excel), iz katere bi bilo razvidno, kateri prejemnik tajnih podatkov je na prvem mestu glede na nevračilo tajnih podatkov Službi za tajne podatke (služba bi mesečno obvestila vodjo stalnega predstavništva o dolžnikih tajnih podatkov).

Izboljšan model organiziranosti pri delu s tajnimi podatki je možno informacijsko podpreti in nadgraditi.

Prejemniki tajnih podatkov bodo hitreje pridobili tajne podatke preko informacijsko tehnološkega sistema, zmanjšalo se bo fotokopiranje tajnih podatkov (fotokopiranje v skladu s predpisi in protipravno fotokopiranje) in izboljšala se bo zavest prejemnikov tajnih podatkov pri delu s tajnimi podatki.

Službe za tajne podatke bodo lahko imele sodoben informacijsko tehnološki sistem s polavtomatskim dokumentiranjem in označevanjem dokumentov, zmanjšalo pa se bo tudi arhiviranje. Tajni podatki do stopnje tajnosti TAJNO oziroma SECRET UE bodo v zaprtem mrežnem sistemu, do stopnje tajnosti INTERNO oziroma RESTREINT UE pa v odprtem sistemu (na delovnih postajah z dostopom do zunanjih mrežnih povezav). Omenjen sistem poznajo že dalj časa razvite države članice Evropske unije (Nemčija, Francija, Finska). Prispeli tajni podatki se bodo optično prebrali in vnesli v bazo podatkov. Z uporabo informacijske tehnologije in novih metod in postopkov dela službam za tajne podatke ne bi bilo več potrebno fizično razmnoževati tajnih podatkov stopnje tajnosti TAJNO oziroma SECRET UE, odpravilo pa bi se tudi dokumentiranje v delovodnikih za stopnji tajnosti TAJNO oziroma SECRET UE in STROGO TAJNO oziroma TRÈS SECRET UE/EU TOP SECRET.

Prenos tajnih podatkov do stopnje tajnosti TAJNO oziroma SECRET UE lahko poteka preko informacijskega sistema med službama za tajne podatke stalnega predstavništva in Ministrstva za zunanje zadeve Republike Slovenije, zaradi česar ni več potrebna kurirska služba za prenos tajnih podatkov do navedene stopnje tajnosti.

Pregledal sem številne biografske enote s področja tajnih podatkov v spletni bazi podatkov Cobiss in ugotovil, da tema organiziranost in delovanje službe za tajne podatke še ni bila raziskana, obdelana in predstavljena javnosti. Delno so posamezni sklopi s področja tajnih podatkov obravnavani v domačih in tujih člankih, diplomskih, specialističnih in magistrskih delih. V specialističnem delu sem prikazal novost na obravnavanem področju. Do sedaj ni bilo nič zapisano o celovitem prikazu težav pri delu s tajnimi podatki, zasnovi modela organiziranosti in o informacijsko tehnološkem sistemu, metodah in postopkih, ki bi celovito prikazali izboljšan in učinkovit sistem poslovanja s tajnimi podatki tako za prejemnike tajnih podatkov kot tudi za službe za

poslovanje s tajnimi podatki. V specialističnem delu sem uporabil pridobljene izkušnje vodenja Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju in sodelovanja z nacionalnimi službami in službami Evropske unije, kjer sem odkrival nove metode in postopke pri delu s tajnimi podatki, ki jih nismo uporabljali, bi jih pa lahko.

Uporaba raziskovalnega dela bi nudila možnost za kreativen prispevek k razvoju stroke. Potrebna bi bila podpora strokovnjakov s področja informatike in varnostno tehničnih služb.

V Republiki Sloveniji iz meni neznanih (znanih) razlogov ni volje, da bi se obstoječi sistem spremenil, zato tudi niso bila v ta namen opravljena nobena resna raziskovanja. Opisane so zgolj metode in postopki dela, ki temeljijo na pravnih predpisih, brez inovativnih metod.

Zaradi občutljivosti področja tajnih podatkov ne obstajajo knjige s tematiko o sistemu poslovanja s tajnimi podatki, napisanih pa je več strokovnih člankov o normativni ureditvi in o delu s tajnimi podatki. Vsaka država želi imeti skrit sistem poslovanja s tajnimi podatki, saj bi se z razkritjem sistema lahko ogrozila varnost tajnosti podatkov, varnost organa in varnost države. Nikjer ne bo mogoče prebrati, kako je v praksi urejeno poslovanje s tajnimi podatki v drugih državah, ampak le pravna ureditev poslovanja, ki pa lahko dopušča strog zaprt sistem poslovanja s tajnimi podatki (neuporaba informacijske tehnologije pri poslovanju s tajnimi podatki) ali pa odprt sistem, ki je za uporabnike prijazen zaradi uporabe informacijsko tehnoloških rešitev. V času dela na stalnem predstavništvu v Bruslju sem videl (zapisano ni nikjer, pač pa po pripovedovanju diplomatov, predstavnikov Sveta, Komisije in drugih oseb), da imajo države članice Evropske unije od strogo zaprtih sistemov (bivše komunistične države) pa do informacijsko naprednih odprtih sistemov pri poslovanju s tajnimi podatki (skandinavske države). Daljša je tradicija demokracije v državi, bolj je sistem odprt. Poslovanje s tajnimi podatki poteka v starejših parlamentarnih demokracijah (t. i. gentlemanski sistem) tudi po "sistemu iz roke v roko", kjer velja načelo zaupanja (Združene države Amerike, Velika Britanija).

V specialističnem delu sem uporabil naslednje metode raziskovanja, s katerimi sem rešil problem in predmet raziskovanja, dokazal postavljene hipoteze, dosegel namen in cilje raziskovanja ter odgovoril na vprašanja:

- Metoda deskripcije

Z metodo deskripcije sem predstavil vse pravne predpise Republike Slovenije, Sveta Evropske unije in Evropske komisije s področja tajnih podatkov. Poudarek je na Zakonu o tajnih podatkih, Uredbi o varovanju tajnih podatkov, Sklepu o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja, Uredbi o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, Uredbi o

varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov, Predpisih Sveta Evropske Unije o varovanju tajnosti in na Pravilniku Evropske komisije o varnosti.

- Primerjalna metoda

Med seboj sem primerjal predpise o varovanju in delu s tajnimi podatki Republike Slovenije in Evropske unije ter izpostavil bistvene razlike. Primerjal sem tudi predlagano organiziranost Službe za tajne podatke po nacionalnih predpisih z organiziranostjo službe po predpisih Evropske unije.

- Metoda analize in sinteze

Z analizo sem razčlenil delo s tajnimi podatki na osnovne prvine (nastanek, evidenca, distribucija, prenos, arhiviranje, uničevanje tajnih podatkov) in preučeval vsako prvino ločeno in v povezavi s celoto (delovanje Službe za tajne podatke). S sintezo sem prvine sestavil v celoto in prikazal več opcij delovanja Službe za tajne podatke (različni modeli, postopki in tehnike poslovanja s tajnimi podatki).

- Metoda modeliranja

V delu sem si postavil različne modele poslovanja s tajnimi podatki in z raziskovanjem prikazal več metod in postopkov za dosego cilja. Kot temeljni model (model, ki bo največ prispeval k stroki) sem si postavil informacijsko tehnološki sistem.

- Induktivna in deduktivna metoda

Z induktivno metodo sem iz posamičnih delov poslovanja s tajnimi podatki prišel do splošne ugotovitve izboljšanja poslovanja (na primer: optično branje tajnih podatkov in vnos v informacijski sistem ter s tem polavtomatsko evidentiranje podatkov prinese prejemnikom tajnih podatkov takojšen dostop do tajnih podatkov; oba sklopa sta izvedena skoraj istočasno, t. j. vnos-dostop).

Z deduktivno metodo sem iz splošnih stališč prišel do konkretnih posamičnih sklepov (na primer: z uvedbo elektronskega prenosa tajnih podatkov drugi službi za poslovanje s tajnimi podatki (odprava kurirske službe za prenos tajnih podatkov) pridobi prejemnik tajni podatek ažurno; oba sklopa sta izvedena skoraj istočasno, t. j. vnos-dostop).

V specialističnem delu so najprej predstavljeni pravni predpisi Republike Slovenije s področja tajnih podatkov (drugo poglavje). Opredeljeni so temeljni pojmi (od nastanka pa do uničenja tajnega podatka, varnostnotehnična oprema in komunikacijsko-informacijski sistemi v službah za tajne podatke).

V tretjem poglavju so prikazani pravni predpisi Evropske unije o tajnih podatkih.

V četrtem poglavju je opravljena primerjava med predpisi o tajnih podatkih v Republiki Sloveniji in v Evropski uniji. Prikazani so učinki pravne ureditve tajnih podatkov

Evropske unije na nacionalne predpise (neposredna uporabnost, primarnost – načelo supremacije in avtonomnost prava Evropske unije).

V petem poglavju je opisan postopek ustanovitve Službe za tajne podatke na stalnem predstavništvu in pričetek dela službe ob sodelovanju s pristojnimi službami stalnega predstavništva in Ministrstva za zunanje zadeve (Služba za tajne podatke, Služba za informacijsko tehnologijo, Varnostno tehnična služba in Finančno računovodska služba) ter s službami Sveta Evropske unije. Prikazane so tudi težave, ki se pričnejo pojavljati pri delu Službe za tajne podatke (organizacijsko-tehnične, kadrovske in normativne).

V šestem poglavju je prikazanih več organizacijskih možnosti za odpravo težav pri delovanju Službe za tajne podatke. Zasnovan je model organiziranosti službe, ki temelji na pridobljenih izkušnjah vodenja službe in lastnem znanju brez podpore Služb za informacijsko tehnologijo in Varnostno tehničnih služb stalnega predstavništva in Ministrstva za zunanje zadeve. Odpravljene so administrativne ovire, povečana je sledljivost tajnih podatkov, zmanjšana je možnost protipravnega ravnanja s tajnimi podatki (razmnoževanje, uničenje, izguba tajnih podatkov), zmanjšan je obseg distribucije in s tem je tudi zmanjšano arhiviranje ter povečana odgovornost ravnanja s tajnimi podatki.

Sedmo poglavje vsebuje prikaz izdelave in opis informacijsko podprtega sistema modelu organiziranosti (razvoj informacijsko tehnološkega sistema). Nov sistem poenostavi delo s tajnimi podatki službam za tajne podatke, prejemnikom tajnih podatkov pa omogoča bolj varen in ažuren dostop do podatkov. Z novim sistemom je omogočena hitrejša obdelava in distribucija tajnih podatkov prejemnikom v Republiki Sloveniji in na stalnem predstavništvu. Zmanjša se razmnoževanje tajnih podatkov, kurirska služba pa je potrebna samo še za najvišjo stopnjo tajnosti STROGO TAJNO oziroma TRÈS SECRET UE/EU TOP SECRET. Zmanjšajo se tudi materialni stroški Službe za tajne podatke.

Osmo poglavje vsebuje uresničene cilje oziroma dosežke raziskave.

V devetem poglavju so preverjene hipoteze raziskovanja.

Prispevek rezultatov raziskave k stroki je opisan v desetem poglavju.

V enajstem poglavju je prikazana uporabnost rezultatov raziskave.

Zaključek specialističnega dela predstavlja povzetek najpomembnejših ugotovitev in spoznanj, ki so obširno obrazložena v samem delu.

Zaključku sledijo seznam uporabljene literature in virov, seznam tabel, seznam uporabljenih kratic, seznam prilog in izjava o avtorstvu z navedbo lektorja.

2 PRAVNI PREDPISI REPUBLIKE SLOVENIJE S PODROČJA TAJNIH PODATKOV

V Republiki Sloveniji do uveljavitve Zakona o tajnih podatkih (Uradni list RS, št. 87/2001) dne 23. 11. 2001 ni bil sprejet noben pravni predpis o tajnih podatkih, ki bi celovito uredil področje dela s tajnimi podatki v javni upravi. Delo s tajnimi podatki so urejali podzakonski predpisi za posamezne organe javne uprave (Policija, Slovenska vojska, Ministrstvo za zunanje zadeve Republike Slovenije itn.). Približevanje vstopa Republike Slovenije v Evropsko unijo (in tudi v zvezo Nato) je pospešilo sprejem Zakona o tajnih podatkih zaradi prevzema pravnega reda Evropske unije in upoštevanja roka za uskladitev pravnega reda Republike Slovenije s pravnim redom Evropske unije. S sprejetjem Zakona o tajnih podatkih je bil zaključen postopek pogajanj z Evropsko unijo v poglavju 24 "Pravosodje in notranje zadeve" (Černetič in Brožič, 2003, str. 575).

Vlada Republike Slovenije je dne 9. 2. 2000 poslala Državnemu zboru Republike Slovenije predlog zakona o tajnih podatkih, kar je bil prelomni dogodek pri obravnavanju tajnih podatkov.

Po eni strani je bilo treba čim bolj dosledno zagotoviti javnost dela in dostopnost do podatkov in informacij državnih organov ter vse s tem povezane pravice javnosti in posameznikov, po drugi strani pa zagotoviti, da bodo tisti podatki in informacije, ki so določeni kot tajni, iz razlogov, ki so ne na pravno ustrezen način določeni, ampak tudi v praksi legitimno uporabljeni, ustrezno in dosledno varovani (Poročevalec DZ RS, 2000, str. 4). Do informacije javnega značaja je upravičena vsaka oseba ne glede na nacionalno pripadnost (Foerstel, 1999, str. 123). Javnost dela državnih organov, odprtost in preglednost (transparentnost) njihovega dela v povezavi z možnostjo dostopa do podatkov in informacij javnega značaja so značilnost sodobne demokratične in pravne države (Rovšek, 2001, str. 35).

Tajnosti nikakor ne moremo in ne smemo enačiti s pojmom skrivnosti. Pri tajnosti ne gre za neznane stvari, temveč za znane, pri katerih lastnik podatkov noče, da se z njimi seznani širši krog subjektov (Čaleta, 2003, str. 13).

Zakon o tajnih podatkih predstavlja pravni predpis, ki prvič v samostojni Sloveniji obširno ureja področje tajnih podatkov in hkrati predstavlja podlago za sprejem podzakonskih pravnih predpisov, s čimer je v celoti urejeno ravnanje s tajnimi podatki in normativno poskrbljeno za varnost. Toda v praksi pri delu s tajnimi podatki se kažejo problemi, ki jih pravni predpisi niso predvideli. Pomanjkljivosti in predlogi za odpravo pomanjkljivosti so opisani v naslednjih poglavjih specialističnega dela.

2.1 ZAKON O TAJNIH PODATKIH

2.1.1 Definicija tajnega podatka

Zakon o tajnih podatkih (Uradni list RS, št. 87/2001, 101/2003, 135/2003 – UPB1, 28/2006 in 50/2006 – UPB2) je temeljni pravni akt, s katerim se določajo 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 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. Po tem zakonu morajo ravnati tudi dobavitelji, izvajalci gradenj ali izvajalci storitev (organizacije), ki se jim tajni podatki posredujejo zaradi izvršitve naročil organa. 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, 1. člen).

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 zavarovati pred nepoklicanimi osebami, in ki je določeno in označeno za tajno. Tajni podatek tuje države je podatek, ki ga je Republiki Sloveniji oziroma njenim organom posredovala tuja država oziroma njen organ ali mednarodna organizacija oziroma njen organ v pričakovanju, da bo ostal tajen, ter podatek, ki je rezultat sodelovanja Republike Slovenije oziroma njenih organov s tujo državo ali mednarodno organizacijo oziroma njihovimi organi, in za katerega se dogovori, da mora ostati tajen. Varovanje in dostop do tajnih podatkov tuje države ali mednarodne organizacije se izvaja v skladu z Zakonom o tajnih podatkih ali predpisi, izdanimi na njegovi podlagi, oziroma v skladu z mednarodno pogodbo, ki jo je s tujo državo ali mednarodno organizacijo sklenila Republika Slovenija. Tuji tajni podatki praviloma ohranijo oznake, ki so v rabi v tuji državi ali mednarodni organizaciji, ali pa se označijo z Zakonom o tajnih podatkih, pri čemer morajo biti stopnje tajnosti primerljive, če ni drugače določeno z mednarodno pogodbo. Dokument je vsak napisan, narisan, natisnjen, razmnožen, posnet, fotografiran, magneten, optičen ali kakšen drugačen zapis tajnega podatka. Sredstvo, ki vsebuje tajne podatke, se imenuje medij (ZTP, 2. člen). V svetu informacijske družbe je potrebno vsak tajni podatek evalvirati in ustrezno uporabiti (Mount, 1985).

Oseba se seznani ali pridobi tajni podatek na podlagi dovoljenja za dostop do tajnih podatkov zaradi opravljanja funkcije ali izvajanja naloge na delovnem mestu. Brez dovoljenja za dostop do tajnih podatkov lahko dostopajo do tajnih podatkov z opravljanjem svoje funkcije najvišji funkcionarji oblasti od predsednika republike pa do informacijskega pooblaščenca s podpisom izjave, da so seznanjeni s pravnimi predpisi s

področja varovanja tajnih podatkov in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi (ZTP, 3. člen).

Za tajnega se določi podatek, ki je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi lahko nastale škodljive posledice za varnost države ali za njene politične ali gospodarske koristi (ZTP, 5. člen). 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, 6. člen). Določitev podatkov in informacij za tajne je v današnjem času lahko najenostavnejša možnost in način omejevanja javnosti dela državnih organov, ki se lahko zlorablja za prikrivanje različnih nepravilnosti ali celo nezakonitosti v teh organih (Žirovnik, 2005, str. 298).

V javnosti se največkrat s strani politikov in novinarjev krši 8. člen Zakona o tajnih podatkih, ki določa, da so osebe, ki opravljajo funkcijo ali delajo v organih, dolžne varovati tajne podatke ne glede na to, kako so zanje izvedele. Dolžnost varovanja tajnih podatkov ne preneha, ko osebi preneha funkcija ali delo v organu.

Tajnost mora služiti splošnim in posebnim interesom ter preprečevati možnost, da bi jim kaj škodilo. Le tako je lahko tajnost vrednota in daje varnosti pomen dobrine (Anžič v: Henigman, 2007, str. 172).

2.1.2 Določanje tajnih podatkov

Podatek določijo za tajnega naslednje pooblaščene osebe: predstojnik organa, izvoljeni ali imenovani funkcionarji organa (pooblaščeni morajo biti na podlagi pravnih predpisov ali na podlagi pisnega pooblastila predstojnika) in zaposlene osebe v organu, ki jih je za to pisno pooblastil predstojnik tega organa. Stopnjo STROGO TAJNO lahko določijo samo predsednik republike, predsednik državnega zbora in drugi z zakonom določeni najvišji funkcionarji oblasti.

Stopnjo tajnosti podatka določi pooblaščena oseba na podlagi pisne ocene, pri čemer mora oceniti možne škodljive posledice za varnost države ali za njene politične ali gospodarske koristi, če bi bil podatek razkrit nepoklicani osebi. Podatku se določi tudi način prenehanja in označi s predpisanimi oznakami. Določitev določenih podatkov za tajne je v nasprotju z načelom javnosti dela (Rep, 2001, str. 216).

Po mnenju strokovnjakov bi bilo potrebno določiti tajnost podatkov "pred", in ne "ob nastanku" (Mekina, 2001, str. 24).

Tajni podatki imajo glede na možne škodljive posledice za varnost in koristi države eno od naslednjih stopenj tajnosti (ZTP, 13. člen):

- STROGO TAJNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese Republike Slovenije ali jim nepopravljivo škodovalo;
- TAJNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo varnosti ali interesom Republike Slovenije;
- ZAUPNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom Republike Slovenije; in
- INTERNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo delovanju ali izvajanju nalog organa.

Pooblaščena oseba mora pri določanju tajnosti podatka določiti najnižjo stopnjo tajnosti, ki še zagotavlja varovanje podatka, potrebno za varstvo interesov ali varnosti države, tajnost podatka pa mora preklicati oziroma spremeniti, ko ni več pogojev, da bi imel podatek določeno stopnjo tajnosti. Najtežja naloga pri izvajanju Zakona o tajnih podatkih je spreminjanje aktualne miselnosti uporabnikov tajnih podatkov, katere značilnost je preobširno in pretirano določanje stopenj tajnosti (Antončič, 2001, str. 29). Posameznik pri določanju tajnosti podatkov ne presoja po logiki, temveč avtomatsko in brez razmisleka določi tajnost podatka (Arnejčič, 2001, str. 52).

Po terorističnem napadu na Združene države Amerike 11. 9. 2001 se je brez pravega razloga podvojilo število tajnih podatkov (Relyea, 2008). Z določanjem podatkov za tajne brez pravne podlage lahko prihaja do namernega zavajanja javnosti (Rourke, 1966, str. 183).

Vsak tajni podatek mora biti označen s stopnjo tajnosti in s podatki o organu.

Tajnost podatka preneha na določen datum, z nastopom določenega dogodka, s potekom določenega časa in s preklicem tajnosti. Kadar ni mogoče določiti načina prenehanja tajnosti podatka, tajnost preneha s potekom časa, ki je določen v zakonu, ki ureja arhivsko gradivo in arhive. Pooblaščena oseba mora tajne podatke stopnje tajnosti STROGO TAJNO pregledati enkrat letno, ostale stopnje tajnosti pa vsaka tri leta in oceniti, ali še obstaja potreba po njihovi tajnosti.

2.1.3 Dovoljenje za dostop do tajnih podatkov

Dovoljenja za dostop do tajnih podatkov stopenj tajnosti ZAUPNO, TAJNO ali STROGO TAJNO izdajajo pristojni organi oziroma funkcionarji v skladu z Zakonom o tajnih podatkih. O izdaji dovoljenja se obvesti nacionalni varnostni organ (Urad Vlade Republike Slovenije za varovanje tajnih podatkov).

Glede na predvideni dostop osebe do podatkov različnih stopenj tajnosti pristojni organ opravi (ZTP, 22.a člen):

- osnovno varnostno preverjanje (dostop do tajnih podatkov stopnje ZAUPNO),

- razširjeno varnostno preverjanje (dostop do tajnih podatkov stopnje TAJNO) in
- razširjeno varnostno preverjanje z varnostnim poizvedovanjem (dostop do tajnih podatkov stopnje STROGO TAJNO).

Med varnostnim preverjanjem so pristojni organi zbirali tudi podatke o zdravstvenem stanju preverjanega (Praprotnik, 2003, str. 2). Ustavno sodišče Republike Slovenije je s sklepom št. U-I-79/03-7 z dne 8. 5. 2003 zadržalo izvajanje varnostnega preverjanja oseb zaradi posega v človekove pravice, ki nastane z zbiranjem osebnih podatkov v postopku varnostnega preverjanja. Zaradi ustavitve varnostnega preverjanja in izdajanja novih dovoljenj za dostop do tajnih podatkov so imele osebe, ki so delovale v odborih Nata težave, ker je pogoj za sodelovanje v odborih veljavno dovoljenje za dostop do tajnih podatkov (Praprotnik, 2003, str. 2). Z uveljavitvijo novele Zakona o tajnih podatkih (Uradni list RS, št. 101/2003 (ZTP-A)) dne 22. 10. 2003 so se v postopku varnostnega preverjanja prenehali zbirati podatki o zdravstvenem stanju preverjanega, pristojni organi pa so začeli zopet izdajati dovoljenja za dostop do tajnih podatkov. V Združenih državah Amerike se zdravstveno stanje preverja ob preiskavi osebnega ozadja z enkratnim obsegom in v periodični ponovni preiskavi tega preverjanja ni več izrecno navedenega (Anžič in Trbovšek, 2001, str. 44).

Pri varnostnem preverjanju ne gre zgolj za zbiranje osebnih podatkov, ampak tudi za širši poseg v zasebnost (Žirovnik, 2001, str. 140).

Pri osnovnem varnostnem preverjanju pristojni organ preveri navedbe osebe v vprašalniku za varnostno preverjanje. Pri tem lahko od osebe in iz uradnih evidenc zbira in uporablja zakonsko določene podatke. Pri razširjenem varnostnem preverjanju pristojni organ poleg osnovnega varnostnega preverjanja od preverjane osebe, drugih organov, pristojnih za varnostno preverjanje, ali iz že obstoječih zbirk podatkov preveri še podatke iz posebnega vprašalnika. Če se ugotovi sum varnostnega zadržka, pristojni organ z varnostnim poizvedovanjem dodatno preveri tiste podatke, ki se nanašajo na posamezen varnostni zadržek, le če preverjana oseba s tem pisno soglaša in izpolni dodatni vprašalnik. V nasprotnem primeru lahko pristojni organ zavrne izdajo dovoljenja za dostop do tajnih podatkov.

Varnostno poizvedovanje se opravi tako, da pristojni organ opravi razgovor z osebami, ki jih je v dodatnem vprašalniku navedla preverjana oseba in ki lahko potrdijo podatke, navedene v vprašalnikih. Če se pri preverjanju podatkov ugotovi sum varnostnega zadržka, lahko pristojni organ preveri podatke v zvezi z varnostnim zadržkom tudi pri drugih osebah, organih ali organizacijah, ki o preverjani osebi kaj vedo.

Če se pri razširjenem varnostnem preverjanju in razširjenem varnostnem preverjanju z varnostnim poizvedovanjem osebe pojavi sum varnostnega zadržka, ki je povezan z njenim zakoncem ali zunajzakonskim partnerjem oziroma katero koli polnoletno osebo, ki živi s preverjano osebo v skupnem gospodinjstvu, se lahko z njimi opravi razgovor o

domnevnih varnostnih zadržkih, z njihovim pisnim soglasjem pa se lahko osnovno varnostno preverijo.

V Združenih državah Amerike se posebej preverjajo tudi potovanja v tujino, zveze s tujci, zdravstvene kartoteke in podobno (Brožič v: Mekina, 2001, str. 24).

V postopku varnostnega preverjanja je potrebno upoštevati spoštovanje človekovih pravic in temeljnih svoboščin (Črnčec, 2004). Interes države pri varovanju nacionalne varnosti mora biti sorazmeren s pomembnostjo posega v posameznikovo pravico do spoštovanja zasebnosti. Zakon o tajnih podatkih v postopku varnostnega preverjanja posega predaleč in ni sorazmeren s posameznikovimi ustavno zagotovljenimi pravicami (Lalić, 2003, str. 21).

Postopek varnostnega preverjanja oziroma postopek za izdajo dovoljenja za dostop do tajnih podatkov se začne na podlagi pisnega predloga predstojnika organa oziroma druge osebe, kot je določeno v Zakonu o tajnih podatkih, in mora vsebovati podatke o stopnji tajnosti, pisno soglasje preverjane osebe za varnostno preverjanje, dokazilo o opravljenem usposabljanju s področja obravnavanja tajnih podatkov, pisno izjavo o seznanitvi s predpisi s področja tajnih podatkov in zaprto ovojnico z izpolnjenim varnostnim vprašalnikom preverjane osebe.

Za pridobitev dovoljenja za dostop do tajnih podatkov stopnje tajnosti (ZTP, 25. člen):

- ZAUPNO je potrebno izpolniti osnovni vprašalnik,
- TAJNO je potrebno izpolniti osnovni in posebni vprašalnik,
- STROGO TAJNO je potrebno izpolniti osnovni, posebni in dodatni vprašalnik.

Pristojni organ izda osebi po opravljenem osnovnem varnostnem preverjanju dovoljenje za dostop do tajnih podatkov stopnje ZAUPNO z veljavnostjo desetih let, po razširjenem varnostnem preverjanju dovoljenje za dostop do tajnih podatkov stopnje TAJNO z veljavnostjo petih let, po razširjenem varnostnem preverjanju z varnostnim poizvedovanjem pa dovoljenje za dostop do tajnih podatkov stopnje STROGO TAJNO z veljavnostjo petih let.

Dovoljenje za dostop do tajnih podatkov je temporalna odločba, katerega veljava se po izteku v izreku določenega roka izteče. Zakon o tajnih podatkih bi bilo priporočljivo novelirati in opredeliti pravno podlago tako, da se ob izdaji novega dovoljenja za višjo stopnjo tajnosti prejšnje razveljavi z dnem veljavnosti novega dovoljenja oziroma se v izreku ali vsaj v obrazložitvi opredeli, kako novo dovoljenje vpliva na prejšnje, saj slednje z novim izgubi smisel (Kovač, 2008, str. 11 in 13).

Izdaja dovoljenja za dostop do tajnih podatkov se lahko zavrne, če obstajajo varnostni zadržki (ZTP, 27. člen):

- lažne navedbe podatkov preverjane osebe v varnostnem vprašalniku ali v razgovoru za varnostno preverjanje;
- neizbrisane pravnomočne obsodbe na najmanj tri mesece nepogojne zaporne kazni za kazniva dejanja, ki se preganjajo po uradni dolžnosti;
- dokončen disciplinski ukrep zaradi težje disciplinske kršitve s področja obravnavanja in varovanja tajnih podatkov;
- odvisnost od alkohola, drog oziroma druge zasvojenosti, ki bi lahko vplivale na zavrnitev izdaje dovoljenja;
- drugih ugotovitev varnostnega preverjanja, ki vzbujajo utemeljene dvome v posameznikovo verodostojnost, zanesljivost in lojalnost za varno obravnavanje tajnih podatkov idr.

Varnostni zadržki so ugotovitve varnostnega preverjanja, iz katerih izhaja, da obstajajo dvomi o zanesljivosti in lojalnosti osebe, ki naj bi dobila dovoljenje za dostop do tajnih podatkov (Weiss Janžek, 2008, str. 28).

Pri osebi z dovoljenjem za dostop do tajnih podatkov pri kateri obstaja sum obstoja varnostnega zadržka, se opravi vmesno varnostno preverjanje. Vmesno se varnostno preveri med drugim tudi oseba pred izvajanjem nalog na delovnih mestih, na katerih se zahteva dostop do tajnih podatkov, če je od izdaje dovoljenja do nastopa izvajanja nalog na delovnih mestih preteklo več kot 12 mesecev, in če oseba z veljavnim dovoljenjem po več kot 12 mesecih prične ponovno delati s tajnimi podatki.

Predstojnik organa predlaga uvedbo postopka vmesnega varnostnega preverjanja za ponovno potrditev veljavnosti dovoljenja. Postopek potrditve veljavnosti dovoljenja je enak postopku, kot je določen za izdajo dovoljenja za dostop do tajnih podatkov.

Osebi, ki ne da soglasja za uvedbo vmesnega varnostnega preverjanja ali ne da soglasja za uvedbo postopka potrditve veljavnosti dovoljenja, ali ne izpolni ustreznega varnostnega vprašalnika, se dovoljenje prekliče. Če oseba ne izpolnjuje pogojev za zasedbo delovnega mesta, ker ji je bilo zavrnjeno ali preklicano dovoljenje za dostop do tajnih podatkov, se uporabljajo določbe zakona, ki ureja sistem javnih uslužbencev.[1] Varnostno preverjanje je za delavce bodoči negotov dogodek, od katerega je v temelju odvisen delavčev položaj (Vodovnik, 2001, str. 91).

Izjemoma se osebi lahko dovoli enkraten dostop do tajnih podatkov, katerih stopnja tajnosti je za eno stopnjo višja od stopnje tajnosti, za katero je tej osebi izdano dovoljenje. Tak dostop je mogoč samo na podlagi pisne utemeljitve njenega predstojnika o razlogih za nujnost dostopa in je omejen le na tiste tajne podatke, ki so nujno potrebni za izpolnitev določenega dela.

[1] Zakon o javnih uslužbencih (Uradni list RS, št. 56/2002, 23/2005, 35/2005 – UPB1, 62/2005 – odločba US, 113/2005, 21/2006 – odločba US, 23/2006 – sklep US, 32/2006 – UPB2, 62/2006 – sklep US, 131/2006 – odločba US, 33/2007, 63/2007 – UPB3 in 65/2008).

Preverjenim osebam je praktično onemogočen vpogled v obdelane podatke, ki se nanašajo nanje, kar predstavlja problem, če varnostno preverjanje postavimo v kontekst ustavnih pravic zasebnosti (Kečanović, 2001, str. 187).

2.1.4 Dostop do tajnih podatkov in njihovo varovanje

Do tajnih podatkov imajo pravico dostopa samo osebe z dovoljenjem in se morajo s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog.[2] Dostop imajo samo do tajnih podatkov stopnje tajnosti, ki je določena v dovoljenju. Noben ne sme dobiti tajnega podatka prej in v večjem obsegu, kot je to potrebno za opravljanje njegovih delovnih nalog ali funkcije (ZTP, 31. člen).

Osebe imajo lahko dostop do tajnih podatkov stopnje INTERNO, če so predhodno opravile osnovno usposabljanje za obravnavo in varovanje tajnih podatkov, če podpišejo izjavo, da so seznanjene s pravnimi predpisi s področja tajnih podatkov in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi.[3]

Dostop do tajnih podatkov ni pravica vsakega posameznika, pač pa privilegij, ki je dodeljen zgolj tistim, za katere se v postopku varnostnega preverjanja oceni, da bodo nesporno varnostno zanesljivi v prihodnosti (Brožič, 2001, str. 161).

Prejemnik tajnih podatkov brez soglasja organa, ki mu je posredoval tajne podatke, ne sme posredovati teh podatkov drugim prejemnikom, razen če tako določajo pravni predpisi. Pooblaščena oseba organa mora vzpostaviti ažuren pregled in nadzor nad distribucijo tajnih podatkov zunaj organa. Iz pregleda mora biti razvidno, kdaj in komu so bili tajni podatki posredovani.

Organ mora uvesti postopke in ukrepe varovanja tajnih podatkov in preprečiti njihovo nepooblaščeno razkritje, predstojnik organa pa mora o tem izdati akt. Postopki in ukrepi obsegajo (ZTP, 38. člen):

- splošne varnostne ukrepe;
- varovanje oseb, ki imajo dostop do tajnih podatkov;
- varovanje prostorov;
- varovanje dokumentov in medijev, ki vsebujejo tajne podatke;
- varovanje komunikacij, po katerih se prenašajo tajni podatki;
- način označevanja stopenj tajnosti;
- varovanje opreme, s katero se obravnavajo tajni podatki;

[2] Pravni predpisi Evropske unije s področja tajnih podatkov določajo, da imajo osebe pravico dostopa do tajnih podatkov na podlagi potrebe po vedenju (angl. need to know), kar pomeni ožjo dodelitev pravice dostopa do tajnih podatkov glede na Zakon o tajnih podatkih.

[3] V Službi za tajne podatke se je večkrat pojavilo vprašanje, ali potrebujejo osebe za dostop do tajnih podatkov Evropske unije stopnje tajnosti RESTREINT UE dovoljenje za dostop do tajnih podatkov. V nadaljevanju specialističnega dela je podan odgovor na to vprašanje.

- način seznanitve uporabnikov z ukrepi in postopki varovanja tajnih podatkov;
- kontrolo in evidentiranje dostopov do tajnih podatkov;
- kontrolo in evidentiranje pošiljanja in distribucije tajnih podatkov.

Predstojnik organa je dolžan enkrat letno zagotoviti dodatno usposabljanje oseb, ki delajo s tajnimi podatki stopnje tajnosti ZAUPNO in višje.

Tajni podatki se v organih hranijo tako, da imajo dostop do podatkov le osebe z dovoljenjem za dostop do tajnih podatkov in ki jih potrebujejo pri opravljanju dela. Prenos tajnih podatkov izven prostorov organa je možen le ob upoštevanju predpisanih varnostnih ukrepov in postopkov, ki morajo zagotoviti, da jih prejme oseba, ki ima dovoljenje za dostop do tajnih podatkov in je do teh podatkov upravičena. Ukrepi in postopki varovanja pošiljanja tajnih podatkov izven prostorov organa se predpišejo glede na stopnjo tajnosti teh podatkov. Tajni podatki se ne smejo prenašati po nezaščitenih komunikacijskih sredstvih.

Osebe, ki ugotovijo, da je prišlo do izgube ali nepooblaščenega razkritja tajnih podatkov, morajo takoj obvestiti pooblaščeno osebo, ki mora poskrbeti za odpravo škodljivih posledic.

2.1.5 Nadzor nad izvajanjem pravnih predpisov s področja tajnih podatkov in predpisane sankcije za kršenje teh predpisov

Za notranji nadzor nad izvajanjem pravnih predpisov s področja tajnih podatkov so odgovorni predstojniki organov. Če se v organih obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje, se za notranji nadzor in strokovne naloge z delom s tajnimi podatki sistemizira delovno mesto ali pa se za to zadolži notranjo organizacijsko enoto organa.

Inšpekcijski nadzor opravlja Inšpektorat Republike Slovenije za notranje zadeve, na obrambnem področju pa Inšpektorat Republike Slovenije za obrambo.

Nacionalni varnostni organ spremlja in usklajuje stanje na področju dela s tajnimi podatki, skrbi za izvrševanje mednarodnih pogodb, izdaja in preklicuje dovoljenja osebam za dostop do tujih tajnih podatkov, sodeluje z nacionalnimi varnostnimi organi tujih držav in z mednarodnimi organizacijami ter vodi evidenco dovoljenj za dostop do tajnih podatkov.

Kršenje predpisov s področja tajnih podatkov se sankcionira z globo od 417,29 EUR pa do zapora do petih let.[4]

[4] Kazen zapora do petih let predpisuje 260. člen Kazenskega zakonika (Uradni list RS, št. 55/2008, 66/2008 – popravek in 39/2009).

Zloraba instituta tajnosti nastane domnevno zaradi postavljanja posameznika pred drugimi delavci, kot odziv na kompleks manjvrednosti, kot dokazovanje pomembnosti dostopa do izbranih, ožjemu krogu ljudi dosegljivih podatkov, včasih pa tudi kot prikrivanje strokovnega neznanja (Arnejčič, 2001, str. 75).

"Odgovornost tistih, ki so sicer po zakonu pooblaščeni, da pridobivajo, uporabljajo, posredujejo – obdelujejo podatke o zasebnosti državljanov in tajnih zadevah države, dobesedno "kriči in tuli" po nadzoru ter doslednem sankcioniranju kršitev in zlorab." (Kečanović, 2002, str. 10).

2.2 UREDBA O VAROVANJU TAJNIH PODATKOV

2.2.1 Ukrepi varovanja tajnih podatkov

Z Uredbo o varovanju tajnih podatkov (Uradni list RS, št. 74/2005) so določeni načini in oblike označevanja tajnih podatkov, fizični, organizacijski in tehnični ukrepi ter obvezne sestavine postopkov za varovanje tajnih podatkov, ki jih morajo pri vzpostavitvi sistema ukrepov in postopkov varovanja tajnih podatkov upoštevati in zagotoviti vsi organi (UVTP, 1. člen).

Sistem postopkov in ukrepov varovanja tajnih podatkov, ki ustreza stopnji tajnosti in količini tajnih podatkov ter onemogoča njihovo razkritje nepooblaščenim osebam, se vzpostavi z naslednjimi ukrepi (UVTP, 2. člen):

- fizični ukrepi (neposredno fizično varovanje tajnih podatkov, prostorov ali objektov);
- organizacijski ukrepi (ravnanje organa pri pripravi, pošiljanju, hrambi, uničenju in označevanju tajnih podatkov) in
- tehnični ukrepi (varovanje tajnih podatkov, prostorov ali objektov s tehničnimi sredstvi).

Poleg teh ukrepov ali namesto njih se za tuje tajne podatke izvajajo tudi drugi varnostni ukrepi, ki so določeni z mednarodno pogodbo.

2.2.2 Označevanje tajnih podatkov

Pisni dokumenti morajo imeti stopnjo tajnosti označeno v glavi in nogi vseh strani dokumenta, v nogi poleg stopnje tajnosti pa mora biti navedena tudi zaporedna številka strani glede na skupno število strani dokumenta (na primer 3/10). Naslovna stran dokumenta je lahko brez oznake zaporedne številke strani. Oznaka stopnje tajnosti mora biti na medijih (na primer zemljevidi, fotografije, slikovni in zvočni zapisi)

in na morebitnih ovojih medija vidno natiskana, natipkana, napisana, naslikana, nalepljena ali kako drugače pritrjena s primernimi sredstvi.

Dokumenti ali mediji stopnje tajnosti TAJNO in STROGO TAJNO morajo imeti še podatke o številki izvoda dokumenta, številu, številki in datumu morebitnih prilog. Dokumenti stopnje tajnosti STROGO TAJNO se morajo dodatno označiti z rdečo črto debeline najmanj štiri milimetre, ki poteka diagonalno pod kotom 45 stopinj štiri centimetre od zgornjega desnega roba strani. Različne stopnje tajnosti dokumentov morajo biti označene z različnimi vrstami pisav. Višja je stopnja tajnosti dokumenta, večje morajo biti črke za oznako tajnosti. Pisna ocena, na podlagi katere je bila določena stopnja tajnosti podatka, se hrani kot priloga dokumenta.

Dokument ima lahko označene določene odstavke z različno stopnjo tajnosti, s tem da je začetek in konec odstavka označen s simboli (I), (Z), (T) ali s (ST). Dokument mora biti označen z najvišjo stopnjo tajnosti posameznega odstavka.

Kopija dokumenta mora imeti oznako stopnje tajnosti izvirnika in oznako, da je kopija. Na strani dokumenta se v višini zgornje oznake stopnje tajnosti na desno stran napišeta beseda KOPIJA in njena zaporedna številka. Enako se označi kopija tajnega podatka v elektronski obliki. Pri izvirniku dokumenta je potrebno evidentirati prejemnike kopij.

V primeru spremembe ali preklica stopnje tajnosti, se na dokumentu ali mediju prečrtajo prvotne oznake tajnosti, pod staro oznako ali nad njo pa se označi z novo oznako stopnja tajnosti oziroma preklic, dokumentu ali mediju pa se priloži dokument, ki je podlaga za spremembo stopnje tajnosti. Pooblaščena oseba mora zagotoviti, da so o spremembi tajnosti obveščeni vsi prejemniki.

2.2.3 Obdelava in hramba tajnih podatkov

Tajni podatki stopnje tajnosti INTERNO se lahko obravnavajo in hranijo v upravnem območju, tajni podatki višjih stopenj tajnosti pa v varnostnem območju I. ali II. stopnje.

Vstop v varnostno območje I. stopnje pomeni že dostop do tajnih podatkov (primer: zemljevid na steni, ki ima določeno stopnjo tajnosti). V tem območju je potrebno izvajati naslednje varnostne ukrepe (UVTP, 10. člen):

- sistem vhodnega nadzora, ki zagotavlja popoln nadzor nad vstopom oziroma izstopom oseb in vozil v to območje, dovoljuje vstop samo osebam, ki imajo ustrezno dovoljenje za dostop do tajnih podatkov in so v tem območju zaposlene oziroma imajo posebno dovoljenje za vstop v to območje;
- vodenje razvida tajnih podatkov, s katerimi se oseba seznani že ob samem vstopu v varnostno območje;

- prepoved vnosa mehanskih, elektronskih in magnetno optičnih naprav;
- neposredno in neprekinjeno fizično varovanje varnostnega območja ali elektronski sistem za protivlomno varovanje območja, katerega alarmni signal je vezan na nadzorni center (čas za intervencijo mora znašati manj od sedmih minut) in kjer mora biti zagotovljen celovit nadzor območja iz nadzornega centra, sistem pa mora imeti zagotovljeno rezervno napajanje;
- po končanem delovnem času se pregledajo prostori.

Oseba lahko vstopi v varnostno območje I. stopnje le na podlagi izdanega dovoljenja s strani pooblaščene osebe.

Vstop v varnostno območje II. stopnje ne omogoča dostopa do tajnih podatkov (tajni podatki so ustrezno shranjeni), v njem pa se izvajajo naslednji ukrepi (UVTP, 10. člen):

- sistem vhodnega nadzora, ki vstop v območje dovoljuje samo osebam z ustreznim dovoljenjem za dostop do tajnih podatkov in morajo v območje vstopiti zaradi opravljanja delovnih nalog;
- osebe, ki delajo v varnostnem območju, imajo dostop le do tistih tajnih podatkov, ki jih potrebujejo za opravljanje delovnih nalog;
- sistem nadzora gibanja, ki zagotavlja, da druge osebe vstopajo v varnostno območje samo v spremstvu v varnostnem območju zaposlene osebe ali ob izvajanju druge enakovredne oblike nadzora, ki zagotavlja, da bo oseba vstopila samo v dele območja, povezane z namenom obiska, in če je to potrebno, se bo seznanila le s tistimi tajnimi podatki, ki so povezani z namenom obiska;
- dovoljen je vnos mehanskih, elektronskih in magnetno optičnih naprav, vendar morajo biti izključene. Njihovo uporabo odobri pristojna oseba;
- po končanem delovnem času se območje varuje s sistemom fizičnega ali protivlomnega varovanja.

Varnostno območje meji na upravno območje, ki lahko obsega vse poslovne prostore organa. V upravnem območju je lahko vzpostavljen nadzor vstopanja oziroma gibanja oseb in vozil.

Dostopi oseb in vozil v varnostna območja morajo biti pod nadzorom in evidentirani, osebe pa morajo imeti na vidnem mestu pripete identifikacijsko izkaznico.

Varnostna in upravna območja določi predstojnik organa s sklepom, pred tem pa si mora organ pridobiti mnenje nacionalnega varnostnega organa o ustreznosti varnostnotehnične opreme in ukrepov varovanja območja.

Pred vstopom v varnostno območje mora biti na vidnem mestu obvestilo o varnostnem območju z ukrepi, ki se izvajajo v območju. Iz varnostnih razlogov lahko predstojnik organa v sklepu o določitvi varnostnega območja določi, da se varnostno območje ne označi z obvestilom.

Vstop zaposlenih v varnostna in upravna območja se nadzira s fizičnim nadzorom, ki ga lahko dopolnjuje sistem samodejnega prepoznavanja identifikacijskih kartic oziroma biometričnih značilnosti vstopajočih oseb (na primer vstop s čitalcem prstnega odtisa). Pri vstopu ostalih oseb mora biti izkazan tudi namen obiska, osebi pa se izda začasna identifikacijska kartica, njeno gibanje v varnostnem območju pa mora biti ustrezno nadzirano in evidentirano.

Naprave za obdelovanje tajnih podatkov v varnostnih območjih lahko uporabljajo samo za ta namen pooblaščene osebe (na primer uporaba fotokopirnega stroja).

Zunaj varnostnega območja se lahko obdelujejo tajni podatki, če je območje fizično ali tehnično varovano, dostop do območja pa nadzorovano. Tajni podatek mora imeti oseba ves čas pod nadzorom, po končani obdelavi pa ga mora vrniti v varnostno območje. Tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje se lahko obravnavajo izven prostorov organa v skladu z načrtom ukrepov in postopkov za varovanje tajnega podatka, ki ga izdela odgovorna oseba. 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.[5]

Da bi se varnostno območje I. stopnje in varnostna območja, kjer se ustno razpravlja o tajnih podatkih stopnje tajnosti TAJNO ali višje stopnje, zaščitilo pred poskusi prisluškovanja, je potrebno opraviti protiprisluškovalni pregled območij s strani pristojnih organov (UVTP, 18. člen):

- ob določitvi varnostnega območja,
- ob vsakem posegu v območju,
- ob spremembi zaposlenih v območju in
- najmanj vsakih dvanajst mesecev.

Tajni podatki stopnje tajnosti INTERNO se hranijo v pisarniških ali kovinskih omarah, stopnje tajnosti ZAUPNO in TAJNO v blagajnah protivlomne stopnje II, stopnje tajnosti STROGO TAJNO pa v blagajnah protivlomne stopnje III. Na blagajnah se v zgornji levi kot vrat pritrdi oznaka glede na stopnjo tajnosti podatkov v blagajni s črkami Z, T in ST.

Predstojnik organa določi osebe, ki poznajo nastavitve kombinacij ključavnic na blagajnah, nastavitve pa je potrebno zamenjati (UVTP, 20. člen):

- po namestitvi blagajn,
- vsakih šest mesecev in
- ko oseba, ki je poznala nastavitev, preneha opravljati naloge v organu.

[5] Osebam, ki izgubijo tajni podatek, se lahko odpove delovno razmerje.

Ključi varnostnega območja se morajo hraniti v posebnem prostoru zunaj tega območja, kjer je onemogočen dostop nepooblaščenim osebam.

2.2.4 Prenos tajnih podatkov

Tajni podatki se prenašajo v zaprti in neprosojni ovojnici. Tajni podatki stopnje tajnosti INTERNO se lahko prenašajo zunaj varnostnega območja po lastni prenosni mreži ali priporočeni pošti s povratnico[6], stopnje tajnosti ZAUPNO ali višje stopnje pa po lastni prenosni mreži ali s kurirsko službo v dveh ovojnicah, kjer je zunanja ovojnica iz trdnega, neprosojnega in neprepustnega materiala in na kateri morajo biti podatki o naslovniku, pošiljatelju in številki dokumenta. Iz zunanje ovojnice ne sme biti razvidno, da vsebuje tajni podatek. Notranja ovojnica mora imeti oznako stopnje tajnosti, številko dokumenta in podatke o naslovniku in pošiljatelju. Pri prenosu tajnih podatkov stopnje tajnosti ZAUPNO in TAJNO zunaj varnostnega območja se namesto zunanje ovojnice lahko uporabi zaklenjen ali zapečaten kovček, škatla ali torba. Pri prenosu tajnih podatkov stopnje tajnosti STROGO TAJNO zunaj varnostnega območja se namesto zunanje ovojnice uporabi zaprt kovček, škatla ali torba z zapiranjem na ključ ali šifrirno kombinacijo, pri prenosu pa sodelujeta najmanj dve osebi.

V organu se mora določiti, kje se sprejemajo nosilci tajnih podatkov in kdo jih sprejema. Naslovnik ali oseba, ki je pooblaščena za sprejem nosilcev tajnih podatkov, potrdi njihov prejem z vpisom v dostavno oziroma kurirsko knjigo. Osebe, ki prenašajo tajne podatke, morajo biti varnostno preverjene glede na stopnjo tajnosti tajnih podatkov, ki jih prenašajo.

Za prenose tajnih podatkov stopnje tajnosti TAJNO ali višje stopnje zunaj varnostnih območij organi izdelajo načrt poti in varovanja prenosa tajnih podatkov, ki mora vsebovati tudi ukrepe ob morebitnem poskusu odtujitve tajnih podatkov, prometnih nesrečah, prenočevanju in drugih podobnih dogodkih z določenimi glavnimi in pomožnimi potmi.

Kurirji se morajo usposabljati najmanj enkrat na leto za varnost prenosa tajnih podatkov pri pristojnih organih, pri prenosu tajnih podatkov stopnje tajnosti ZAUPNO ali višje stopnje pa morajo imeti pisno pooblastilo predstojnika organa za prenos tajnih podatkov, ki ga morajo pokazati na zahtevo osebe, ki predaja oziroma prejema tajne podatke. Policisti morajo kurirju na njegovo zaprosilo zagotavljati pomoč. Nobena oseba nima pravice vpogleda v tajne podatke (na primer carinik), v kolikor se kurir izkaže z veljavnim pooblastilom.

[6] V praksi se prenos po pošti ne uporablja zaradi nevarnosti izgube oziroma razkritja tajnih podatkov.

2.2.5 Razmnoževanje tajnih podatkov

Tajne podatke se lahko kopira na podlagi pisarniške odredbe s strani pooblaščene osebe v varnostnem območju.[7] Pri kopiji mora biti razvidno, iz katerega dokumenta oziroma dela dokumenta je narejena kopija (številka, datum dokumenta in številka strani). Na dokumentu mora biti označena morebitna prepoved kopiranja. V Zvezni republiki Nemčiji tajne podatke najnižje stopnje tajnosti ni potrebno kopirati v varnostnem območju (Bundesamt für Sicherheit in der Informationstechnik, 2006), v državah članicah zveze Nato pa se jih lahko kopira v upravnem območju (North Atlantic Council, 2002).

Tajne podatke stopnje tajnosti STROGO TAJNO se ne sme kopirati. Kopijo se lahko izdela le v organu, kjer je bil izdan izvirnik dokumenta.

2.2.6 Evidentiranje tajnih podatkov

Tajne podatke se evidentira na podlagi Uredbe o varovanju tajnih podatkov in Uredbe o upravnem poslovanju (Uradni list RS, št. 20/2005, 106/2005, 30/2006, 86/2006, 32/2007, 63/2007, 115/2007, 122/2007 – popravek, 31/2008 in 35/2009).[8] Iz vpisov v evidenco tajnih podatkov ne sme biti razvidna vsebina tajnega podatka.

Elektronski sistem hrambe tajnih podatkov mora biti fizično ločen od drugih informacijskih sistemov, lahko pa se uporablja tehnologija navideznega zasebnega omrežja s kriptozaščitnimi postopki in ukrepi.

Za tajne podatke stopnje tajnosti TAJNO in STROGO TAJNO je potrebno voditi seznam vpogledov, ki vsebuje (UVTP, 29. člen):

- številko, datum, stopnjo tajnosti in številko izvoda dokumenta s tajnim podatkom;
- ime in priimek osebe, ki se je seznanila s tajnim podatkom;
- datum in čas seznanitve;[9]
- način seznanitve;
- podpis osebe, ki se je seznanila s tajnim podatkom.

Seznam vpogledov se hrani skupaj z dokumentom, ki vsebuje tajne podatke.

---

[7] Najbolj pogosto kršitev pri delu s tajnimi podatki predstavlja protipravno kopiranje tajnih podatkov s strani nepooblaščenih oseb. Za tako ravnanje se lahko osebi odpove delovno razmerje.

[8] Službe za tajne podatke porabijo večino časa za evidentiranje in izdelavo kopij tajnih podatkov stopnje tajnosti INTERNO, saj je teh podatkov količinsko največ napram ostalim stopnjam tajnosti.

[9] Datum in čas seznanitve sta pomembna elementa pri zbiranju informacij ob morebitnem odtekanju tajnih podatkov.

2.2.7 Uničenje in arhiviranje tajnih podatkov

Tajne podatke lahko uniči tričlanska komisija za uničenje tajnih podatkov, ki jo določi pooblaščena oseba. En član komisije mora biti oseba, ki je v organu pristojna za delo s tajnimi podatki. V zapisnik o uničenju tajnih podatkov se vpišejo številka, datum in stopnja tajnosti uničenega podatka, pri uničenju tajnih podatkov stopnje tajnosti STROGO TAJNO pa je potrebno obvestiti organ, ki je izdal dokument. Seznam vpogledov se ne sme uničiti, ampak se ga priloži zapisniku.[10] Tajne podatke je potrebno uničiti do nerazpoznavnosti.[11]

Tajni podatki se arhivirajo v skladu s pravnimi prepisi, ki urejajo arhivsko dejavnost. Pri zajemu in pretvorbi papirnatega gradiva z optičnim bralnikom v digitalno obliko se ga ne sme uničiti, ampak ga je potrebno arhivirati (Žumer, 2008, str. 41 in 50).

V zvezi z dostopom do arhivskega gradiva, ki ga hranijo javni arhivi, je v demokratičnih državah zakonodajalcem naloženo, naj najdejo pravo pot med transparentnostjo in potrebnim varovanjem tajnosti ter pravic posamezika (Križaj, 2007, str. 72).

Javno arhivsko gradivo, ki vsebuje podatke, ki se nanašajo na državno in javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države ter njene gospodarske interese ter poslovne in davčne skrivnosti, in katerih razkritje nepoklicani osebi bi lahko povzročilo škodljive posledice za varnost države in drugih oseb ter njihove interese, postane dostopno za uporabo praviloma najkasneje 40 let po nastanku (ZVDAGA, 65. člen).

Podatke, informacije oziroma dokumente, ki so določeni kot tajni, moramo varovati na predpisan način vse od nastanka pa do poteka roka tajnosti. Velika večina tajnih dokumentov ima tudi značaj trajnega arhivskega gradiva, ki se izroča pristojnim javnim arhivom še med veljavnostjo tajnosti ali po prenehanju. Tudi arhivi morajo po prevzemu tajnega gradiva ali gradiva z osebnimi podatki varovati različne stopnje in roke tajnosti (Žumer, 2003, str. 17). V Sloveniji bo potrebno urediti ravnanje s tajnimi arhivi in varovanje osebnih in drugih občutljivih podatkov, ki jih vsebuje arhivsko gradivo (Žumer, 2003, 24).

2.2.8 Načrt varovanja tajnih podatkov

V organu je potrebno v načrtu varovanja tajnih podatkov natančno predpisati fizične, organizacijske in tehnične ukrepe za varovanje tajnih podatkov v varnostnih območjih

[10] Drugo najbolj pogosto kršitev pri delu s tajnimi podatki predstavlja uničevanje ali izgubo tajnih podatkov s strani prejemnikov tajnih podatkov.
[11] Uničevanje z ustreznim rezalnikom papirja ali z industrijskim uničenjem (s pomočjo kemičnih sredstev).

organa, ki obsega splošni in posebni del. Za tajne podatke do stopnje tajnosti ZAUPNO zadostuje izdelan posebni načrt varovanja (UVTP, 32. člen).

Splošni del načrta varovanja vsebuje (UVTP, 33. člen):

- oceno ogroženosti;
- opis glavnega in pomožnih objektov (lega, vhodi, izhodi, zasilni izhodi, skica oziroma fotografije objekta, glavne in pomožne poti do objekta in podatki o varnostnotehnični opremi);
- podatke o nosilcu varnostnega načrta;
- zaščitne ukrepe za osebe, ki imajo dostop do tajnih podatkov.

Posebni del načrta varovanja vsebuje (UVTP, 33. člen):

- ukrepe fizičnega varovanja (zunanje in notranje fizično varovanje, varnostne točke z opisi nalog izvajalcev);
- ukrepe tehničnega varovanja (zunanje in notranje tehnično varovanje, nadzor nad vstopom in izstopom, alarmni sistem in postopki ob sprožitvah posameznih stopenj alarmov, dokumentiranje);
- postopke ob nasilnem vstopu in nepredvidenem dogodku (požaru, potresu, povodnji in drugih naravnih nesrečah);
- postopke in ukrepe ob izgubi, razkritju ali odtujitvi tajnega podatka;
- ukrepe in postopke pri opravljanju vzdrževalnih in drugih del v varnostnih območjih.

Načrt varovanja je potrebno stalno dopolnjevati in ga enkrat na leto pregledati.[12]

2.2.9 Postopek ob zlorabi tajnega podatka

V primeru ugotovitve zlorabe tajnega podatka je potrebno takoj seznaniti pooblaščeno osebo, preprečiti možnost nadaljnje zlorabe in poskušati izslediti odtujeni tajni podatek. Obvesti se tudi organ, ki je določil tajnost podatku, in nacionalni varnostni organ. Če se pri zlorabi kaže sum kaznivega dejanja, mora predstojnik organ seznaniti policijo.

V seznanitvi se navede podatke, ki so potrebni za izsledite tajnega podatka (vrsta medija tajnega podatka, stopnja tajnosti, organ, številka, datum, številka kopije, prejemnik, kratka vsebina, opis okoliščin zlorabe, seznam oseb, ki so oziroma bi lahko imele dostop do tajnega podatka, informacija o obvestilu organu, ki je določil tajni podatek, in seznam izvedenih ukrepov o preprečitvi nadaljnje zlorabe).

[12] Načrtu varovanja je potrebno določiti stopnjo tajnosti in ga distribuirati čim manjšemu številu oseb.

2.3 UREDBA O VARNOSTNEM PREVERJANJU IN IZDAJI DOVOLJENJ ZA DOSTOP DO TAJNIH PODATKOV

Z Uredbo o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Uradni list RS, št. 71/2006 in 138/2006) je (UVPIDDTP, 1. člen):

- določen postopek varnostnega preverjanja oseb, ki zaradi opravljanja delovnih nalog potrebujejo dovoljenje za dostop do tajnih podatkov, postopek vmesnega varnostnega preverjanja in postopek izdaje in preklica dovoljenja;
- določen postopek izdaje in preklica dovoljenja osebam za dostop do tujih tajnih podatkov;
- predpisan program in način osnovnega in dodatnega usposabljanja oseb za delo s tajnimi podatki.

V sistemizaciji in organizaciji delovnih mest v organih morajo biti opredeljena delovna mesta, kjer se zahteva dostop do tajnih podatkov Republike Slovenije in do tujih tajnih podatkov pri opravljanju dela.[13] Ker nekateri zaposleni ne pridobijo dovoljenja za dostop do tajnih podatkov, morajo zamenjati svoje delovno področje, čeprav so strokovnjaki na tem področju (Brožič, 2002, str. 31). Varnostno preverjanje oseb je faza kadrovskega postopka, ki zagotavlja kadre, ki bodo sposobni varovati tajnost podatkov glede na stopnjo tajnosti oziroma spoštovati predpise o tajnosti podatkov. Torej v tem primeru govorimo o profesionalizaciji in strokovnosti (Miklavčič, 2001, str. 97).

2.3.1 Postopek varnostnega preverjanja

Postopek varnostnega preverjanja se prične na pisni predlog predstojnika organa ali osebe, ki jo predstojnik pooblasti, z osebnimi podatki osebe in stopnjo tajnosti, za katero se izdaja dovoljenje za dostop do tajnih podatkov. K predlogu se predloži (UVPIDDTP, 4. člen):

- potrdilo o opravljenem osnovnem usposabljanju s področja varovanja tajnih podatkov, mlajše od enega leta;
- pisno soglasje osebe za varnostno preverjanje;
- izjavo o seznanitvi s predpisi s področja tajnih podatkov in
- izpolnjene ustrezne vprašalnike za varnostno preverjanje.

Z varnostnim preverjanjem se preverijo podatki o osebi iz varnostnih vprašalnikov. Če se pojavijo varnostni zadržki pri osnovnem ali razširjenem varnostnem preverjanju, pristojni organ pozove preverjano osebo za predložitev soglasja za varnostno preverjanje z varnostnim poizvedovanjem in izpolnjenega dodatnega vprašalnika ter je pouči o posledici opustitve teh dejanj.

[13] Zavrnitev izdaje dovoljenja za dostop do tajnih podatkov pomeni neizpolnjevanje pogojev za zasedbo delovnega mesta, česar posledica je odpoved delovnega razmerja.

Uradna oseba organa v postopku varnostnega preverjanja za razjasnitev določenih okoliščin lahko opravi pogovor s preverjano osebo in drugimi relevantnimi osebami, pri tem pa ne sme ogroziti virov informacij, ki se nanašajo na podatke iz varnostnih vprašalnikov. Pogovor se sklene z zapisnikom.

Če se pri razširjenem varnostnem preverjanju in pri razširjenem varnostnem preverjanju z varnostnim poizvedovanjem pokaže varnostni zadržek, se lahko po pogovoru s preverjano osebo opravi pogovor z njenim zakoncem ali zunajzakonskim partnerjem oziroma katero koli polnoletno osebo, ki živi s preverjano osebo v skupnem gospodinjstvu, ki se je lahko z njenim soglasjem osnovno varnostno preveri. V kolikor oseba odkloni osnovno varnostno preverjanje, organ odloči o dovoljenju za dostop do tajnih podatkov na podlagi zbranih podatkov.[14]

Pristojni funkcionar izda preverjani osebi dovoljenje za dostop do tajnih podatkov v obliki pisne odločbe in kartice, če varnostni zadržki v postopku pridobitve dovoljenja niso bili izkazani, v nasprotnem primeru se izdaja dovoljenje zavrne.

2.3.2 Vmesno varnostno preverjanje in varnostno preverjanje za potrditev veljavnosti dovoljenja

Predstojnik organa lahko za osebo, pri kateri se pojavi sum varnostnega zadržka, predlaga pristojnemu organu vmesno varnostno preverjanje. Če se pri osebi potrdi varnostni zadržek, se ji dovoljenje za dostop do tajnih podatkov prekliče. Če oseba nasprotuje vmesnemu varnostnemu preverjanju ali če v določenem roku ne izpolni obrazca za vmesno varnostno preverjanje, predstojnik organa poda predlog pristojnemu organu za preklic dovoljenja za dostop do tajnih podatkov.[15]

Predstojnik organa poda pisni predlog pristojnemu organu za začetek postopek varnostnega preverjanja za potrditev veljavnosti dovoljenja, osebo pa mora o tem pisno seznaniti ter jo pozvati za izdajo pisnega soglasja na predpisanem obrazcu.

2.3.3 Tuji tajni podatki

Nacionalni varnostni organ izdaja dovoljenja za dostop do tujih tajnih podatkov na podlagi pisnega predloga (zaprosila) predstojnika organa ali njegovega pooblaščenca oziroma druge osebe v skladu z Zakonom o tajnih podatkov, ki mora vsebovati (UVPIDDTP, 16. člen):

- ime in priimek osebe,
- datum in kraj rojstva osebe,

[14] Organ v tem primeru zavrne izdajo dovoljenja za dostop do tajnih podatkov.
[15] Preklic dovoljenja pomeni neizpolnjevanje potrebnih pogojev za zasedbo delovnega mesta.

- navedbo tuje države ali mednarodne organizacije, katere tajne podatke bo obdelovala oseba, in
- naziv delovnega mesta.

K predlogu je potrebno predložiti izjavo o seznanitvi osebe s predpisi o varovanju tujih tajnih podatkov (Evropska unija, Nato itd.).

Dovoljenje za dostop do tujih tajnih podatkov se izda osebi za čas dela s tujimi tajnimi podatki v organu, če ima veljavno dovoljenje za dostop do tajnih podatkov Republike Slovenije. Po prenehanju dela s tujimi tajnimi podatki, nacionalni varnostni organ dovoljenje prekliče po predhodnem obvestilu predstojnika organa.

2.3.4 Najave obiskov in preveritve dovoljenj

Obiske v tujini, kjer se bodo obravnavali tuji tajni podatki, najavi najmanj pet dni pred obiskom predstojnik organa pri nacionalnem varnostnem organu, ki posreduje najavo organu tuje države ali mednarodne organizacije v skladu z mednarodno pogodbo ali predpisi mednarodnih organizacij.

Nacionalni varnostni organ sprejema najave obiskov tujih predstavnikov v Republiki Sloveniji, ki morajo imeti dovoljenje za dostop do tajnih podatkov matične države. V kolikor se tuji predstavnik ne more izkazati z dovoljenjem, nacionalni varnostni organ preveri pri pristojnih organih v tujini o ustreznosti dovoljenj tujih predstavnikov v skladu z mednarodno pogodbo ali predpisi mednarodnih organizacij.

2.3.5 Usposabljanje za obravnavo in varovanje tajnih podatkov

Eden izmed pogojev, ki mora biti izpolnjen, da oseba pridobi pravico (dovoljenje) dostopa do tajnih podatkov, je opravljen tečaj osnovnega usposabljanja za obravnavo in varovanje tajnih podatkov.

Dodatnega usposabljanja za obravnavo in varovanje tajnih podatkov se morajo enkrat na leto udeležiti osebe, ki imajo dovoljenje za dostop do tajnih podatkov stopnje tajnosti ZAUPNO ali višje in ki delajo s tajnimi podatki. Dodatno usposabljanje predstavlja skrajšano obliko osnovnega usposabljanja s specifičnimi primeri s področja tajnih podatkov.

Osnovno in dodatno usposabljanje izvajajo v organih s strani predstojnika organa določene osebe, lahko pa ga izvaja tudi nacionalni varnostni organ ali organizacija,

katere osnovna dejavnost je usposabljanje in izobraževanje posameznikov. Po končanem usposabljanju se udeležencem izda potrdilo.[16]

2.4 SKLEP O DOLOČITVI POGOJEV ZA VARNOSTNOTEHNIČNO OPREMO, KI SE SME VGRAJEVATI V VARNOSTNA OBMOČJA

2.4.1 Varnostnotehnična oprema varnostnega območja

S Sklepom o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja (Uradni list RS, št. 94/2006) so določeni minimalni varnostni pogoji, ki jim mora ustrezati varnostnotehnična oprema v varnostnih območjih (SDPVOVVO, 1. člen).

Varnostno območje mora imeti zidove narejene iz armiranega betona ali iz drugega materiala enake trdnosti (SDPVOVVO, 2. člen):

- zunanji zidovi morajo biti široki 15 centimetrov;
- če se nahaja varnostno območje v drugem nadstropju poslopja ali višje, so zidovi lahko široki 10 centimetrov; in
- zidovi, ki mejijo na upravno območje, morajo biti široki 10 centimetrov.

Na zidove varnostnega območja je treba namestiti tipala alarmne naprave, ki zaznava tresenje, standarda SIST EN 50131 (razred 3), če so zidovi del zunanjih zidov drugega objekta, ki ga organ ne nadzira.

Vstop v varnostno območje mora biti zaščiten s protivlomnimi vrati s tritočkovnim zapiranjem standarda SIST EN 1627 (stopnja 4), ki imajo na zunanjem delu slepo kljuko in protivlomno zaščiteno ključavnico s cilindričnim vložkom po standardu SIST EN 1303 (stopnja mehanske odpornosti 2). Protivlomna vrata se za vsakim odpiranjem zapirajo s pomočjo vgrajenega samodejnega zapirala.

Na oknih se namestijo kontaktni senzorji standarda SIST EN 50131 (razred 3) ali pa kovinsko okovje s ključavnico. V pritličju in kletnih prostorih je na notranjih straneh oken kovinska plošča debeline dveh milimetrov z odprtinami dveh centimetrov, ki onemogoča iznos kakršnihkoli predmetov. Na oknih, ki mejijo na nenadzorovano območje, se do višine pet metrov in pol z notranje strani namestijo kovinske varnostne rešetke premera dveh centimetrov z razmakom 15 centimetrov ali pa jih nadomestijo okna z vgrajenim protivlomnim steklom standarda SIST EN 356 (razreda P 8 B oziroma razreda P 6 B v primeru fizičnega nadzora objekta z zunanje strani).

[16] Na podlagi potrdila o osnovnem usposabljanju in s podpisom izjave o seznanitvi s pravnimi predpisi s področja tajnih podatkov in o zavezi ravnanja s tajnimi podatki v skladu s temi predpisi imajo lahko osebe dostop do tajnih podatkov stopnje tajnosti INTERNO.

Površina prezračevalnega ali klimatizacijskega sistema, ki je povezan z varnostnim območjem, mora znašati do 200 cm2, v nasprotnem primeru pa mora biti zaščitena z znotraj pritrjenimi varnostnimi rešetkami z odprtinami do 200 cm2. Zunanji del sistema mora onemogočiti nepooblaščen dostop oseb in prenos zvoka iz varnostnega območja.

Tajni podatki stopnje tajnosti ZAUPNO in TAJNO se hranijo v blagajnah standarda SIST EN 1143, stopnje tajnosti STROGO TAJNO pa standarda SIST EN 1143. Blagajne morajo biti opremljene z elektronsko ali pa mehansko ključavnico standarda SIST EN 1300 (razred B).

Ključi varnostnega območja se hranijo v upravnem območju ali prostoru z neprekinjenim fizičnim ali tehničnim varovanjem (SDPVOVVO, 11. člen):

- v blagajni standarda SIST EN 1143 ustrezne protivlomne stopnje z nameščeno elektronsko ključavnico standarda SIST EN 1300 razreda B ali pa
- v elektronskem sistemu za shranjevanje ključev (sistem ključar) standarda SIST EN 50131.[17]

Tajni podatki v papirnati obliki se uničujejo z rezalnikom papirja, ki zagotavlja vzdolžni in prečni razrez papirja velikosti 0,8 mm x 15 mm (razrez do nerazpoznavnosti in neobnovljivosti tajnih podatkov).[18]

Pred vhodom v varnostno območje I. stopnje morajo biti (SDPVOVVO, 13. in 14. člen):

- postavljene omarice za shranjevanje elektronskih naprav, ki se ne smejo vnašati v varnostno območje;
- postavljena detektorska vrata za odkrivanje orožja in kovin, ki jih lahko nadomestijo ročni detektorji ali pa detektorska vrata pred vhodom v poslopje.

Če je na vhodu ali izhodu nameščen sistem pristopne kontrole, mora ustrezati standardu SIST EN 50133 (razred 3, kategorija pristopa B).[19]

Objekt z varnostnim območjem mora imeti osvetljene vse vhode in izhode z osvetljenostjo najmanj 40 luksov. Za osvetlitev se lahko uporabljajo senzorska stikala. Osvetlitev lahko nadomestijo infrardeči reflektorji za nočno osvetljevanje.

Če je objekt opremljen z videonadzorom, morajo biti izpolnjeni naslednji pogoji (SDPVOVVO, 17. člen):

- visokoresolucijske kamere morajo imeti najmanj 460 linij horizontalne resolucije in pokrivati vse vhode in izhode ter funkcionalno zemljišče objekta;

[17] Dostop do sistema ključar je mogoč z vpisom varnostne kode.
[18] List papirja formata A4 se razreže na 5.198 kosov.
[19] V prostore se vstopa oziroma izstopa s pomočjo elektronske kartice. Vsi vstopi in izstopi so evidentirani (ime in priimek, datum in čas).

- tehnična naprava sistema mora biti nameščena v varnostnem ali upravnem območju;
- posnetki videonadzora se hranijo najmanj 60 dni in
- gostota posnetkov mora znašati en posnetek na sekundo, kakovost pa mora biti najmanj formata SVHS.

Dostop to tehnične naprave sistema in do posnetkov imajo lahko le pristojne osebe.

Prostori organa se lahko opremijo s sistemom samodejnega zaznavanja gibanja oseb standarda SIST EN 50131 (razred 3). Alarmni signal standarda SIST EN 50136 (razred M 4) se mora prenašati po nadzorovani naročniški liniji od nastanka do prikaza alarma v varnostno-nadzornem centru, čas zaznave napake pa mora ustrezati standardu SIST EN 50136 (razred T 5).

2.4.2 Varnostnotehnična oprema upravnega območja

Vhod v upravno območje je lahko opremljen s protivlomnimi vrati s tritočkovnim zapiranjem standarda SIST EN 1627 (stopnja 2), ki imajo na zunanjem delu slepo kljuko in protivlomno zaščito. Vrata morajo imeti vgrajen cilindrični vložek za ključavnico standarda SIST EN 1303 (stopnja mehanske odpornosti 2), na notranji strani pa mora biti vgrajeno samodejno zapiralo, ki omogoča zapiranje vrat za vsakim odpiranjem.

V kolikor se v upravno območje namešča sistem za samodejno zaznavanje gibanja oseb, mora ustrezati standardu SIST EN 50131 (razred 2). Alarmni signal se mora prenašati po nadzorovani naročniški liniji od nastanka do prikaza alarma v varnostno-nadzornem centru s časom prenosa standarda SIST EN 50136 (razred M 3). Omogočena mora biti preverka zaznave napake med naročniškim modulom in nadzornim centrom standarda SIST EN 50136 (razred T4).

2.5 UREDBA O VAROVANJU TAJNIH PODATKOV V KOMUNIKACIJSKO INFORMACIJSKIH SISTEMIH

Z Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 48/2007) so določeni fizični, organizacijski in tehnični ukrepi ter postopki varovanja tajnih podatkov v komunikacijskih in informacijskih sistemih, ki jih morajo upoštevati in izvajati organi. Pri varovanju tajnih podatkov drugih držav ali mednarodnih organizacij v komunikacijskih in informacijskih sistemih se poleg ali namesto ukrepov, predpisanih z uredbo, izvajajo tudi drugi ukrepi, določeni z mednarodno pogodbo ali sprejetimi mednarodnimi obveznostmi (UVTPKIS, 1. člen).

S sistemom fizičnih, organizacijskih in tehničnih ukrepov se načrtno varuje tajne podatke v komunikacijskih in informacijskih sistemih organov pred nepooblaščenimi osebami, hkrati pa se zagotovi celovitost in razpoložljivost tajnih podatkov. Problem nastane, če sisteme nadzorujejo politiki za svoje zasebne namene (Schneier in Banisar, 1997). Predstojnik organa je odgovoren za izvajanje ukrepov varovanja tajnih podatkov v posameznih sistemih, za vzpostavitev in vzdrževanje sistema pa mora imenovati upravljalca sistema.

Pred začetkom obdelave podatkov v komunikacijsko informacijskem sistemu mora predstojnik izdati sklep o potrditvi izvajanja vseh ukrepov za zagotovitev varnega delovanja sistema (varnostna odobritev sistema). V sistemu, kjer se obdelujejo tajni podatki stopnje tajnosti ZAUPNO ali višje, mora predstojnik pred izdajo sklepa pridobiti od nacionalnega varnostnega organa mnenje o ustreznosti sistema. Pri vsakem posegu v sistem ali pri spremembi sistema mora upravljalec ponovno uvesti postopek varnostne odobritve sistema.

Nacionalni varnostni organ izda mnenje o sistemu, ko prejme od organa naslednje dokumente, ki jih izdela upravljalec sistema (UVTPKIS, 5. člen):

- načrt varovanja sistema z opisom in načrtom sistema, varnostnimi zahtevami sistema, varnostnimi okolji, varnostnimi protiukrepi in varnostnim upravljanjem sistema;
- oceno varnostnih tveganj z oceno stanja sistema in z oceno stopnje tveganja in
- varnostna navodila za delo v sistemu z varnostnim upravljanjem in organiziranostjo varnosti sistema, informacijsko varnostjo, načrtovanjem ukrepov ob nepredvidenih dogodkih, upravljanjem in spreminjanjem nastavitve sistema, splošnimi varnostnimi navodili za uporabnike in odgovorne osebe.

Upravljalec sistema mora dokumente stalno dopolnjevati, enkrat letno pa preveriti ustreznost ukrepov.

Posamezni sistem lahko deluje (UVTPKIS, 6. člen):

- neselektivno (v njem se obdelujejo tajni podatki za ožje število interesno povezanih uporabnikov z dovoljenjem za dostop do tajnih podatkov STROGO TAJNO in s pravico vpogleda v vse tajne podatke),[20]
- selektivno (v njem se obdelujejo tajni podatki različnih stopenj tajnosti in je namenjen osebam z dovoljenjem za dostop do tajnih podatkov STROGO TAJNO s pravico selektivnega vpogleda v tajne podatke na podlagi različnih potreb do vedenja),
- dvojno selektivno (v njem se obdelujejo tajni podatki različnih stopenj tajnosti in je namenjen osebam z dovoljenjem za dostop do tajnih podatkov različnih

[20] Pravico dostopa v sistem ima upravljalec sistema, vodja informacijske varnosti, vodja organa in osebe, katere pooblasti vodja organa. Vse osebe morajo imeti dovoljenje za dostop do tajnih podatkov najvišje stopnje tajnosti.

stopenj tajnosti s pravico selektivnega vpogleda v tajne podatke na podlagi različnih potreb do vedenja).

Selektivni pristop k sistemu in selektivni dostop do podatkov se rešujeta s pomočjo strojne in programske opreme. Upravljalec sistema mora za vsak svoj sistem pisno opredeliti varnostni način delovanja.

2.5.1 Fizični in organizacijski ukrepi varovanja

Ključni deli sistema, v katerem se obdelujejo tajni podatki stopnje tajnosti ZAUPNO in višje stopnje v nešifrirani obliki, morajo biti nameščeni v varnostno območje, ključni deli pa morajo biti ustrezno označeni s stopnjo tajnosti (UVTPKIS, 7. člen). Na določenih delih sistema se tajni podatki lahko obravnavajo izven varnostnega območja, če je prostor fizično ali tehnično varovan in je nepooblaščenim osebam onemogočen dostop.

V prostor s ključnimi deli sistema lahko samostojno vstopajo osebe z dovoljenjem za dostop do tajnih podatkov ustrezne stopnje tajnosti glede na dele sistema na podlagi pooblastila predstojnika organa, ki je lahko v obliki seznama, zaradi opravljanja delovnih nalog (vzdrževanje, dograjevanje delov sistema ipd.). Upravljalec sistema mora seznam teh oseb izobesiti na vidnem mestu prostora.

Za izvajanje fizičnih, organizacijskih in tehničnih ukrepov varovanja tajnih podatkov v komunikacijskih in informacijskih sistemih predstojnik organa določi vodjo informacijske varnosti in ji podeli ustrezna pisna pooblastila. Če sistem vsebuje dislocirane enote, lahko predstojnik organa določi lokalnega vodjo informacijske varnosti (oseba, ki je odgovorna za informacijsko varnost dislocirane enote sistema). Naloge vodje informacijske varnosti oziroma lokalnega vodje informacijske varnosti lahko opravlja tudi predstojnik organa oziroma predstojnik dislocirane enote.

V kolikor pride v sistemu do kritičnega dogodka, mora vodja informacijske varnosti obvestiti nacionalni varnostni organ o sprejetih ukrepih za primer kritičnega dogodka.

2.5.2 Tehnični ukrepi in postopki varovanja

Za vse uporabnike sistema mora upravljalec sistema izdelati postopke identifikacije in overitve dostopa v sistem, uporabniki pa morajo biti o tem seznanjeni. Postopke identifikacije in overitev dostopa uporabnikov v sistem določi komisija za informacijsko varnost, ki jo ustanovi Vlada Republike Slovenije.

Uporabniku sistema je dostop omejen na tiste tajne podatke, ki jih potrebuje za opravljanje svojih nalog. Upravljalec sistema izdela varnostno shemo, iz katere so razvidni identifikacijski podatki uporabnika in njegove pravice do posameznih tajnih

podatkov. Varnostno shemo upravljalec sistema sproti popravlja, v kolikor pride do spremembe na delovnih mestih in do spremembe potrebe po vedenju uporabnikov sistema.

Dostop uporabnikov do tajnih podatkov od stopnje tajnosti ZAUPNO ali višje v sistemu mora omogočati nadzor nad vstopi v sistem (UVTPKIS, 13. člen):[21]

- kdo je stopil v sistem,
- kdaj je kdo stopil v sistem,
- od kod je bilo vstopljeno v sistem in
- kdaj so bili tajni podatki obravnavani.

Način nadzora in spremljanje posegov v sistem mora upravljalec sistema pisno opredeliti, vse posege v sistem pa mora dokumentirati.

Tajni podatki se zunaj varnostnega in upravnega območja prenašajo po komunikacijskih in informacijskih sistemih in v pomnilnih medijih le v šifrirani obliki,[22] katere rešitve potrdi komisija za informacijsko varnost.

Tajni podatki stopnje tajnosti do vključno TAJNO se lahko izjemoma prenašajo v nešifrirani obliki z dovoljenjem predstojnika organa ali pooblaščene osebe v naslednjih izrednih okoliščinah (UVTPKIS, 14. člen):

- preteče ali dejanske krize, spopad ali vojne razmere in
- kadar je hitrost dostave bistvenega pomena in pri tem niso na voljo sredstva in metode za šifrirno zaščito ter se ocenjuje, da je možnost zlorabe poslanih tajnih podatkov zelo majhna.

Komunikacijsko informacijski sistemi se med seboj lahko povezujejo po nadzorovanih in varovanih vstopno-izstopnih točkah, skozi katere potekajo vsi servisi in storitve, če se s tem strinjajo upravljalci sistemov in če se izvedejo z navodili komisije za informacijsko varnost.

Če se v sistemih obdelujejo tajni podatki stopnje tajnosti ZAUPNO ali višje, morajo biti vsi deli sistema zaščiteni proti neželenemu elektromagnetnemu sevanju, ki lahko povzroči nekontrolirano odtekanje tajnih podatkov. Zaščito proti neželenemu elektromagnetnemu sevanju morajo zagotoviti upravljalci sistemov in mora biti del načrta varovanja. Meritve proti neželenemu elektromagnetnemu sevanju opravljajo pristojni organi.

[21] Nadzor nad vstopi v sistem poveča sledljivost tajnih podatkov.
[22] Šifriranje (kodiranje) tajnega podatka pomeni spremembo podatka s kriptografskimi postopki v neberljiv podatek, ki se ga lahko za branje odšifrira.

2.6 SKLEP O USTANOVITVI, NALOGAH IN ORGANIZACIJI URADA VLADE REPUBLIKE SLOVENIJE ZA VAROVANJE TAJNIH PODATKOV

Naloge nacionalnega varnostnega organa opravlja Urad Vlade Republike Slovenije za varovanje tajnih podatkov, ki je bil ustanovljen leta 2002 na podlagi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Uradni list RS, št. 6/2002).

Urad je vladna služba in opravlja naslednje naloge s področja tajnih podatkov (SUNOUVRSVTP, 2. člen):

- Spremlja stanje na področju določanja in varovanja tajnih podatkov preko poročil, ki so jih na njegovo zahtevo dolžni predložiti posamezni državni organi, organi lokalnih skupnosti, nosilci javnih pooblastil ter gospodarske družbe in organizacije, ki pridobijo ali razpolagajo s tajnimi podatki.
- Predlaga Vladi Republike Slovenije v sprejem standarde za fizično, organizacijsko in tehnično varovanje tajnih podatkov. Pri pripravi standardov za varstvo tajnih podatkov sodeluje z drugimi organi, še zlasti z Generalno policijsko upravo in Slovensko obveščevalno-varnostno agencijo. Pri pripravi standardov za varstvo tajnih podatkov pri elektronskem poslovanju urad sodeluje z Ministrstvom za visoko šolstvo, znanost in tehnologijo Republike Slovenije.
- Sodeluje z ustreznimi organi Evropske unije, zveze NATO in organi drugih mednarodnih organizacij in držav ter skrbi za izvrševanje sprejetih mednarodnih obveznosti in mednarodnih pogodb o varovanju podatkov. Če vlada za posamezne primere ne določi drugače, je urad dolžan voditi ažuren pregled in nadzor nad distribucijo tajnih podatkov mednarodnih organizacij in držav.
- Za vlado in ministrstva pripravlja predloge predpisov, ki se nanašajo na varovanje tajnih podatkov.
- Daje mnenje o skladnosti splošnih aktov o določanju, varovanju in dostopu do tajnih podatkov z zakonom. Posamezni organi so dolžni osnutek splošnega akta predložiti uradu v pregled pred njegovim sprejemom. Če urad ne poda mnenja v 14 dneh od prejema predloga, se šteje, da na predlog akta nima pripomb.
- Za posamezne vrste splošnih aktov organov lahko urad izdaja priporočila, vzorčne akte itd.
- Koordinira delovanje državnih organov, pristojnih za varnostno preverjanje v skladu z Uredbo o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov.
- Vodi evidenco izdanih dovoljenj, ki vsebuje identifikacijske podatke imetnika dovoljenja (ime in priimek ter datum in kraj rojstva), organ pri katerem je imetnik zaposlen in stopnjo tajnosti podatkov, do katerih lahko dostopa.
- Urad je dolžan zagotoviti ustrezno varovanje podatkov iz navedene evidence.

- Za zaposlene v Slovenski obveščevalno-varnostni agenciji, Obveščevalno-varnostni službi Ministrstva za obrambo Republike Slovenije in v Upravi kriminalistične policije Generalne policijske uprave, ki opravljajo operativno delo izven prostorov organa, se ne sporoča identifikacijskih podatkov, če bi njihovo razkritje lahko povečalo nevarnost za njihovo zdravje ali življenje. V teh primerih se navede samo podatek o zasedbi delovnega mesta ter o stopnji tajnosti podatkov, do katerih oseba lahko dostopa.
- Navedene podatke in njihove spremembe so uradu dolžni tekoče sporočati državni organi in službe, ki so pristojne za varnostno preverjanje.
- Organom predlaga ukrepe za izboljšanje varovanja tajnih podatkov, jim svetuje, organizira izobraževanja in odgovarja na strokovna vprašanja s področja varovanja tajnih podatkov.
- V skladu s predpisi, sklepi vlade in navodili generalnega sekretarja vlade opravlja druge naloge s področja varovanja tajnih podatkov.

2.7 UREDBA O NOTRANJEM NADZORU NAD IZVAJANJEM ZAKONA O TAJNIH PODATKIH IN PREDPISOV, IZDANIH NA NJEGOVI PODLAGI

Z Uredbo o notranjem nadzoru nad izvajanjem Zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi (Uradni list RS, št. 106/2002), so določeni oblika, način in vsebina izvajanja notranjega nadzora nad izvajanjem Zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi (UNNIZTPPINP, 1. člen).

Notranji nadzor na področju varovanja tajnih podatkov se opravlja v obliki (UNNIZTPPINP, 2., 3. in 4. člen):

- splošnega nadzora (preverijo se vse dejavnosti organa v zvezi s spoštovanjem predpisov s področja tajnih podatkov) in
- tematskega nadzora (preverijo se posamezne dejavnosti organa, ki se nanašajo na spoštovanje predpisov s področja tajnih podatkov).

Preverjanje utemeljenosti določitve tajnosti in stopnje tajnosti z vsebino tajnega dokumenta se sme preverjati le posamično s tematskimi nadzori (Lunežnik, 2004, str. 26).

Notranji nadzor opravljajo pooblaščene osebe organa z dovoljenjem za dostop do tajnih podatkov, za manjše organe pa lahko na podlagi dogovora med organi nadzor opravi določena služba organa. Notranji nadzor se lahko opravlja napovedano ali nenapovedano na podlagi letnega načrta organa ali na zahtevo predstojnika organa.

Z notranjim nadzorom se preverja (UNNIZTPPINP, 8. člen):

- ustreznost načrtov varovanja;
- ustreznost tehničnih, fizičnih in organizacijskih ukrepov za varovanje tajnih podatkov;
- ustreznost obdelave tajnih podatkov;
- ali imajo prejemniki tajnih podatkov ustrezno dovoljenje za dostop do tajnih podatkov in potrebo po vedenju;
- ali se izvaja osnovno in dodatno usposabljanje za obravnavo in varovanje tajnih podatkov;
- vodenje evidenc o izdanih dovoljenih za dostop do tajnih podatkov in o preklicih dovoljenj in
- vodenje posebnega dela kadrovske evidence.

Če so bile pri nadzoru ugotovljene nepravilnosti, se pristojni osebi oziroma notranji organizacijski enoti organa predlaga ukrepe in postavi rok za odpravo nepravilnosti. Po preteku roka lahko pooblaščena oseba opravi preverjanje odprave pomanjkljivosti. Pooblaščena oseba o tem sestavi poročilo, na katerega lahko nadzorovanec poda pripombe v 15 dneh. Pooblaščena oseba nato izda končno poročilo z morebitnimi pripombami nadzorovanca.

2.8 UREDBA O IZVAJANJU INŠPEKCIJSKEGA NADZORA NA PODROČJU VAROVANJA TAJNIH PODATKOV IN VSEBINI POSEBNEGA DELA STROKOVNEGA IZPITA ZA INŠPEKTORJA

Na področju varovanja in obdelave tajnih podatkov je z Uredbo o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja (Uradni list RS, št. 94/2006) predpisan inšpekcijski nadzor in vsebina izpita za inšpektorja (UIINPVTPVPDSII, 1. člen).

Inšpekcijski nadzor nad izvrševanjem predpisov s področja tajnih podatkov Republike Slovenije in tujih tajnih podatkov opravlja Inšpektorat Republike Slovenije za notranje zadeve, na obrambnem področju pa Inšpektorat Republike Slovenije za obrambo.

Glavni inšpektor na svojem področju vodi inšpektorat, organizira in koordinira delo inšpektorjev in odgovarja za delo inšpekcije.

Uredba določa naslednje vrste inšpekcij, ki so lahko napovedane ali pa nenapovedane (UIINPVTPVPDSII, 5. člen):

- redne inšpekcije se opravljajo v okviru letnih načrtov dela inšpektorata;
- izredne inšpekcije predlaga Vlada Republike Slovenije ali glavni inšpektor;
- izredne inšpekcije se lahko opravijo na podlagi prijav, pritožb in sporočil fizičnih in pravnih oseb;

- ponovne inšpekcije se opravijo z namenom preveritve odpravljenih pomanjkljivosti, ki jih je ugotovil inšpektor (o izvedbi ponovnih inšpekcij odloči glavni inšpektor na predlog pristojnega inšpektorja).

Inšpekcije lahko opravljajo posamezni inšpektorji ali pa skupina inšpektorjev, kjer vodja skupine usklajuje delo inšpektorjev med opravljanjem inšpekcije in izdaja pravne akte (zapisniki, odločbe ipd.).

Inšpektorji se morajo pred inšpekcijo ustrezno pripraviti, kar obsega (UIINPVTPVPDSII, 8. člen):

- preučitev pravnih predpisov;
- preučitev relevantnih podatkov o zavezani stranki;
- izdelavo opomnika za izvedbo inšpekcije in
- pripravo vadbenih dokumentov (na primer vprašalniki).

V primeru, ko opravlja inšpekcijo skupina inšpektorjev, mora vodja skupine organizirati in uskladiti delo inšpektorjev.

Če je inšpekcija napovedana, mora biti o tem obveščena zavezana stranka, ki zagotovi pogoje za nemoteno opravljanje inšpekcije. Smiselno se ravna v primeru vaje, ki jo odredi glavni inšpektor.

Inšpektorji samostojno vodijo postopek inšpekcije in izdajajo pravne akte v skladu z zakonom, ki ureja inšpekcijski nadzor, in zakonom, ki ureja splošni upravni postopek. Inšpektorji v svojih aktih ne smejo razkriti tajnega podatka.

Inšpektorji morajo opraviti strokovni izpit po predpisanem programu, ki obsega poznavanje predpisov s področja tajnih podatkov Republike Slovenije in tujih tajnih podatkov, za katere varovanje in obdelavo se je Republika Slovenija zavezala z mednarodnimi pogodbami.

V mnogih primerih je preventivni nadzor enostavnejši in manj tvegan; tisti, ki nadzira, se navadno ne bo odločil za sankcijo ali kakšen drug ukrep zoper nadziranca (Gostič, 2006, str. 13).

3 PRAVNI PREDPISI EVROPSKE UNIJE O TAJNIH PODATKIH

Z vstopom Republike Slovenije v Evropsko unijo leta 2004 je Republika Slovenija izgubila del pravne suverenosti, sprejela pravo Evropske unije in sprejela naslednja načela:

- načelo neposredne uporabnosti (pravni predpisi Evropske unije se v Republiki Sloveniji uporabljajo neposredno brez posredovanja organov v notranjem pravnem redu države);
- načelo primarnosti ali načelo supremacije (pravni predpisi Evropske unije prevladajo nad vsemi pravnimi predpisi v Republiki Sloveniji, tudi nad Ustavo Republike Slovenije) in
- načelo avtonomnosti prava (pravni red Evropske unije je neodvisen od pravnega reda Republike Slovenije in ga v Republiki Sloveniji ni mogoče spreminjati ali kako drugače interpretirati).

Evropska unija je torej naddržavna tvorba, je več kakor navadna mednarodna organizacija, pa vendarle manj kakor federalna država (Grilc, 2001, str. 101).

Varnost in delo s tajnimi podatki Evropske unije določajo Predpisi Sveta Evropske unije o varovanju tajnosti (Uradni list ES, št. L 101/1/2001, L 63/48/2004, L 193/31/2005, L 346/18/2005 in L 164/24/2007) in Pravilnik Komisije o varnosti (Uradni list ES, št. L 317/1/2001, L 29/39/2005, L 31/66/2005, L 34/32/2006 in L 215/38/2006).

Države članice sprejmejo ukrepe na državni ravni, ki so potrebni za spoštovanje Predpisov Sveta Evropske unije o varovanju tajnosti, kadar njihovi pristojni organi in uradniki delajo s tajnimi podatki Evropske unije (PSEUVT, 4. točka preambule in 2. člen). V skladu s tema določiloma je bil v Republiki Sloveniji leta 2001 sprejet Zakon o tajnih podatkih.

"Svet pozdravlja namero Komisije, da bo zaradi nemotenega izvajanja postopka odločanja Unije do datuma začetka uporabe tega sklepa uvedla obširen sistem, ki bo usklajen s prilogami k sklepu. Svet poudarja pomen vključevanja, kadar je to ustrezno, Evropskega parlamenta in Komisije v pravila in standarde o zaupnosti, potrebne za varstvo interesov Unije in njenih držav članic." (PSEUVT, 5. in 6. točka preambule). Na podlagi teh določb je bil sprejet Pravilnik Komisije o varnosti.

3.1 PREDPISI SVETA EVROPSKE UNIJE O VAROVANJU TAJNOSTI

3.1.1 Temeljna načela in minimalni standardi varovanja tajnosti

Temeljna načela in minimalne standarde varovanja tajnosti morajo spoštovati Svet Evropske unije, Generalni sekretariat Sveta, države članice in decentralizirane agencije Evropske unije.

Tajni podatek Evropske unije (v nadaljevanju tajni podatek EU) je vsak podatek in gradivo (na primer zemljevid, zgoščenka ipd.), katerega razkritje nepooblaščeni osebi bi lahko škodovalo interesom Evropske unije ali eni ali več državam članicam, če imajo taki podatki svoj izvor bodisi znotraj Evropske unije ali pa prihajajo iz držav članic, tretjih držav ali mednarodnih organizacij.

Glavni cilji varovanja tajnosti so varovati tajne podatke EU pred dostopom nepooblaščenih oseb, tajne podatke v komunikacijskih in informacijskih sistemih, objekte, v katerih se nahajajo tajni podatki, in v primeru napake oceniti in preprečiti nadaljnjo škodo.

Osebe, ki potrebujejo dostop do tajnih podatkov stopnje tajnosti CONFIDENTIEL UE ali višje stopnje, morajo biti varnostno preverjene. Posebno natančno morajo biti varnostno preverjene osebe, ki bodo prejemale večje število tajnih podatkov stopnje tajnosti SECRET UE in ki bodo prejemale tajne podatke stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET.

Če se izkaže, da oseba, ki obdeluje tajne podatke, predstavlja tveganje za varnost, se ji prepreči ali pa odstrani od izvajanja nalog, kjer bi lahko škodovala interesom varnosti, o tem pa se obvesti pristojni organ.

Ukrepi varovanja tajnosti zagotavljajo, da pridobijo tajne podatke osebe na podlagi načela potrebe po seznanitvi s podatki (potreba po vedenju)[23] zaradi opravljanja funkcije ali delovnih nalog, ki je temeljno načelo za vse vidike v zvezi z varovanjem tajnosti. Tajne podatke zveze Nato lahko pridobijo osebe z dovoljenjem za dostop do tajnih podatkov in s potrebo po vedenju (Nato, 2005). Pri razvrščanju tajnih podatkov po stopnji tajnosti se je potrebno izogniti previsoki ali prenizki stopnji tajnosti. Za zaščito tajnih podatkov v izrednih razmerah je potrebno pripraviti načrte zaščite podatkov, za zaščito tajnih podatkov, ki se obdelujejo ali hranijo s pomočjo komunikacijskih in informacijskih sistemov, pa je potrebno sprejeti protiukrepe za preprečevanje dostopa nepooblaščenim osebam (INFOSEC).[24] Zaradi silovitega razvoja informatike v osemdesetih je bila varnostna politika dopolnjena z informacijsko

[23] Angl. need to know.
[24] INFOSEC je kratica za informacijsko varnost.

varnostjo (Antončič, 2001, str. 20). Fizični ukrepi za zaščito pomembnih objektov, v katerih so tajni podatki, predstavljajo najboljšo zaščito pred morebitnim vohunjenjem ali naklepno uničevalno dejavnostjo; samo varnostno preverjanje osebja še ne pomeni učinkovitega nadomestila.[25]

3.1.2 Organiziranost varovanja tajnosti v Svetu Evropske unije

Generalni sekretar Sveta Evropske unije izvaja varnostno politiko Sveta in jo v povezavi z nacionalnimi varnostnimi organi usklajuje. Države članice morajo ustanoviti centralni arhivski urad na stopnji TRÈS SECRET UE/EU TOP SECRET na zahtevo generalnega sekretarja (naloge centralnega arhivskega urada opravlja v Republiki Sloveniji centralni register za tajne podatke EU v okviru Službe za tajne podatke Ministrstva za zunanje zadeve Republike Slovenije).

Nacionalni varnostni organ (Urad Vlade Republike Slovenije za varovanje tajnih podatkov) je pristojen za varovanje tajnih podatkov EU, za akreditacijo arhivskih uradov na stopnji TRÈS SECRET UE/EU TOP SECRET (centralni register in podregistri za tajne podatke EU), za opravljanje inšpekcijskih nadzorov skupaj z Varnostnim uradom Generalnega sekretariata Sveta Evropske unije), za varnostno preverjanje oseb in izdajo dovoljenj za tajne podatke EU ter za oblikovanje načrtov varovanja.

3.1.3 Razvrščanje in označevanje tajnih podatkov

Tajni podatki EU so razvrščeni po naslednjih stopnjah tajnosti (PSVT, 1., 2., 3. in 4. odstavek, oddelek II):

- TRÈS SECRET UE/EU TOP SECRET (stopnja tajnosti se uporablja samo za podatke in gradivo, katerih razkritje nepooblaščeni osebi bi lahko imelo izjemno težke posledice za bistvene interese Evropske unije ali ene ali več njenih držav članic);
- SECRET UE (stopnja tajnosti se uporablja samo za podatke in gradivo, katerih razkritje nepooblaščeni osebi bi lahko resno škodovalo bistvenim interesom Evropske unije ali ene ali več njenih držav članic);
- CONFIDENTIEL UE (stopnja tajnosti se uporablja za podatke in gradivo, katerih razkritje nepooblaščeni osebi bi lahko škodovalo bistvenim interesom Evropske unije ali ene ali več njenih držav članic) in
- RESTREINT UE (stopnja tajnosti se uporablja za podatke in gradivo, katerih razkritje nepooblaščeni osebi bi lahko bilo škodljivo za interese Evropske unije ali ene ali več njenih držav članic).

[25] S tem določilom bi se strokovnjaki s področja varnostno-obveščevalnih služb težko strinjali, saj je človek bolj ranljiv v smislu odtekanja informacij kot pa fizični ukrepi za zaščito objektov.

V kolikor podatki in gradivo ni namenjeno javni objavi, se označi z oznako LIMITE, ki ne predstavlja stopnje tajnosti.[26]

3.1.4 Sistem razvrščanja tajnih podatkov po stopnjah tajnosti

Stopnja tajnosti podatkov se določi samo, če je to potrebno. Stopnja tajnosti podatkov se določi glede na stopnjo občutljivosti njihove vsebine na jasen in pravilen način in se zadrži samo tako dolgo, kot je potrebno za zaščito podatkov. Visoka stopnja tajnosti zagotavlja boljšo zaščito dokumenta, vendar lahko rutinsko določanje previsokih stopenj povzroči izgubo zaupanja v vrednost sistema razvrščanja. Po drugi strani pa dokumenti zaradi varnosti podatkov ne smejo imeti prenizke stopnje tajnosti.

Tajnim podatkom EU se lahko zniža ali prekliče stopnja tajnosti le z dovoljenjem izdajatelja tajnega podatka, izdajatelj pa je o tem dolžan obvestiti vse prejemnike tajnih podatkov. Če je mogoče, izdajatelji na podatkih določijo datum ali obdobje, ko je stopnjo tajnosti vsebine mogoče znižati ali preklicati. V nasprotnem primeru izdajatelji tajne podatke preverjajo v roku petih let.

3.1.5 Fizično varovanje tajnosti

Z ukrepi fizičnega varovanja tajnosti se prepreči nepooblaščenim osebam dostop do tajnih podatkov in gradiva Evropske unije v prostorih zgradb in v komunikacijskih in informacijskih sistemih.

V območjih, kjer se obdelujejo in shranjujejo tajni podatki stopnje tajnosti CONFIDENTIEL UE ali višje stopnje, je potrebno vzpostaviti (PSVT, 5. odstavek, oddelek IV):

- varnostno območje I. stopnje (sam vstop v to območje pomeni seznanitev s tajnimi podatki; okolica varnostnega območja mora biti ustrezno zavarovana, vhodi in izhodi območja pa nadzorovani; s sistemom vhodnega nadzora se dovoli dostop v območje samo preverjenim in pooblaščenim osebam; v območju mora biti nameščen razvid (opis) tajnih podatkov, ki se nahajajo v območju);[27]
- varnostno območje II. stopnje (vstop v območje ne pomeni seznanitve s tajnimi podatki zaradi vzpostavljene zaščite s pomočjo notranjega nadzora; okolica varnostnega območja mora biti ustrezno zavarovana, vhodi in izhodi območja pa nadzorovani; s sistemom vhodnega nadzora se brez spremstva dovoli dostop v območje samo preverjenim in pooblaščenim osebam).

[26] Dokumente z oznako LIMITE se lahko obdeluje na enak način kot interne dokumente organa.
[27] V službah za tajne podatke v Republiki Sloveniji se je pojavljalo vprašanje, ali se razvid namesti znotraj ali izven varnostnega območja I. stopnje.

Po izteku delovnega časa je potrebno pregledati varnostna območja in zagotoviti, da je ustrezno poskrbljeno za varnost tajnih podatkov EU.

Ob varnostnem območju se lahko vzpostavi upravno območje z nižjo stopnjo varovanja, kjer se obdelujejo in hranijo tajni podatki stopnje tajnosti RESTREINT UE.

Tajni podatki EU stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET se hranijo v vsebnikih tipa A, stopnje tajnosti SECRET UE in CONFIDENTIEL EU v vsebnikih tipa B, stopnje tajnosti RESTREINT EU pa v vsebnikih tipa C (pisarniško pohištvo). Enaki tipi veljajo za ključavnice vsebnikov. Blagajne in ključavnice odobri na nacionalni ravni nacionalni varnostni organ. Delovni ključi, nadomestni varnostni ključi in nastavitve kombinacij se hranijo v ločenih varnostnih vsebnikih. Ti ključi in nastavitve kombinacij morajo biti deležni enako stroge varnostne zaščite kakor gradivo, do katerega omogočajo dostop.

Ves čas se morajo izvajati vsi ustrezni ukrepi, ki zagotavljajo, da tajnih podatkov EU ne more videti (niti po naključju) nobena nepooblaščena oseba. Prostori ali območja, v katerih se pogosto razpravlja o tajnih podatkih stopnje tajnosti SECRET UE ali višje, se v primerih tveganja zaščitijo pred pasivnimi ali aktivnimi poskusi prisluškovanja.

3.1.6 Splošna pravila o načelu potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog in varnostno preverjanje

Dostop do tajnih podatkov EU se dovoli samo osebam, za katere zaradi opravljanja dela velja načelo potrebe po seznanitvi s podatki (potreba po vedenju).[28] Dostop do tajnih podatkov stopenj TRÈS SECRET UE/EU TOP SECRET, SECRET UE in CONFIDENTIEL UE se dovoli samo osebam, ki imajo dovoljenje za dostop do tajnih podatkov, ki ga pridobijo po končanem postopku varnostnega preverjanja. Dovoljenje določa stopnjo tajnosti podatkov, do katerih ima lahko preverjena oseba dostop, in datum prenehanja veljavnosti potrdila.

Osebe, za katere se zahteva dostop do podatkov tajnosti TRÈS SECRET UE/EU TOP SECRET, imenuje pristojna oseba, njihova imena pa se hranijo v arhivskem uradu TRÈS SECRET UE/EU TOP SECRET. Osebe, ki imajo dostop do tajnih podatkov od stopnje tajnosti CONFIDENTIEL UE ali višje, se morajo seznaniti s predpisi s področja tajnih podatkov in se zavedati posledic neodgovornega ravnanja s tajnimi podatki v skladu z nacionalnim pravom in pravom Evropske unije; za stopnjo tajnosti TRÈS SECRET UE/EU TOP SECRET morajo osebe podpisati posebno varnostno potrdilo. Osebe z

[28] Angl. need to know.

dostopom do tajnih podatkov stopnje tajnosti RESTREINT UE se opozori na pomembnost teh predpisov in na posledice neodgovornega ravnanja.[29]

Če oseba zapusti delovno mesto ali se jo premesti, na delovno mesto, kjer ne dela več s tajnimi podatki, mora arhivski urad uvesti postopek primopredaje tajnih podatkov.

3.1.7 Priprava, razpošiljanje, prenos, shranjevanje in uničevanje tajnega gradiva Evropske unije

Dokumente Evropske unije se označuje s stopnjo tajnosti zgoraj in spodaj na sredini vsake strani, vsaka stran pa mora biti oštevilčena. Dokument je opremljen s številko in datumom. Pri dokumentih TRÈS SECRET UE/EU TOP SECRET in SECRET UE mora biti številka vidna na vsaki strani. Kopije dokumentov morajo imeti na prvi strani oznako številke kopije skupaj s celotnim številom strani. Na prvi strani dokumenta stopnje tajnosti CONFIDENTIEL UE in višje mora biti naveden seznam vseh dodatkov in prilog.

Tajni podatki EU se razpošiljajo samo osebam, ki imajo potrebo po vedenju zaradi opravljanja dela in ki imajo dovoljenje za dostop do tajnih podatkov. Prvo razpošiljanje določi organ izvora. Arhivski urad mora vsak tajni podatek stopnje tajnosti CONFIDENTIEL UE ali višje ob prihodu ali izhodu iz urada vpisati v evidenco (v delovodnik ali pa v računalniški nosilec). Vpisati je potrebno reference, datum in po potrebi številko kopije, da je omogočena prepoznava dokumentov.

Tajni podatki stopnje tajnosti CONFIDENTIEL UE se prenašajo v odpornih in neprozornih dvojnih ovojnicah. Notranja ovojnica se označi s stopnjo tajnosti EU, z delovnim nazivom osebe in z naslovom naslovnika. Notranja ovojnica se lahko odpre le v arhivskem uradu. Notranja ovojnica vsebuje tudi potrdilo o prejemu s številko, datumom in kopijo dokumenta. Iz zunanje ovojnice ne sme biti razvidno, da vsebuje tajni podatek. Znotraj prostorov se tajni podatki prenašajo v zalepljenih ovojnicah, na katerih je ime naslovnika.

Prenos tajnih podatkov EU lahko poteka glede na stopnjo tajnosti na naslednje načine (PSVT, 13. in 16. odstavek, oddelek VII):

- TRÈS SECRET UE/EU TOP SECRET in SECRET UE (znotraj države prenaša tajne podatke kurirska služba ali osebe, ki imajo dostop do teh podatkov);
- SECRET UE in CONFIDENTIEL UE (znotraj države se podatke lahko pošilja po pošti, če to dovoljujejo nacionalni predpisi, s kurirsko službo ali s pomočjo oseb, ki imajo dovoljenje za dostop teh do tajnih podatkov).[30]

[29] Evropska unija ima zelo odprt sistem dela s tajnimi podatki RESTREINT UE v primerjavi z Republiko Slovenijo.
[30] V Republiki Sloveniji se lahko pošilja po pošti le tajne podatke stopnje tajnosti INTERNO.

Tajne podatke stopnje tajnosti CONFIDENTIEL UE ali višje iz ene države članice Evropske unije v drugo državo članico prenašajo diplomatske poštne ali vojaške kurirske službe. Prenos se lahko opravi tudi osebno za stopnje tajnosti SECRET UE in CONFIDENTIEL UE, če ima prenašalec ustrezno dovoljenje za dostop do tajnih podatkov, če je pošiljka zapečatena z uradno plombo in opremljena z uradnimi nalepkami, če ima prenašalec kurirsko pismo za prenos tajnih podatkov (priloga 1), če se pri prenosu po kopnem ne prečka nobena nečlanica Evropske unije in če prenašalec prebere in podpiše varnostna navodila. Država članica mora za osebni prenos pripraviti ustrezna navodila.

Pri prenosu tajnih podatkov stopnje tajnosti RESTREINT UE mora biti zagotovljeno, da ne pridejo v roke nepooblaščenim osebam.

Kurirji morajo imeti ustrezno dovoljenje za dostop do tajnih podatkov EU. Pri prenosu tajnih podatkov stopnje tajnosti RESTREINT UE ne potrebujejo dovoljenja.

Kopiranje tajnih podatkov stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET in SECRET UE dovoli le organ izvora, ostale stopnje tajnosti se pa lahko kopira pod pogojem strogega spoštovanja načela potrebe po vedenju zaradi opravljanja funkcije ali delovnih nalog.

Arhivski uradi TRÈS SECRET UE/EU TOP SECRET morajo enkrat na leto opraviti popis tajnih podatkov stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET, podatke nižje stopnje tajnosti pa se v skladu z nacionalnimi predpisi interno preverja zaradi morebitnih znižanj oziroma preklicev stopenj tajnosti ali njihovega uničenja.

Tajne podatke se lahko arhivira s snemanjem na mikrofilm ali shrani na magnetna ali optična sredstva zaradi preprečevanja prekomernega kopičenja tajnih podatkov. Izvirnike je po arhiviranju potrebno uničiti.

Tajne podatke EU se lahko tudi rutinsko uniči zaradi nepotrebnega kopičenja odvisno od stopnje tajnosti podatka (PSVT, 31., 32., 33. in 34. odstavek, oddelek VII):

- TRÈS SECRET UE/EU TOP SECRET (podatki se uničijo v centralnem arhivskem uradu TRÈS SECRET UE/EU TOP SECRET ob prisotnosti dveh pristojnih oseb; o tem se sestavi zapisnik);
- SECRET UE (podatki se uničijo v arhivskem uradu TRÈS SECRET UE/EU TOP SECRET ob prisotnosti ene pristojne osebe; o tem se sestavi zapisnik);
- CONFIDENTIEL UE (podatki se uničijo v arhivskem uradu ob prisotnosti ene pristojne osebe, o tem se sestavi poročilo v skladu z nacionalnimi predpisi);
- RESTREINT UE (podatke uniči arhivski urad ali uporabnik v skladu z nacionalnimi predpisi).[31]

[31] Tajne podatke Republike Slovenije vseh stopenj tajnosti komisijsko uniči tričlanska komisija.

3.1.8 Arhivski uradi TRÈS SECRET UE/EU TOP SECRET

Arhivski uradi TRÈS SECRET UE/EU TOP SECRET so pristojni za arhiviranje, rokovanje z dokumenti stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET in za njihovo razpošiljanje. Vodja arhivskega urada v vsaki državi članici je zadolžen za nadzor na stopnji TRÈS SECRET UE/EU TOP SECRET. Centralni arhivski uradi opravljajo funkcijo glavnega sprejemnega in odpremnega organa v državah članicah. Podarhivski uradi skrbijo za notranje upravljanje z dokumenti stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET.

Naloge centralnega arhivskega urada opravlja v Republiki Sloveniji Služba za tajne podatke Ministrstva za zunanje zadeve Republike Slovenije (centralni register za tajne podatke EU). Naloge podarhivskih uradov v Republiki Sloveniji opravljajta Službi za tajne podatke na Ministrstvu za obrambo Republike Slovenije in na Ministrstvu za notranje zadeve Republike Slovenije, v tujini pa jih opravlja Služba za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju.

3.1.9 Kršitve varovanja tajnosti in ogrožanje tajnih podatkov Evropske unije

Kršitve varnosti nastanejo kot posledica dejanja ali opustitve dejanja z neupoštevanjem pravnih predpisov s področja tajnih podatkov Sveta Evropske unije in držav članic, kar bi lahko ogrozilo ali izpostavilo nevarnosti tajne podatke EU.

Do ogrožanja tajnih podatkov EU pride, če do podatkov pridejo nepooblaščene osebe oziroma da obstaja verjetnost, da bi do tega prišlo (PSVT, 2. odstavek, oddelek X):

- če osebe nimajo dovoljenja za dostop do tajnih podatkov in
- če osebe, ki nimajo potrebe po vedenju zaradi opravljanja funkcije ali delovnih nalog.

Če se ugotovi kršitev varovanja tajnosti ali izguba tajnega podatka EU, mora biti o tem obveščen varnostni organ države članice, ki ugotovi dejstva in okoliščine, do katerih je prišlo, poskuša zmanjšati storjeno škodo z ustreznimi ukrepi in obvesti pristojne organe o posledicah kršitve varnosti.

Varnostni organ mora pridobiti naslednje podatke (PSVT, 5. odstavek, oddelek X):

- opis tajnega podatka s stopnjo tajnosti, številko in številko kopije, datumom, organom izvora, predmetom in razsežnostjo tajnega podatka;
- opis okoliščin, v katerih je prišlo do kršitve varnosti, vključno z datumom in obdobjem, v katerem je bil tajni podatek izpostavljen ogrožanju;
- izjavo o obveščenosti organa izvora.

Varnostni organ mora o dogodkih poročati podarhivskemu uradu, ki poroča preko centralnega arhivskega urada Varnostnemu uradu Generalnega sekretariata Sveta Evropske unije. Če je prišlo do dogodka na področju pristojnosti države članice, mora biti o tem obveščen Varnostni urad Generalnega sekretariata Sveta s strani nacionalnega varnostnega organa. Varnostni urad nadalje ukrepa v okviru svojih pristojnosti.

V zvezi s tajnimi podatki stopnje tajnosti RESTREINT UE je treba poročati le, če imajo neobičajne lastnosti.

Oseba, ki je odgovorna za ogrožanje tajnih podatkov EU, je disciplinsko odgovorna v skladu z ustreznimi pravili in predpisi.

3.1.10 Zaščita podatkov v sistemih informacijske tehnologije in v komunikacijskih sistemih

Komunikacijski in informacijski sistemi ter omrežja, v katerih se obdelujejo ali hranijo tajnih podatki EU, so izpostavljeni številnim varnostnim tveganjem (PSVT, 5. odstavek, oddelek XI):

- nepooblaščen dostop oseb,
- ponarejanje, spreminjanje in izbris tajnih podatkov in
- nezaželene operacije zbiranja podatkov in sabotaž.

Ukrepe varovanja tajnosti v sistemih določi organ za varnostno akreditacijo (Security Accreditation Authority – SAA) in so sorazmerni glede na ocenjeno tveganje ter skladni z določbami Predpisov Sveta o varovanju tajnosti. Za vse sisteme, v katerih se obdelujejo tajni podatki stopnje tajnosti CONFIDENTITEL UE ali višje, mora organ, ki je pristojen za delovanje sistema (IT System Operational Authority – ITSOA) v sodelovanju z organom INFOSEC (organ za informacijsko varnost) pripraviti izjavo o zahtevah za varovanje tajnosti v sistemu (SSRS – SYSTEM-Specific Security Requirement Statement), ki jo potrdi SAA (dodelitev akreditacije). Izjavo se lahko zahteva tudi za stopnjo tajnosti RESTREINT UE.

Sistemi se akreditirajo glede na naslednje načine delovanja (PSVT, 15., 16. in 17. odstavek, oddelek XI):

- dedicated (do sistema imajo dostop osebe z dovoljenjem za dostop do tajnih podatkov TRÈS SECRET UE/EU TOP SECRET in imajo pravico dostopa do vseh tajnih podatkov, ki se v sistemu obdelujejo),
- system high (do sistema imajo dostop osebe z dovoljenjem za dostop do tajnih podatkov TRÈS SECRET UE/EU TOP SECRET in imajo pravico dostopa do tistih tajnih podatkov, za katere imajo potrebo do vedenja zaradi opravljanja dela),

- multi-level (do sistema imajo dostop osebe brez dovoljenja za dostop do tajnih podatkov in imajo pravico dostopa do tistih tajnih podatkov, za katere imajo potrebo do vedenja zaradi opravljanja dela).[32]

Organ za varnostno akreditacijo (SAA) informacijsko-komunikacijskega sistema je lahko (PSVT, 35. odstavek, oddelek XI):

- nacionalni varnostni organ ali
- organ, ki ga določi generalni sekretar.

Sistemi in komponente sistemov, ki delujejo v državi članici, ostajajo v pristojnosti te države članice.

Uporabniki sistema morajo imeti dovoljenje za dostop do tajnih podatkov EU in morajo imeti potrebo po vedenju zaradi opravljanja dela. Sisteme se vzpostavlja na način, da nobena posamezna oseba ne more v celoti poznati sistema ali imeti nadzora nad njegovimi ključnimi varnostnimi točkami. Cilj tega je doseči, da nihče ne bi mogel povzročiti spremembe ali namerno poškodovati sistema ali omrežja brez sodelovanja ene ali več drugih oseb.

Za območja s programsko in strojno opremo, s katero se obdelujejo tajni podatki stopnje tajnosti CONFIDENTIEL UE ali višje s pomočjo informacijske tehnologije, se vzpostavijo varnostna območja I. ali II. stopnje.

Na območjih z informacijsko tehnologijo, kjer je mogoče vplivati na varnost sistema, se ne sme zadrževati en sam uslužbenec.

Evidenca dostopa do tajnih podatkov stopnje tajnosti SECRET UE in višje se vodi avtomatsko (kontrolni zapisi) ali z ročnimi vpisi v vpisnik. Evidenca se hrani v skladu s Predpisi Sveta o varovanju tajnosti. Kadar se pošiljajo tajni podatki iz sistema na oddaljen terminal, se za nadzor nad pošiljanjem na daljavo določijo postopki, ki jih odobri SAA. Pri podatkih stopnje tajnosti SECRET UE in višje taki postopki vsebujejo posebna navodila glede sledljivosti teh podatkov.

Tajni podatki EU do stopnje tajnosti SECRET UE se lahko prenašajo kot razvidno besedilo (brez kriptografskih metod) v izrednih razmerah pod pogojem, da je za vsak tak prenos izdano posebno dovoljenje (PSVT, 68. odstavek, oddelek XI):

- v času preteče ali dejanske krize, spopada ali vojnih razmer; in
- kadar je hitrost dostave bistvenega pomena ter sredstva za kriptografski zapis niso na voljo in se ocenjuje, da poslanih podatkov ni mogoče pravočasno uporabiti zaradi vplivanja na potek operacij.

[32] Velja za tajne podatke EU stopnje tajnosti RESTREINT UE.

Sistemi, ki obdelujejo tajne podatke stopnje tajnosti CONFIDENTIEL UE in višje, morajo biti zaščiteni proti neželenemu elektromagnetnemu sevanju, katerih preučevanje in nadzor sta določena kot "tempest".

Nova ali spremenjena verzija programske opreme se lahko uporablja za obdelavo tajnih podatkov EU, ko jo odobri ITSOA.

3.1.11 Sporočanje tajnih podatkov Evropske unije tretjim državam ali mednarodnim organizacijam

Tajne podatke EU se lahko distribuira tretjim državam ali mednarodnim organizacijam le z odločitvijo Sveta Evropske unije na podlagi (PSVT, 1. odstavek, oddelek XII):

- značaja in vsebine takih podatkov,
- prejemnikove potrebe po vedenju zaradi opravljanja dela,
- obsega ugodnosti za Evropsko unijo.

Če imajo tajni podatki EU izvor v državi članici, mora takšno posredovanje odobriti država članica.

Ko Svet Evropske unije sprejme odločitev, da se tajni podatki lahko distribuirajo ali izmenjujejo z določeno državo ali mednarodno organizacijo, sprejme tudi odločitev o ravni mogočega sodelovanja, kar je odvisno zlasti od varnostne politike in predpisov, ki jih uporablja zadevna država ali organizacija, in dogovor o postopkih varovanja tajnosti za izmenjavo tajnih podatkov, s katerim se določi namen sodelovanja in skupna pravila za zaščito tajnih podatkov.

Tajni podatki se lahko posredujejo tretji osebi (potreba po delitvi – angl. need to share), ki mora biti nujno seznanjena z vsebino tajnega podatka (Henigman, 2007, str. 177).

3.1.12 Primerjava nacionalnih oznak stopenj tajnosti

Stopnje tajnosti tajnih podatkov EU in držav članic so si medsebojno ekvivalentne, kot je prikazano za del držav članic v tabeli 1.

Tabela 1: Primerjava oznak stopenj tajnosti

Stopnja tajnosti EU	Très secret UE/EU top secret	Secret UE	Confidentiel UE	Restreint UE
Francija	très secret défense	secret défense	confidentiel défense	néant[33]
Italija	segretissimo	segreto	riservatissimo	riservato
Nemčija	streng geheim	geheim	VS – Vertraulich	VS – nur für den Dienstgebrauch
Slovenija	strogo tajno	tajno	zaupno	interno
Španija	secreto	reservado	confidencial	difusión limitada
Združeno kraljestvo	top secret	secret	confidential	restricted

Vir: PSVT (dodatek 2)

3.2 PRAVILNIK KOMISIJE O VARNOSTI

Tako Predpisi Sveta Evropske unije o varovanju tajnosti kot tudi Pravilnik Komisije o varnosti so se pričeli uporabljati s 1. decembrom 2001.

Varnostni sistem Komisije temelji na načelih, ki so določena s Predpisi Sveta Evropske unije o varovanju tajnosti, da bi se zagotovilo nemoteno sprejemanje odločitev v Evropski uniji (PKV, 4. odstavek preambule), saj so bili Predpisi Sveta Evropske unije o varovanju tajnosti sprejeti pred Pravilnikom Komisije o varnosti.

Določbe Pravilnika komisije o varnosti so praktično identične določbam Predpisov Sveta Evropske unije o varovanju tajnosti zaradi zagotovitve enotnega obdelovanja in hrambe tajnih podatkov EU, s tem da Pravilnik Komisije o varnosti vsebuje določbe o osebah in organih Komisije, ki imajo podobne funkcije kot osebe in organi Sveta.

Osebe in organi Komisije, ki so pristojni za delo s tajnimi podatki so (PKV, 11., 12., 13., 14., 25.3.2 in 25.3.3 točka):

- član Komisije, pristojen za varnostne zadeve,
- svetovalna skupina za varnostno politiko Komisije,
- Varnostni odbor Komisije,
- Varnostni urad Komisije,
- organ za akreditacijo varnosti (SAA) in
- organ INFOSEC.

[33] Francija ravna z dokumenti stopnje tajnosti RESTREINT UE v skladu z nacionalnimi predpisi.

4 PRIMERJAVA PRAVNIH PREDPISOV REPUBLIKE SLOVENIJE IN EVROPSKE UNIJE O TAJNIH PODATKIH

Eden izmed razlogov za sprejem Zakona o tajnih podatkih leta 2001 so Predpisi Sveta Evropske unije o varovanju tajnosti (v nadaljevanju Predpisi Sveta). Države članice sprejmejo ukrepe na državni ravni, ki so potrebni za spoštovanje Predpisov Sveta, kadar njihovi pristojni organi in uradniki delajo s tajnimi podatki EU (PSVT, 4. točka preambule in 4. člen).

Nacionalni predpisi (zakoni in podzakonski predpisi) s področja tajnih podatkov so v primerjavi s pravnimi predpisi Evropske unije bolj strogi, kar se tiče dela s tajnimi podatki. V času predsedovanja Republike Slovenije Svetu Evropske unije je bil potreben hiter pretok tajnih podatkov med Stalnim predstavništvom Republike Slovenije pri Evropski uniji v Bruslju in Ministrstvom za zunanje zadeve Republike Slovenije ter med zaposlenimi na stalnem predstavništvu, kar pa je bilo težko doseči zaradi strogih in neživljenjskih nacionalnih predpisov.

Pravico dostopa do tajnih podatkov ima oseba, ki ima dovoljenje za dostop do tajnih podatkov in ki se mora s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog (ZTP, 31. člen). Navedena zakonska dikcija pomeni, da imajo zaposlene osebe z dovoljenjem za dostop do tajnih podatkov pravico dostopa do vseh tajnih podatkov zaradi opravljanja nalog na delovnem mestu. Predpisi Sveta določajo, da morajo imeti osebe tudi potrebo do vedenja (PSVT, 7. točka, del I). Načelo potrebe do vedenja (angl. need to know) je temeljno načelo za vse vidike varovanja tajnosti in se ga obravnava ožje kot opravljanje funkcije ali delovnih nalog. V praksi to pomeni, da zaposleni na določenem delovnem področju nima splošne pravice dostopa do vseh tajnih podatkov s tega področja. V Republiki Sloveniji zaradi tega prihaja do prekomernega razmnoževanja tajnih podatkov. Nastanek tajnega podatka z različnimi temami in njegova distribucija (na primer izdaja brošure s poglavji, ki vsebujejo različne teme, brošuro pa naj bi prejele vse osebe, ki opravljajo delo v zvezi z enim samim poglavjem) pomeni prav tako kršitev načela potrebe po vedenju. Za pravico dostopa do tajnih podatkov zveze Nato morajo osebe prav tako imeti dovoljenje za dostop do tajnih podatkov in potrebo po vedenju (Antončič, 2001, str. 17).

V obveščevalnih strukturah Evropske unije se v okviru nove obveščevalne paradigme načelo potrebe po vedenju ustrezno nadomešča in nadgrajuje z načelom potrebe po deliti z ostalimi (Črnčec, 2009). Potrebno je omogočiti dostop do informacij širokemu krogu inštitucij, ki so tako ali drugače vpete v proces zagotavljanja nacionalne varnosti (Črnčec, 2009, str. 4). Lahko bi se preprečil teroristični napad na Združene države Amerike 11. 9. 2001, če bi pristojne službe med seboj delovale usklajeno in si posredovale tajne podatke (Staniforth, 2009, str. 31).

Da se prepreči prekomerno kopičenje tajnih podatkov v službah za tajne podatke, je potrebno enkrat letno narediti pregled (UVTP, 30. člen) in po potrebi uničiti nepotrebne tajne podatke. Predpisi Sveta določajo pregled tajnih podatkov na pet let (PSVT, 10. odstavek, oddelek III).

V varnostnem območju I. stopnje je potrebno voditi razvid tajnih podatkov, s katerimi se oseba seznani že ob samem vstopu v varnostno območje (UVTP, 10. člen). Določba o razvidu tajnih podatkov po Uredbi o varovanju tajnih podatkov je nerodno formulirana. V praksi se večkrat pojavi vprašanje, ali se razvid namesti pred vhodom ali znotraj varnostnega območja I. stopnje, saj sam vstop v to območje že pomeni seznanitev s tajnimi podatki. Logično je, da razvid ne sme biti nameščen pred vhodom v varnostno območje, saj bi se lahko v tem primeru vsaka oseba pred vhodom seznanila o vrsti tajnih podatkov v varnostnem območju oziroma s tajnimi podatki. Predpisi Sveta določajo, da mora biti v območju nameščen razvid (opis) tajnih podatkov, ki se nahajajo v območju (PSVT, 5. odstavek, oddelek IV), kar odpravi problem namestitve razvida tajnih podatkov oziroma razlage 10. člena Uredbe o varovanju tajnih podatkov.

Osebe imajo pravico dostopa do tajnih podatkov stopnje tajnosti INTERNO z nastopom dela ob podpisu izjave, da so seznanjene s predpisi, ki urejajo varovanje tajnih podatkov, in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi, ter da imajo opravljeno osnovno usposabljanje s področja varovanja tajnih podatkov (ZTP, 31.a člen). Vprašanje, ki se postavi: kako lahko osebe dostopajo do tajnih podatkov EU stopnje tajnosti RESTREINT UE (primerljiva nacionalna stopnja tajnosti je INTERNO), saj pristojni organi za stopnjo tajnosti INTERNO ne izdajajo dovoljenj za dostop do tajnih podatkov. Odgovor na to vprašanje je podan v 13. odstavku oddelka V Predpisov Sveta, ki določa, da imajo osebe dostop do tajnih podatkov RESTREINT UE, ko se opozorijo na pomembnost predpisov Evropske unije o varovanju tajnosti in na posledice malomarnosti (osebe morajo tudi opravljati delo v organu in imeti potrebo po vedenju).

Noben nacionalni predpis ne določa, kaj mora storiti oseba, ki ima pri sebi tajne podatke in ki zapušča delovno mesto v organu oziroma je premeščena na delovno mesto, kjer nima več opravka s tajnimi podatki. Problem se pojavi službam za tajne podatke, ki vodijo evidenco o tajnih podatkih, in v katerih so zaposleni pristojni uradniki, odgovorni za varnost obdelave in hranjenja tajnih podatkov. Delno rešitev predstavlja izdaja internih navodil (ZTP, 38. člen). V opisanem primeru se mora izvesti primopredaja tajnih podatkov (PSVT, 13, odstavek, oddelek V). Primopredaja tajnih podatkov omogoča tudi hitro komisijsko uničenje nepotrebnih kopij tajnih podatkov, saj se primopredajni zapisnik lahko uporabi v postopku uničenja tajnih podatkov. V praksi to pomeni:

- sestavo zapisnika o uničenju tajnega podatka,

- priložitev primopredajnega zapisnika kot prilogo zapisniku o uničenju tajnega podatka in
- takojšnje uničenje tajnih podatkov z rezalnikom papirja.

Za evidentiranje dokumentov, ki vsebujejo tajne podatke, se uporabljajo določbe Uredbe o varovanju tajnih podatkov in Uredbe o upravnem poslovanju (UVTP, 28. člen). Na vsak fizični dokument, ki ga prejme organ, je potrebno odtisniti prejemno štampiljko, ki ima naslednja polja (UUP, 118. člen):

- naziv organa, ki je dokument prejel;
- datum prejema dokumenta;
- označba notranje organizacijske enote ali javnega uslužbenca, ki dokument prejme v reševanje;
- številka zadeve;
- vsebinsko označbo prilog ali skupno število prejetih prilog, če so te navedene že v dokumentu;
- skupen znesek vrednosti na dokumentu nalepljenih ali priloženih nerazveljavljenih kolkov, denarja ali vrednotnic.

O posameznem dokumentu je treba evidentirati naslednje podatke (UUP, 148. člen):

- subjekt dokumenta;
- datum prejema ali odprave dokumenta, pri dokumentih za notranje potrebe pa datum nastanka (vhodni, izhodni in lastni dokumenti);
- številko dokumenta;
- kratko vsebino dokumenta (vsebinsko identifikacijo);
- oznako, ali gre za vhodni, izhodni ali lastni dokument;
- signirni znak organizacijske enote ali delovnega mesta javnega uslužbenca, ki rešuje zadevo oziroma dokument sestavi;
- število in kratek opis prilog;
- ključne besede (opcijsko).

Pri evidentiranju tajnih podatkov je potrebno zapisati obsežno število podatkov razen podatkov, iz katerih ne bi bila razvidna vsebina tajnega podatka (UVTP, 28. člen), kar upočasnjuje delo službam za tajne podatke. Predpisi Sveta so glede evidentiranja tajnih podatkov bolj življenjski, saj določajo, da mora arhivski urad ustanove (služba za tajne podatke) vsak dokument stopnje tajnosti CONFIDENTIEL UE in višje ob prihodu ali izhodu iz ustanove vpisati v evidenco (tajne podatki stopnje tajnosti RESTREINT UE torej ni potrebno evidentirati). Podatki, ki jih je treba vpisati (reference, datum in po potrebi številka kopije), morajo omogočati prepoznavo dokumentov in biti vpisani v vpisnik ali vneseni v posebno varovan računalniški nosilec (PSVT, 6. odstavek, oddelek VII). Glede na to, da ima večina dokumentov najnižjo stopnjo tajnosti INTERNO oziroma RESTREINT UE, službe za tajne podatke v Republiki Sloveniji porabijo pretežni del za pisanje podatkov v evidence, kar predstavlja unikum v Evropski uniji. Preveč

časa se namenja evidentiranju tajnih podatkov namesto izdelavi sistemskih rešitev, ki bi olajšale delo s tajnimi podatki.

Tajni podatki stopnje tajnosti INTERNO se lahko prenašajo po lastni prenosni mreži ali priporočeni pošti s povratnico (UVTP, 21. člen). Prenos tajnih podatkov s priporočeno pošto je rizičen, saj obstaja večja verjetnost, da pridejo tajni podatki v roke nepooblaščenim osebam, kot če bi prenos opravile pristojne osebe. Prenos tajnih podatkov po pošti tudi ne omogoča njihove sledljivosti. Prenos dokumentov stopnje tajnosti RESTREINT UE mora potekati na način, da ob prenosu dokumenti ne morejo preiti v roke nepooblaščenim osebam (PSVT, 21. odstavek, oddelek VII), česar prenos po pošti ne zagotavlja. Teoretično bi lahko nastal večji problem v primeru, da bi se tajnemu podatku določila prenizka stopnja tajnosti glede na vsebino podatka, distribucija bi pa potekala po pošti, kjer bi prišlo do izgube tajnega podatka in do razkritja nepooblaščeni osebi. Pogosti so primeri, ko se dokumentom stopnja tajnosti sploh ne določi, bi se pa morala, in se taki dokumenti razkrijejo nepooblaščenim osebam (medijsko so znani primeri odtekanja dokumentov brez oznake stopenj tajnosti nepristojnim osebam).[34] Ob populizmu, nepotizmu in številnih drugih dejavnikih demokratičnega primitivizma, ki smo jim priča v javnosti, je posebna skrb za tajnost podatkov in varstvo zasebnosti še toliko bolj potrebna (Kečanović, 2001, str. 93).

Zakon o tajnih podatkih za kršilce predpisov s področja varovanja tajnih podatkov predpisuje vmesno varnostno preverjanje (ZTP, 25.b člen), če obstajajo varnostni zadržki, zaradi katerih se osebi zavrne izdaja dovoljenja za dostop do tajnih podatkov v primeru ugotovitev varnostnega preverjanja, ki vzbujajo utemeljene dvome v posameznikovo verodostojnost, zanesljivost in lojalnost za varno obravnavanje tajnih podatkov (ZTP, 27. člen). Če oseba ne izpolnjuje pogojev za zasedbo delovnega mesta, ker ji je bilo zavrnjeno ali preklicano dovoljenje za dostop do tajnih podatkov, se uporabljajo določbe Zakona o javnih uslužbencih (Uradni list RS, št. 56/2002, 23/2005, 35/2005 – UPB1, 62/2005 – odločba US, 113/2005, 21/2006 – odločba US, 23/2006 – sklep US, 32/2006 – UPB2, 62/2006 – sklep US, 131/2006 – odločba US, 33/2007, 63/2007 – UPB3 in 65/2008), kar pomeni prenehanje delovnega razmerja. Predpisi Sveta določajo disciplinsko odgovornost za osebe, ki so odgovorne za ogrožanje tajnih podatkov EU, in ne določajo sankcije prenehanja delovnega razmerja.

Pri primerjavi pravnih predpisov Republike Slovenije in Evropske unije o tajnih podatkih se pokaže precejšnja medsebojna podobnost v pravni ureditvi. Zakon o tajnih podatkih je bil sprejet v naglici zaradi vključevanja Republike Slovenije v evro-atlantske povezave in zaradi Predpisov Sveta, zaradi česar je pravna ureditev obravnavanja tajnih podatkov nesistematično urejena, kar je deloma odpravila Uredba o varovanju

[34] Leta 2007 je v Sloveniji izbruhnila afera "washingtonska depeša". Veleposlaništvo Republike Slovenije v Washingtonu D. C. ni označilo s stopnjo tajnosti depeše, čeprav bi to moralo storiti. Depeša je prišla nepooblaščeno v roke novinarjem beograjske Politike in ljubljanskega Dnevnika.

tajnih podatkov, ki je bila sprejeta leta 2005, t. j. štiri leta po sprejemu Zakona o tajnih podatkih. Da je bil Zakon o tajnih podatkov slabo pripravljen, se kaže pri branju Uredbe o varovanju tajnih podatkov, kjer se med obema pravnima predpisoma mešajo in podvajajo pravne dikcije.

5 USTANOVITEV SLUŽBE ZA TAJNE PODATKE NA STALNEM PREDSTAVNIŠTVU REPUBLIKE SLOVENIJE PRI EVROPSKI UNIJI

Stalno predstavništvo Republike Slovenije pri Evropski uniji v Bruslju je diplomatsko-konzularno predstavništvo Republike Slovenije, ki zastopa interese države pri Evropski uniji. Zaposleni diplomati stalnega predstavništva skupaj s preostalimi predstavniki iz 26 držav članic predstavljajo Svet Evropske Unije, ki mu predseduje na vsake pol leta druga država članica. Zaradi slovenskega predsedovanja Svetu Evropske unije v prvi polovici leta 2008 so bile potrebne številne priprave in usposabljanja za ta namen določenih oseb, ki so prišli iz različnih organov javne uprave. Poleti leta 2006 se je stalno predstavništvo preselilo na novo lokacijo na naslovu Rue du Commerce 44 v Bruslju (sedemnadstropna stavba), kjer je v času predsedovanja delalo več kot 170 oseb. Delo na stalnem predstavništvu je organizirano po delovnih skupinah, katerim nudijo strokovno-tehnično podporo notranje službe, med katerimi je tudi Služba za tajne podatke. Notranjim službam zagotavljajo podporo službe Ministrstva za zunanje zadeve Republike Slovenije.

5.1 USTANOVITEV SLUŽBE ZA TAJNE PODATKE

Na stalnem predstavništvu je bila na novi lokaciji ustanovljena Služba za tajne podatke, ki skrbi za rokovanje, razpošiljanje in arhiviranje tajnih podatkov Republike Slovenije, za delo s tajnimi podatki Evropske unije pa je bil v okviru službe ustanovljen podarhivski urad TRÈS SECRET UE/EU TOP SECRET, imenovan tudi podregister (angl. subregistry) za tajne podatke EU (PSVT, 4. odstavek, oddelek VIII).

Služba za tajne podatke prejema tajne podatke EU od evropskih inštitucij in od Službe za tajne podatke Ministrstva za zunanje zadeve, ki jih distribuira zaposlenim na stalnem predstavništvu. Služba za tajne podatke pošilja tajne podatke EU Službi za tajne podatke Ministrstva za zunanje zadeve, katera jih naprej distribuira med zaposlene na ministrstvu in pošilja pristojnim organom v Republiki Sloveniji (PSVT, 2. odstavek, oddelek VIII), s čimer se tokokrog prenosa tajnih podatkov zaključi.

Za vzpostavitev Službe za tajne podatke je bilo potrebno izpolniti določene naloge in sprejeti ustrezne postopke in ukrepe, s čimer je služba lahko pridobila akreditacijo Urada Vlade Republike Slovenije za varovanje tajnih podatkov za delovanje službe s stopnjo tajnosti STROGO TAJNO oziroma TRÈS SECRET UE/EU TOP SECRET.

V specialističnem delu je opisana Služba za tajne podatke zaradi specifike dela na način, ki še dopušča varovanje tajnosti dela službe. V nalogi ni navedeno, kje se nahajajo prostori službe, ali so varnostna območja označena ali prikrita ipd.

Služba za tajne podatke na stalnem predstavništvu je pričela delovati v ustrezno varovanem območju, v katerega je imelo več oseb pravico dostopa, kar je v nasprotju z definicijo delovanja službe. Najprej je bilo potrebno premagati to oviro in nepooblaščenim osebam preprečiti dostop do prostorov službe, kar se je zgodilo z ad hoc ustno razglasitvijo varnostnega območja I. stopnje. Zaposleni, ki so dotedaj imeli pravico dostopa do prostorov službe, so se počutili ogrožene in prizadete, saj se jim je odvzela pravica, ki so jo imeli na stari lokaciji stalnega predstavništva, ko se lahko nemoteno gibali po vseh prostorih stalnega predstavništva. V Službi za tajne podatke je bila dne 18. septembra 2006 izvedena taktična poteza in pripravljen sklep, s katerim se je dovolil vstop v prostore službe samo zaposlenim osebam v službi, v primeru intervencijskega dostopa pa določenim pristojnim osebam stalnega predstavništva (UVTP, 10. člen). Ko je bil sklep podpisan s strani predstojnika organa (ministra za zunanje zadeve), bi se lahko vsak nepooblaščen vstop v varnostno območje I. stopnje ustrezno sankcioniral (skrajna sankcija je odpoved delovnega razmerja). Sklep je bil vročen po elektronski pošti vsem osebam, ki so pred izdajo sklepa nepooblaščeno vstopale v prostore službe.

Službo za tajne podatke je bilo potrebno opremiti z varnostnotehnično opremo, s katero bi se lahko obdelovali tajni podatki najvišje stopnje tajnosti:

- rezalnik papirja s specifiko vzdolžnega in prečnega razreza papirja (angl. cross cut paper shredder) velikosti 0,8 mm x 15 mm z razrezom do nerazpoznavnosti in neobnovljivosti tajnih podatkov (SDPVOVVO, 12. člen);
- varnostne blagajne standarda SIST EN 1143 protivlomne stopnje III z nameščenimi elektronskimi oziroma mehanskimi ključavnicami standarda SIST EN 1300 razreda (UVTP, 19 člen in SDPVOVVO, 10. člen);
- informacijska tehnologija (strojna in programska oprema);
- tiskalniki in
- fotokopirni stroj.

Ob izhodu iz varnostnega območja I. stopnje se je namestil razvid tajnih podatkov, na katerem je navedeno, s kakšnimi tajnimi podatki se seznani oseba z vstopom v varnostno območje (UVTP, 10. člen).

Služba za tajne podatke je preverila, ali so izpolnjeni naslednji varnostni pogoji za varnostno območje I. stopnje (UVTP, 10. člen):

- sistem vhodnega nadzora, ki zagotavlja popoln nadzor nad vstopom oziroma izstopom oseb v to območje, dovoljuje vstop samo osebam, ki imajo ustrezno dovoljenje za dostop do tajnih podatkov in so v tem območju zaposlene oziroma imajo posebno dovoljenje za vstop v to območje;

- neposredno in neprekinjeno fizično varovanje varnostnega območja, ki se lahko na podlagi ocene ogroženosti dopolni ali nadomesti z elektronskim sistemom za protivlomno varovanje varnostnega območja, katerega alarmni signal je vezan na enoto, odgovorno za ukrepanje ob alarmu (nadzorni center); intervencijski čas mora biti krajši od sedmih minut;
- ob nadomestitvi fizičnega varovanja s sistemom tehničnega varovanja mora ta sistem zagotavljati celovit nadzor varnostnega območja, ki mora biti nadzorovano iz nadzornega centra, sistem pa mora imeti zagotovljeno rezervno napajanje.

Pri varnostnih zahtevah se je v Službi za tajne podatke pojavilo nekaj odprtih vprašanj v zvezi z zahtevami, ki so predpisane za varnostno območje I. stopnje, ki pa so se rešila. Na stalnem predstavništvu je za namestitev ustrezne varnostnotehnične opreme in pripravo ustreznih varnostnotehničnih navodil in postopkov pristojna Varnostno tehnična služba Ministrstva za zunanje zadeve.

Z vzpostavitvijo varnostnega območja I. stopnje in namestitvijo potrebne opreme za delovanje Službe za tajne podatke je obstajala možnost poskusov aktivnega (nameščenost prisluškovalnih naprav) ali pasivnega (prisluškovanje iz zunanjosti prostorov stalnega predstavništva) prisluškovanja, zato je pristojna služba opravila protiprisluškovalni pregled (UVTP, 18. člen).

Služba za tajne podatke je vzpostavila evidenco vstopov in gibanja v varnostnem območju I. stopnje (UVTP, 14. člen), s katero se je pred vstopom oseb v varnostno območje preverila njihova identiteta in namen obiska (priloga 2). Osebe morajo podpisati tudi posebno izjavo, da so seznanjene s predpisi s področja varovanja tajnih podatkov, opozorjene pa so tudi na kazensko odgovornost izdaje tajnosti. Za izdajo tajnosti je predpisana kazen zapora do petih let (KZ-1, 260. člen). Izjava je pripravljena v slovenskem, angleškem in francoskem jeziku (priloga 3, 4 in 5).

Za zaposlene v Službi za tajne podatke so bile izdelane identifikacijske izkaznice, ki morajo biti pripete na vidnem mestu. Na izkaznici se nahaja slika zaposlenega, ime in priimek ter njegov status (UVTP, 11. člen).

Služba za tajne podatke je pričela voditi seznam vpogledov za tajne podatke stopnje tajnosti TAJNO oziroma SECRET UE ali višje (UVTP, 29. člen), ki se prej ni vodil.

Vsak organ ob upoštevanju postopkov in ukrepov, določenih z Uredbo o varovanju tajnih podatkov, izdela načrt varovanja tajnih podatkov, s katerim glede na stopnjo tajnosti podatkov in oceno ogroženosti podrobneje predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov v I. ali II. varnostnem območju (UVTP, 32. člen). Za izdelavo načrta varovanja tajnih podatkov je pristojna Varnostno tehnična služba Ministrstva za zunanje zadeve, ki je po številnih

intervencijah stalnega predstavništva šele po enem letu od delovanja Službe za tajne podatke izdelala načrt varovanja, ki je sestavljen iz splošnega in posebnega dela ter zajema vse varnostne vidike varovanja stalnega predstavništva in tajnih podatkov (UVTP, 32. člen):

- oceno ogroženosti;
- opis glavnega in pomožnih objektov (lega, vhodi, izhodi, zasilni izhodi, skica oziroma fotografije objekta, glavne in pomožne poti do objekta ter podatki o varnostnotehnični opremi);
- podatke o nosilcu varnostnega načrta;
- zaščitne ukrepe za osebe, ki imajo dostop do tajnih podatkov;
- ukrepe fizičnega varovanja (zunanje in notranje fizično varovanje, varnostne točke z opisi nalog izvajalcev);
- ukrepe tehničnega varovanja (zunanje in notranje tehnično varovanje, nadzor nad vstopom in izstopom, alarmni sistem in postopki ob sprožitvah posameznih stopenj alarmov, dokumentiranje);
- postopke ob nasilnem vstopu in nepredvidenem dogodku: požaru, potresu, povodnji in drugih naravnih nesrečah;
- postopke in ukrepe ob izgubi, razkritju ali odtujitvi tajnega podatka in
- ukrepe in postopke pri opravljanju vzdrževalnih in drugih del v varnostnih območjih.

Ko je bil izdelan načrt varovanja, je stalno predstavništvo zaprosilo Urad Vlade Republike Slovenije za varovanje tajnih podatkov za akreditacijo Službe za tajne podatke za najvišjo stopnjo tajnosti. Po pregledu prostorov, varnostnotehnične opreme in postopkov dela v Službi za tajne podatke je urad izdal akreditacijsko potrdilo za delovanje službe za stopnjo tajnosti STROGO TAJNO oziroma TRÈS SECRET UE/EU TOP SECRET (PSVT, 10. odstavek, oddelek I).

5.2 TEŽAVE IN POMANJKLJIVOSTI PRI ZAČETKU DELOVANJA SLUŽBE

Služba za tajne podatke je imela do konca septembra leta 2006 vzpostavljeno varnostno območje I. stopnje, ustrezno informacijsko in tehnično opremo, delo s tajnimi podatki pa ni potekalo z varnostnimi standardi, ki so določeni v predpisih Republike Slovenije in Evropske unije o varovanju tajnosti.

Diplomati (prejemniki tajnih podatkov) so na novi lokaciji stalnega predstavništva pričakovali enak sistem distribucije in dela s tajnimi podatki kot na stari lokaciji (protipraven način poslovanja). Služba za tajne podatke je prvi mesec delovanja (september 2006) na novi lokaciji delala po ustaljenih metodah, obenem se je pa pripravljala na prehod na nov način poslovanja s tajnimi podatki v skladu s pravnimi predpisi.

Služba za tajne podatke je distribuirala tajne podatke prejemnikom prvi mesec delovanja na naslednje načine:

- Izdelalo se je ustrezno število kopij tajnih dokumentov, ki so se evidentirali v delovodnik glede na opravljanje dela diplomatov v delovnih skupinah brez upoštevanja načela potrebe po vedenju. Kopije bi se morale izdelati v manjšem obsegu po načelu potrebe po vedenju (ZTP, 31. člen).
- Tajne podatke in delovodnike so uradniki službe fizično nosili od pisarne do pisarne in jih vročili prejemnikom, ki so prevzem potrdili z vpisom datuma in podpisom. Tajne podatke bi morali prejemniki prevzeti v Službi za tajne podatke (UVTP, 16. člen).
- Zaradi velike količine tajnih podatkov in delovodnikov, v katerih se je vodila evidenca tajnih podatkov za različne stopnje tajnosti, je obstajala verjetnost izgube tajnih podatkov ali delovodnikov pri njihovem prenosu. 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 (UVTP, 16. člen).
- V kolikor prejemnika tajnega podatka ni bilo v pisarni, je Služba za tajne podatke tudi večkrat poskušala vročiti tajni podatek prejemniku. Prejemniki bi morali prevzemati tajne podatke v Službi za tajne podatke, služba bi pa morala ukiniti distribucijo neprevzemnikom tajnih podatkov (UVTP, 16. člen).
- V nekaterih primerih tajnega podatka ni bilo mogoče vročiti prejemniku zaradi njegove odsotnosti. Tajni podatek bi se moral vročiti prejemniku v Službi za tajne podatke. V kolikor bi bil prejemnik odsoten, bi bil tajni podatek arhiviran in pripravljen na vročitev ob vrnitvi prejemnika na delovno mesto (UVTP, 16. člen).

Služba za tajne podatke je zaznala prvi mesec delovanja naslednja protipravna ravnanja:

- služba je prejemala kopije tajnih podatkov, iz katerih je bilo razvidno, da so nastale s protipravnim kopiranjem; kopija tajnega podatka se lahko izdela le v Službi za tajne podatke na podlagi pisarniške odredbe (UVTP, 26. člen);
- prejemniki so zahtevali določen tajni podatek, pri čemer se je izkazalo, da ga imajo pri sebi (vpogled v delovodnik tajnih podatkov); ob opravljenem razgovoru so prejemniki priznali, da so tajne podatke vrgli v koš za smeti oziroma založili.

V prvem mesecu delovanja službe so se pokazale naslednje slabosti v zvezi z delom s tajnimi podatki in s pravico dostopa do tajnih podatkov:

- prejemniki tajnih podatkov se niso menili za predpise s področja varovanja tajnih podatkov niti jih niso poznali;
- nekateri diplomati so celo rekli, da za njih Zakon o tajnih podatkih ne velja;

- na stalno predstavništvo so prihajali novi diplomati, ki niso imeli izdanega dovoljenja za dostop do tajnih podatkov, obenem so pa od službe zahtevali tajne podatke (v službi se je pojavilo vprašanje, kdo bi prevzel odgovornost za posledice, če bi bila diplomatom izdaja dovoljenja za dostop do tajnih podatkov zavrnjena).

Zaradi opisanih težav je vodja Službe za tajne podatke na stalnem predstavništvu imel konec septembra leta 2006 sestanek z vodjo stalnega predstavništva (veleposlanik – stalni predstavnik) in mu obrazložil situacijo neustreznega dela s tajnimi podatki in ga opozoril:

- na kazenske določbe Zakona o tajnih podatkih in Kazenskega zakonika (Uradni list RS, št. 55/2008, 66/2008 – popravek in 39/2009), ki predpisujeta za kršenje predpisov s področja tajnih podatkov globo od 417,29 EUR dalje pa do zapora do petih let;
- na dejstvo, da je kot vodja stalnega predstavništva objektivno odgovoren za kršenje in neupoštevanje predpisov;
- da se za diplomate, ki kršijo pravne predpise s področja tajnih podatkov, lahko predlaga vmesno varnostno preverjanje, pri čemer se jim lahko zavrne izdaja dovoljenja za dostop do tajnih podatkov, česar posledica je odpoved delovnega razmerja.

Sestanek je pomenil odprto pot Službi za tajne podatke, da pripravi interna navodila za delo s tajnimi podatki in sprejme ustrezne ukrepe, da bi se preprečilo protipravno ravnanje s tajnimi podatki. Dogovorjeno je bilo tudi, da se prične uporabljati čitalnica za branje tajnih podatkov v varnostnem območju II. stopnje, kjer lahko diplomati prevzamejo ali preberejo tajne podatke od uradnikov Službe za tajne podatke.

Vodja stalnega predstavništva je dne 5. oktobra 2006 izdal interno navodilo o prenosu in obdelavi tajnih podatkov na stalnem predstavništvu, ki ga je pripravila Služba za tajne podatke in ki vsebuje naslednje točke:

- diplomati prejmejo o prispelem tajnem podatku elektronsko sporočilo;
- diplomati lahko tajne podatke prevzamejo od Službe za tajne podatke v čitalnici;
- diplomati lahko iznosijo tajne podatke stopnje tajnosti INTERNO oziroma RESTREINT UE iz čitalnice v upravno območje (prostori stalnega predstavništva);
- tajne podatke stopnje tajnosti ZAUPNO oziroma CONFIDENTIEL UE ali višje lahko diplomati preberejo v čitalnici, ne smejo jih pa iznesti iz čitalnice;
- diplomati morajo po obdelavi tajne podatke vrniti Službi za tajne podatke.

Služba za tajne podatke je poslala interno navodilo po elektronski pošti vsem zaposlenim na stalnem predstavništvu, kar je povzročilo nejevoljo med diplomati.

Obseg prejemanja tajnih podatkov se je zmanjšal skoraj za polovico, zaradi česar je tudi služba zmanjšala razmnoževanje tajnih podatkov.

Priprave predsedovanju so bile vsak mesec bolj intenzivne, na stalno predstavništvo so prihajali novi diplomati, število sestankov diplomatov na Svetu Evropske unije je bilo v porastu, kar je pomenilo tudi večjo potrebo po tajnih podatkih. Ker so se tajni podatki obdelovali tudi na sestankih na Svetu, je Služba za tajne podatke diplomatom omogočila iznos tajnih podatkov stopnje tajnosti ZAUPNO oziroma CONFIDENTIEL UE ali višje izven prostorov stalnega predstavništva. Oseba, ki prevzame tajni podatek, to potrdi z lastnoročnim podpisom in s tem prevzame skrb za varnost tajnega podatka (UVTP, 16. člen).

Kadar je Služba za tajne podatke prejela protipravno kopiran tajni podatek, je o tem obvestila po elektronski pošti vodjo stalnega predstavništva in diplomata, katerega tajni podatek se je protipravno kopiral (na dokumentu sta zapisana ime in priimek diplomata). S 1. januarjem 2007 se o protipravnem kopiranju obvešča le vodjo stalnega predstavništva.

Na mesečnih kolegijih je vodja stalnega predstavništva redno opozarjal na dolžnost skrbnega ravnanja s tajnimi podatki in upoštevanje navodil in napotkov Službe za tajne podatke ter opozarjal na kazenske sankcije za kršilce predpisov s področja tajnih podatkov. Vodja je tudi večkrat izpostavil, da je osebno odgovoren zaradi kršenja teh predpisov.

Odgovornost za razvoj varnostne kulture pri posameznih članih in organizacijah v celoti se nahaja na različnih nivojih vodenja in upravljanja teh organizacij. Izobraževanje in proces upravljanja z znanjem ima zelo pomembno vlogo za poviševanje nivoja varnostne kulture in zavedanja po potrebnosti učinkovitega varovanja tajnih podatkov (Čaleta, 2008, str. 270).

Uspešno in učinkovito delovanje organizacije je usmerjeno v doseganje smotrov in ciljev, te pa dosegamo z ustrezno politiko, kjer so cilji podrejeni smotrom in so zastavljeni tako, da tvorijo hierarhijo in postopnost glede na pomembnost pri uresničevanju vizije organizacije (Černetič in Dečman Dobrnjič, 2006, str. 478).

Sistem ravnanja s tajnimi podatki se je na stalnem predstavništvu izboljšal, zmanjšalo pa se je tudi protipravno kopiranje tajnih podatkov.

6 ZASNOVA MODELA ORGANIZIRANOSTI SLUŽBE ZA TAJNE PODATKE

Služba za tajne podatke ima za delovanje potrebno varnostnotehnično opremo, izdelan načrt varovanja, sprejeta interna navodila in sprejete zahteve v skladu z nacionalnimi pravnimi predpisi in predpisi Evropske unije. Ker je večina tajnih podatkov stopnje tajnosti INTERNO oziroma RESTREINT UE (najnižja stopnja tajnosti), ima služba s temi podatki tudi največ dela. Da bi se poenostavilo delo s tajnimi podatki in zmanjšal obseg dela, je potrebno sprejeti nove metode in tehnike dela s tajnimi podatki in zasnovati nov model organiziranosti Službe za tajne podatke. Pri obdelavi tajnih podatkov je možno uvesti nov pristop dela z upoštevanjem pravnih predpisov, ki zmanjša čas obdelave tajnih podatkov in materialne stroške.

6.1 ORGANIZACIJSKE MOŽNOSTI ZA ODPRAVO TEŽAV V SLUŽBI ZA TAJNE PODATKE

6.1.1 Prejem, evidentiranje in distribucija tajnih podatkov

V Službi za tajne podatke poteka prejem tajnih podatkov na naslednji način (UVTP, 16., 26., 28. in 29. člen):

- tajne podatke prejme služba v elektronski ali fizični obliki (angl. hard copy);
- podatki v elektronski obliki se dekriptirajo in natisnejo;
- izdela se ustrezno število kopij tajnega podatka (UVTP, 26. člen);
- število kopij se izdela glede na vsebino tajnega podatka in glede na zaposlene v delovnih skupinah, na katere se vsebina nanaša brez upoštevanja načela potrebe po vedenju (ZTP, 31. člen);
- tajne podatke se vpiše v osem delovodnikov (štirje so namenjeni za nacionalne stopnje tajnosti, štirje pa za stopnje tajnosti Evropske unije): zaporedna številka vpisa, datum vpisa, številka tajnega podatka, številka kopije, ime in priimek prejemnika tajnega podatka (UVTP, 28. člen);
- na vsak tajni podatek se odtisne prejemna štampiljka, vpiše se datum prejema, stopnja tajnosti, številka kopije tajnega podatka in ime ter priimek prejemnika (UVTP, 28. člen);
- po elektronski pošti se obvesti prejemnike tajnih podatkov;
- tajne podatke se zloži v predalčnike, kjer čakajo na prevzem;
- na tajne podatke stopnje tajnosti TAJNO oziroma SECRET UE ali višje stopnje se pripne seznam vpogledov tajnih podatkov (UVTP, 29. člen).

6.1.2 Delo diplomatov s tajnimi podatki

Ko diplomati prejmejo tajne podatke, jih obdelujejo v čitalnici, v upravnem območju (pisarnah stalnega predstavništva) in na sestankih delovnih skupin Sveta Evropske unije.

V času priprav na predsedovanje Svetu se je na stalnem predstavništvu povečal obseg dela diplomatov in število sestankov izven prostorov stalnega predstavništva. Pred pomembnimi sestanki Sveta (na primer Svet za splošne zadeve in zunanje odnose, angl. General Affairs and External Relations Council (GAERC)) se je povečala potreba diplomatov po tajnih podatkih, ki niso mogli fizično prevzeti tajnih podatkov v Službi za tajne podatke. Služba za tajne podatke je po preučitvi pravnih predpisov uvedla v izjemnih primerih distribucijo tajnih podatkov vodji stalnega predstavništva, njegovemu namestniku in vodji Političnega in varnostnega odbora (angl. Political and Security Committee (PSC)) preko imenovanih pooblaščencev. Pooblaščenci so nastopali v funkciji kurirja in so morali imeti dovoljenje za dostop do tajnih podatkov tiste stopnje tajnosti, za katero so bili pooblaščeni za prevzemanje tajnih podatkov. S podpisom o prevzemu tajnega podatka je pooblaščenec prevzel skrb za varnost tajnega podatka (UVTP, 16. člen). Prenos se je opravljal v zaprti in neprosojni ovojnici (UVTP, 21. člen).

Diplomati po prejemu (neprejemu) tajnih podatkov ravnajo na naslednje načine:

- Če pristojni diplomat oceni, da potrebuje tajni podatek še nekdo (podelitev potrebe do vedenja), zaprosi Službo za tajne podatke za izdelavo kopije tajnega podatka (ZTP, 31. člen).
- Diplomati bi morali takoj po obdelavi vrniti tajne podatke Službi za tajne podatke (UVTP, 16. člen), kar pa se zgodi redko.
- Nekateri diplomati po končanem delu puščajo tajne podatke v pisarnah na delovnih površinah, s čimer se krši eno od temeljnih varnostnih načel pri delu s tajnimi podatki (načelo prazne mize). "Javni uslužbenci ne smejo puščati nosilcev z osebnimi podatki, poslovnimi skrivnostmi ali drugimi varovanimi podatki na odprtih površinah pisarniške opreme ali drugih mestih, kjer so dostopni nepooblaščenim osebam. Nosilce podatkov iz prejšnjega odstavka morajo javni uslužbenci varno shraniti vedno, ko niso fizično prisotni v prostoru." (UUP, 84. člen).
- Določeni diplomati založijo tajne podatke: izguba ali zlaganje tajnih podatkov z ostalim službenim in osebnim gradivom (UVTP, 35. člen).
- Določeni diplomati ne sprejemajo tajnih podatkov, kar kaže na malomarnost opravljanja dela.

Tajni podatki stopnje tajnosti INTERNO oziroma RESTREINT UE se lahko hranijo v pisarniških ali kovinskih omarah v prostorih stalnega predstavništva, ki je v celoti določeno kot upravno območje (UVTP, 10. in 19. člen).

6.1.3 Razvoj modela organiziranosti

Tajne podatke EU stopnje tajnosti CONFIDENTIEL UE ali višje je potrebno evidentirati (PSVT, 6. odstavek, oddelek VII). Tajnih podatkov EU najnižje stopnje tajnosti RESTREINT UE torej ni potrebno evidentirati. Evidentiranju tajnih podatkov stopnje tajnosti INTERNO oziroma RESTREINT UE se ni moč izogniti. Tajne podatke vseh stopenj tajnosti je potrebno evidentirati (UVTP, 28. člen in UUP, 118. in 148. člen).

Postopek evidentiranja in distribucije tajnih podatkov bi se lahko izboljšal z novimi metodami dela. Število kopij tajnega podatka se ne bi izdelalo več za vse diplomate, ki delajo na določenem delovnem področju, temveč bi se distribucija omejila glede na njihovo potrebo po vedenju (angl. need to know). Načelo potrebe po vedenju je temeljno načelo pri delu s tajnimi podatki (PSVT, 7. odstavek, del I). Osebe lahko dostopajo do tajnih podatkov, če imajo dovoljenje za dostop do tajnih podatkov in če imajo potrebo po vedenju (Gidiere, 2006, str. 92). Težnja prejemnikov tajnih podatkov je, da bi prejeli čim več tajnih podatkov, čeprav nimajo potrebe po vedenju. Načelo potrebe po vedenju je ožje kot pojem opravljanja funkcije ali delovnih nalog (ZTP, 31. člen). Potrebno bi bilo izdelati distribucijsko listo prejemnikov tajnih podatkov in kratic Sveta Evropske unije (na primer kratica COWEB je namenjena za zahodni del Balkana), ki bi jo določili vodja stalnega predstavništva in vodje notranjih organizacijskih enot stalnega predstavništva, s tem da bi imela Služba za tajne podatke pravico omejitve distribucije v primeru neprevzemanja tajnih podatkov (s tem bi se zmanjšalo prekomerno razmnoževanje tajnih podatkov). Distribucijska lista bi tudi olajšala delo Službi za tajne podatke, saj večkrat ni mogoče določiti prejemnike tajnih podatkov zaradi številnih kratic Sveta, ki so znane zgolj določenim diplomatom (v praksi se kažejo največji problemi na področju notranjih zadev, pravosodja, financ, kmetijstva in gospodarstva). Zaradi napačne distribucije tajnih podatkov lahko prejme tajni podatek oseba, ki nima potrebe do vedenja, kar bi pomenilo protipravno ravnanje službe.

Prejemniki tajnih podatkov potrebujejo učinkovito službo za tajne podatke, ki mora ažurno distribuirati tajne podatke (Hughes, 2008, str. 14).

Pri izdelavi kopij tajnih podatkov bi se na prazen list pred vstavitvijo v tiskalnik ali v fotokopirni stroj večkrat krepko natisnilo diagonalno z različno barvo za posamezno stopnjo tajnosti (priloga 6):

- številko kopije tajnega podatka in
- stopnjo tajnosti,

kar bi omogočilo:

- povečanje sledljivosti tajnega podatka (številka kopije tajnega podatka je vezana na prejemnika),
- zmanjšanje zlorabe podatka (protipravno kopiranje in založitev) in
- olajšalo arhiviranje tajnih podatkov.

Evidentiranje tajnih podatkov se ne bi vodilo več v osmih delovodnikih, temveč s pomočjo ustreznega programa (lahko bi se uporabil program Excel, kar ne bi predstavljalo dodatnega stroška, saj javna uprava uporablja Windows okolje z MS Office), ki ga ni težko izdelati osebam z osnovnim računalniškim znanjem. Prednosti in možnosti računalniške evidence pred vodenjem evidence s pomočjo delovodnikov so naslednje:

- ažuren pregled nad stanjem tajnih podatkov (tajni podatki se lahko iščejo po številki tajnega podatka, kar omogoča takojšen pregled nad tajnimi podatki (v delovodniku je iskanje tajnih podatkov po številki tajnega podatka dolgotrajno); če diplomat ponovno zahteva tajni podatek in sporoči številko tajnega podatka, je iz evidence takoj razvidno, ali je bil tajni podatek vrnjen);
- manj pisanja (zaporedne številke vhodnih dokumentov in datumi vpisa se avtomatsko zapisujejo; pri vnosu inicialk prejemnika tajnega podatka se lahko izpiše ime in priimek prejemnika tajnih podatkov;
- v evidenco se zabeleži dvig tajnega podatka in tudi njegova vrnitev;
- omogočen bi bil prikaz nevračnikov tajnih podatkov Službi za tajne podatke (nevračnika, ki bi bil na prvem mestu, bi služba po elektronski pošti pozvala na vračilo tajnega podatka; vsak mesec bi služba vodji stalnega predstavništva predala seznam nevračnikov tajnih podatkov) in
- sprostitev prostora v blagajni (osem delovodnikov ne bi več zasedalo prostora v blagajni, blagajna lahko ostane zaklenjena).

Za večjo varnost pri delu s tajnimi podatki bi diplomati morali voditi pisno evidenco o prejetih tajnih podatkih stopnje tajnosti INTERNO oziroma RESTREINT UE z navedeno številko in datumom tajnega podatka, kar bi pri vračilu tajnih podatkov Službi za tajne podatke olajšalo delo pri komisijskem uničenju tajnih podatkov (UVTP, 30. člen), zmanjšalo nepotrebno kopičenje podatkov in povečalo odgovornost diplomatov pri delu s tajnimi podatki.

Tajni podatki stopnje tajnosti ZAUPNO oziroma CONFIDENTIEL UE ali višje bi morali biti Službi za tajne podatke vrnjeni po končani obdelavi.

Prejemniku tajnega podatka, ki ga kljub pozivu Službe za tajne podatke po elektronski pošti ne prevzame v 14 dneh in ni odsoten z dela, se ukine distribuiranje tajnih podatkov do preklica službe (s tem se zmanjša nepotrebno fotokopiranje tajnih podatkov in arhiviranje).

Vsak diplomat bi moral po končanem delovnem času v celoti pospraviti delovno površino iz varnostnih razlogov. Vodja stalnega predstavništva bi lahko varnostnikom z dovoljenjem za dostop do tajnih podatkov ustno naročil, da po naključno izbranih nezaklenjenih pisarnah izven delovnega časa opravijo pregled in začasno zasežejo nevarovane tajne podatke, ki bi jih predali Službi za tajne podatke.

Vodja stalnega predstavništva bi lahko za kršilce pravnih predpisov o varovanju tajnosti in za neprejemnike tajnih podatkov uvedel ustrezne sankcije. Diplomati se ne zavedajo ali pa se nočejo zavedati, da so zaradi malomarnega dela s tajnimi podatki lahko predlagani v postopek vmesnega varnostnega preverjanja, kjer se jim lahko zavrne izdaja dovoljenja za dostop do tajnih podatkov, kar posledično pomeni neizpolnjevanje predpisanih pogojev za zasedbo delovnega mesta in odpoved delovnega razmerja.

6.2 IMPLEMENTACIJA MODELA ORGANIZIRANOSTI

6.2.1 Postopki in ukrepi Službe za tajne podatke za uvedbo modela organiziranosti

Vpeljava novega modela organiziranosti v Službi za tajne podatke ne bi predstavljala dodatnih stroškov, stroški bi se kvečjemu zmanjšali. Vpeljava modela organiziranosti je na strani Službe za tajne podatke, uradniki Službe za tajne podatke in diplomati pa se morajo ravnati po dodatnih novih postopkih in ukrepih, ki jih predvideva nov model organiziranosti.

Služba za tajne podatke mora sprejeti naslednje postopke in ukrepe s sodelovanjem pristojnih oseb na stalnem predstavništvu, ki so potrebni za uvedbo novega modela organiziranosti:

- priprava seznama kratic Sveta Evropske unije, ki pokrivajo vsa delovna področja Sveta, ki so zapisane na tajnih podatkih ter od katerih je odvisna dodelitev potrebe po vedenju (primeri kratic: COAFR (delovna skupina za Afriko), COLAT (delovna skupina za Latinsko Ameriko), CONUN (delovna skupina za Združene narode), COTER (delovna skupina za terorizem) itn.);
- sestanek uradnikov Službe za tajne podatke z vodjo stalnega predstavništva (vodja COREPER II, angl. Committee of Permanent Representatives II (Odbor stalnih predstavnikov II), z namestnikom stalnega predstavnika (vodja COREPER I), z vodjo PSC, z vodjo RELEX (delovna skupina za zunanje odnose), z vodjo CIVCOM (delovna skupina za civilno krizno upravljanje) in z vodjo MILITARY COMMITTEE (Vojaški odbor), kjer se na sestanku dogovori o osebah, ki bodo imele potrebo do vedenja pri obravnavanju tajnih podatkov v zvezi s pripravljenim seznamom kratic;
- izdelava distribucijske liste, v kateri so navedeni prejemniki tajnih podatkov EU glede na kratice delovnih področij Sveta;
- izdelava predlog v programu Word za različne stopnje tajnosti dokumentov (na primer: Svet uporablja za stopnjo tajnosti CONFIDENTIEL UE zeleno barvo), tisk predlog in njihov vnos v predalnike ob fotokopirnemu stroju in ob tiskalniku;

- izdelava računalniške evidence za vodenje tajnih podatkov v programu Excel, ki med drugim omogoča takojšnji prikaz nevračnikov tajnih podatkov po številu nevrnjenih tajnih podatkov in stanje v arhivu.

6.2.2 Izdaja internega akta s strani vodje stalnega predstavništva

Služba za tajne podatke mora v zadnji fazi uvedbe modela organiziranosti pripraviti interni akt, ki določa:

- tajne podatke stopnje tajnosti ZAUPNO oziroma CONFIDENTIEL UE morajo prejemniki po obdelavi izven varnostnega območja II. stopnje (čitalnica) vrniti Službi za tajne podatke;
- po končanem delu je treba sprazniti delovne površine (upoštevati načelo prazne mize), vse dokumente je potrebno zakleniti v pisarniške ali kovinske omare (dovoljena je hramba tajnih podatkov stopnje tajnost INTERNO oziroma RESTREINT UE) in zakleniti pisarniški prostor;
- prejemniki morajo voditi pisno evidenco o prejetih tajnih podatkih stopnje tajnosti INTERNO oziroma RESTREINT UE z navedeno številko in datumom tajnega podatka;
- v kolikor prejemnik tajnega podatka kljub pozivu Službe za tajne podatke po elektronski pošti ne prevzame v roku 14 dni in ni odsoten z dela, se mu ukine distribuiranje tajnih podatkov do preklica službe; služba prejemniku ponovno prične distribuirati tajne podatke, ko ji prejemnik predloži pisno soglasje ali soglasje dano po elektronski pošti s strani vodje stalnega predstavništva;
- vsi prejemniki se opozorijo, da jih organ lahko napoti na vmesno varnostno preverjanje, če bodo s tajnimi podatki ravnali malomarno, kar lahko pomeni zavrnitev izdaje dovoljenja za dostop do tajnih podatkov in s tem prenehanje delovnega razmerja;
- Služba za tajne podatke mora vodji stalnega predstavništva mesečno poslati seznam dolžnikov tajnih podatkov z navedbo datuma prevzema tajnega podatka in
- Služba za tajne podatke mora redno obveščati vodjo stalnega predstavništva o vseh protipravnih ravnanjih s tajnimi podatki (nepooblaščeno kopiranje tajnih podatkov ipd.).

Interni akt mora podpisati vodja stalnega predstavništva, ki se ga nato objavi na oglasni deski v programu Lotus Notes in pošlje po elektronski pošti vsem zaposlenim.

6.3 PREDNOSTI DELOVANJA Z MODELOM ORGANIZIRANOSTI

6.3.1 Prednosti v Službi za tajne podatke

Model organiziranosti izboljša organizacijo delovnih procesov pri delu s tajnimi podatki, poveča varnost dela s tajnimi podatki in zmanjša materialne stroške Službi za tajne podatke.
Obdelava tajnih podatkov v službi z novim modelom organiziranosti prinaša naslednje prednosti:

- prejetemu tajnemu podatku se hitreje določi osebe, ki imajo potrebo do vedenja, na podlagi sprejete distribucijske liste (zmanjša se branje tajnih podatkov, da bi se ugotovilo osebe, ki imajo potrebo do vedenja);
- število kopij tajnega podatka se izdela v skladu z distribucijsko listo z upoštevanjem načela potrebe po vedenju (zmanjša se število prejemnikov tajnih podatkov, s tem se zmanjša tudi število kopij tajnega podatka);
- tajni podatki se kopirajo s tiskalnikom ali fotokopirnim strojem na pripravljene predloge, ki vsebujejo prednatisnjene odebeljene barvne znake o stopnji tajnosti in številke kopij (s tem se poveča varnost pri delu s tajnimi podatki, lažje arhiviranje podatkov in zmanjša možnost mešanja tajnih podatkov različnih stopenj tajnosti zaradi vizualnega aspekta, saj je tajnost podatka in številka kopije vidna iz večje oddaljenosti);
- računalniška evidenca zmanjša čas evidentiranja tajnih podatkov (manjše število zapisov) in omogoči natančno evidenco tajnih podatkov s funkcijo takojšnje pridobitve želenih podatkov po različnih iskalnih kriterijih (na primer iskanje tajnega podatka po številki, datumu, prejemniku; prikaz osebe, ki je na prvem mestu po številu nevrnjenih tajnih podatkov ipd.) in
- zmanjšanje kopiranja tajnih podatkov zaradi nesprejemanja tajnih podatkov v čitalnici.

6.3.2 Povečanje odgovornosti diplomatov pri delu s tajnimi podatki

Interni akt vodje stalnega predstavništva poveča odgovornost diplomatov pri delu s tajnimi podatki:

- zmanjšanje števila iznosov tajnih podatkov iz varnostnega območja II. stopnje (čitalnica); povečanje branja tajnih podatkov v čitalnici;
- upoštevanje načela prazne mize in s tem zmanjšanje možnosti založitve tajnega podatka;
- evidenca diplomatov o tajnih podatkih omogoča tudi hitrejše komisijsko uničenje tajnih podatkov;
- povečanje prevzema tajnih podatkov s strani diplomatov;
- zmanjša se protipravno kopiranje tajnih podatkov in

- vodja stalnega predstavništva je tekoče obveščen o dolžnikih tajnih podatkov in o vseh protipravnih ravnanjih pri delu s tajnimi podatki, pri čemer lahko sprejme ustrezne ukrepe.

6.4 MOŽNOST VZPOSTAVITVE MODELA ORGANIZIRANOSTI OB UPOŠTEVANJU PREDPISOV SVETA O VAROVANJU TAJNOSTI

Predpisi Sveta določajo, da je potrebno evidentirati tajne podatke EU stopnje tajnosti CONFIDENTIEL UE ali višje (PSVT, 6. odstavek, oddelek VII). Pri obdelavi tajnih podatkov stopnje tajnosti RESTREINT UE ni potrebno voditi evidence o tajnih podatkih. Glede na to, da je večina tajnih podatkov EU stopnje tajnosti RESTREINT UE, Služba za tajne podatke porabi preko 90 odstotkov časa za obdelavo omenjenih tajnih podatkov.

Če ne bi bili sprejeti Uredba o varovanju tajnih podatkov in Uredba o upravnem poslovanju, bi lahko Služba za tajne podatke neposredno uporabljala Predpise Sveta. V Službi za tajne podatke bi bila lahko zaposlena le ena oseba.

V starejših parlamentarnih demokracijah je poudarek na zaupanju pri ravnanju s tajnimi podatki, t. j. prenos tajnih podatkov iz roke v roko brez evidentiranja tajnih podatkov nižjih stopenj tajnosti (t. i. gentlemanski sistem). V državah z daljšo demokratično tradicijo je načelo tajnosti natančno zakonsko regulirano (Brezovšek in Črnčec, 2004, str. 507). V novih državah članicah Evropske unije, ki prihajajo iz bivšega komunističnega vzhodnega dela Evrope, pri delu s tajnimi podatki uporabljajo zaprt in strog sistem, kjer ne velja načelo zaupanja. Če je delovanje organov zaprto, je veliko več možnosti za nepravilnosti, zlorabo oblasti in različne oblike korupcije (Rovšek v: Henigman, 2007, str. 173).

7 INFORMACIJSKA PODPORA MODELU ORGANIZIRANOSTI SLUŽBE ZA TAJNE PODATKE

Obdelavo tajnih podatkov z modelom organiziranosti je možno podpreti in nadgraditi s pomočjo informacijske tehnologije v smeri hitrejšega in varnejšega prenosa tajnih podatkov, s čimer bi se:

- prejemnikom tajnih podatkov na stalnem predstavništvu olajšalo delo s tajnimi podatki;
- Službi za tajne podatke stalnega predstavništva olajšalo delo priprave, distribucije in hranjenja tajnih podatkov;
- Službi za tajne podatke Ministrstva za zunanje zadeve Republike Slovenije distribuiralo tajne podatke po načelu "v trenutku" (angl. "just in time").

Za izgradnjo in posodobitev informacijskega sistema bi bilo potrebno sodelovanje:

- Službe za tajne podatke stalnega predstavništva in Ministrstva za zunanje zadeve,
- Službe za informacijsko tehnologijo stalnega predstavništva in Ministrstva za zunanje zadeve (v okviru službe na ministrstvu delujejo strokovnjaki, pristojni za INFOSEC),
- Varnostno tehnične službe stalnega predstavništva in Ministrstva za zunanje zadeve in
- Finančno računovodske službe stalnega predstavništva in Ministrstva za zunanje zadeve.

Razvoj informacijsko tehnološkega sistema v Službi za tajne podatke predstavlja kompleksen projekt, kjer je potrebno sodelovanje večjega števila oseb z različnih delovnih področij (angl. brainstorming) in kjer lahko z idejami pomagajo tudi laiki (Bwiti bvba, 2009).

Pri razvoju in izgradnji sistema je treba upoštevati (Urad Vlade Republike Slovenije za varovanje tajnih podatkov, 2009):

- za osebno varnost (tajne podatke lahko prejmejo le osebe, ki imajo veljavno dovoljenje za dostop do tajnih podatkov in potrebo do vedenja),
- za fizično varnost (tajni podatke se varujejo v skladu s fizičnimi, organizacijskimi in tehnološkimi ukrepi varovanja),
- za dokumentacijsko varnost (tajni podatki se lahko obdelujejo in hranijo v skladu s pravnimi predpisi, zagotovljena mora biti njihova sledljivost in onemogočen dostop nepooblaščenih oseb) in
- za informacijsko varnost (INFOSEC):
  - računalniška varnost (COMPUSEC) in
  - komunikacijska varnost (COMSEC):

- varnost prenosnih sistemov (TRANSSEC),
- varnost kriptografskih metod in naprav (CRYPTOSEC) in
- varnost pri elektromagnetnem sevanju elektronskih naprav (EMSEC).

Izgradnja in posodobitev informacijsko tehnološkega sistema srednjeročno ne bi predstavljala večjih stroškov za stalno predstavništvo v primerjavi s stroški, ki nastajajo v zvezi s sedanjo neustrezno (zaprto) ureditvijo poslovanja s tajnimi podatki.

Računalniki in informatika prinašajo človeštvu neslutene možnosti in težko predvidljiv razvoj, hkrati pa tudi nič manjše nevarnosti za omejevanje in ogrožanje njegovih svoboščin ter za povečan nadzor nad njegovo zasebnostjo oziroma možnost zlorabe (Miklavčič, 2001, str. 124).

7.1 IZGRADNJA INFORMACIJSKO TEHNOLOŠKEGA SISTEMA V SLUŽBI ZA TAJNE PODATKE

Informacijsko podprt model organiziranosti Službe za tajne podatke se vzpostavi:

- za elektronsko evidentiranje tajnih podatkov,
- za distribucijo tajnih podatkov zaposlenim po elektronski poti,
- za elektronsko arhiviranje tajnih podatkov in
- za prenos tajnih podatkov Službi za tajne podatke Ministrstva za zunanje zadeve.

Informacijsko tehnološki sistem je namenjen izboljšanju obdelave tajnih podatkov na stalnem predstavništvu, elektronskemu pretoku tajnih podatkov na relaciji Bruselj-Ljubljana-Bruselj (t. i. elektronska kurirska služba) in zmanjšanju materialnih stroškov stalnega predstavništva.

Za vzpostavitev, vodenje in vzdrževanje sistema predstojnik organa imenuje upravljalca sistema (UVTPKIS, 2. člen), ki mora pred pričetkom delovanja sistema pripraviti (UVTPKIS, 5. člen):

- načrt varovanja sistema z opisom in načrtom sistema, varnostnimi zahtevami sistema, varnostnimi okolji, varnostnimi protiukrepi in varnostnim upravljanjem sistema;
- oceno varnostnih tveganj z oceno stanja sistema in z oceno stopnje tveganja in
- varnostna navodila za delo v sistemu z varnostnim upravljanjem in organiziranostjo varnosti sistema, informacijsko varnostjo, načrtovanjem ukrepov ob nepredvidenih dogodkih, upravljanjem in spreminjanjem nastavitve sistema, splošnimi varnostnimi navodili za uporabnike in odgovorne osebe.

Za upravljanje in nadzor nad ukrepi in postopki varovanja tajnih podatkov v sistemu je odgovoren vodja informacijske varnosti, ki ga imenuje predstojnik organa. V dislocirani

enoti organa se imenuje lokalni vodja informacijske varnosti. Naloge (lokalnega) vodje informacijske varnosti lahko opravlja predstojnik organa oziroma predstojnik dislocirane enote (UVTPKIS, 9. člen). Informacijski sistem je lahko tarča terorističnega napada z informacijskimi orodji, katerega cilj je onesposobitev sistema (Belič, 2001, str. 263).
Ob vsakem posegu v varnostnem območju I. stopnje je potrebno opraviti protiprisluškovalni pregled zaradi zaščite pred poskusi prisluškovanja (UVTP, 18. člen).

Informacijsko tehnološki sistem se vzpostavi v treh fazah.

7.1.1 Prva faza izgradnje informacijsko tehnološkega sistema

V prvi fazi izgradnje informacijsko tehnološkega sistema lahko informatiki stalnega predstavništva s sodelovanjem Službe za tajne podatke hitro (v roku enega tedna) in brez večjih stroškov izvedejo naslednje ukrepe:

- nakup dveh optičnih bralnikov,
- izbira rabljenih delovnih postaj (osebni računalniki), ki so arhivirane na stalnem predstavništvu,
- nakup optičnega kabla,
- izdelava računalniškega programa in
- vzpostavitev varnostnega območja II. stopnje (čitalnica) v vsakem nadstropju stalnega predstavništva.

V Službi za tajne podatke (varnostno območje I stopnje) se namesti delovna postaja (na postajo se priključi optični bralnik), ki se jo poveže po varnih vodih, ki so zaščiteni proti neželenemu elektromagnetnemu sevanju (tempest), z ostalimi delovnimi postajami, ki se jih namesti v varnostnih območjih II. stopnje (čitalnice); vsako nadstropje ima eno čitalnico, v kateri se nahaja delovna postaja.

7.1.2 Druga faza izgradnje informacijsko tehnološkega sistema

Postopki druge faze izgradnje informacijsko tehnološkega sistema so najbolj enostavni in najcenejši v primerjavi s postopki prve in tretje faze. Informatiki stalnega predstavništva:

- izdelajo ustrezen program za Lotus Notes v okviru obstoječega informacijskega omrežja na stalnem predstavništvu (nadgradnja sistema) in
- povežejo delovne postaje, ki jih uporabljajo zaposleni v Službi za tajne podatke, z optičnim bralnikom.

Za tehnično podporo programu Lotus Notes v državni upravi je zadolženo podjetje SRC d. o. o. iz Ljubljane, kar je iz varnostnega vidika sporno. V podjetju SRC d. o. o. imajo pregled nad vsemi (sic!) podatki organov državne uprave, ki se obdelujejo s programom Lotus Notes (tudi nad tajnimi podatki).

7.1.3 Tretja faza izgradnje informacijsko tehnološkega sistema

Prenos tajnih podatkov med Službama za tajne podatke na stalnem predstavništvu in na Ministrstvu za zunanje zadeve je najbolj zahtevna naloga, pri kateri mora sodelovati največ strokovnjakov iz obeh služb za tajne podatke, iz obeh služb za informacijsko tehnologijo (strokovnjaki za INFOSEC), iz obeh varnostno tehničnih služb in strokovnjakov s področja kriptografije (šifriranje in dešifriranje tajnih podatkov).

Za šifriran prenos tajnih podatkov med službama je potrebno:

- izdelati informacijski program za prenos tajnih podatkov;
- zakupiti telefonsko linijo med službama za 24 ur na dan in za vse dni v letu;
- kupiti dve delovni postaji;
- kupiti dva optična bralnika in
- kupiti dva tiskalnika.

Delovni postaji se namesti v varnostni območji I. stopnje obeh služb za tajne podatke, poveže z zakupljeno telefonsko linijo in poveže z optičnima bralnikoma in tiskalnikoma.

Pred začetkom delovanja sistema mora Urad Vlade Republike Slovenije za varovanje tajnih podatkov opraviti varnostni pregled informacijsko tehnološkega sistema, po pregledu pa lahko predstojnik organa izda sklep o varnostni odobritvi sistema (UVTPKIS, 4. člen).

7.2 IMPLEMENTACIJA INFORMACIJSKO TEHNOLOŠKEGA SISTEMA

7.2.1 Elektronska distribucija tajnih podatkov do stopnje tajnosti TAJNO oziroma SECRET UE

Služba za tajne podatke lahko distribuira tajne podatke do stopnje tajnosti TAJNO oziroma SECRET UE prejemnikom tajnih podatkov do delovnih postaj v čitalnicah stalnega predstavništva (varnostna območja II. stopnje) s sistemom dvojnega selektivnega delovanja. V vsakem nadstropju stalnega predstavništva je vzpostavljeno eno varnostno območje II. stopnje (čitalnica). Sistem je namenjen osebam s pravico vpogleda v tajne podatke na podlagi različnih potreb do vedenja (UVTPKIS, 6. člen).

Prenos tajnih podatkov stopnje tajnosti TAJNO oziroma SECRET UE je zasnovan na naslednji način:

- Služba za tajne podatke prejme tajne podatke do stopnje tajnosti TAJNO oziroma SECRET UE v papirnati obliki (angl. hard copy) ali na pomnilniških medijih (na primer zgoščenka);

- tajni podatki se obdelajo z optičnim bralnikom in shranijo na trdi disk delovne postaje v I. varnostnem območju;
- tajni podatki se v elektronski obliki (formati *.tiff, *.doc, *.pdf, *.jpg ipd.) distribuirajo osebam na podlagi distribucijske liste, ki jo vsebuje program, glede na kratice delovnega področja Sveta in potrebe po vedenju;
- prejemnike služba obvesti o prispelem tajnem podatku po elektronski pošti;
- tajne podatke lahko prejemniki obdelujejo v varnostnih območjih II. stopnje na delovnih postajah (čitalnica);
- prejemniki lahko zaprosijo Službo za tajne podatke za kopijo tajnega podatka v papirnati obliki;
- program avtomatsko barvno natisne diagonalno stopnjo tajnosti in številko kopije tajnega podatka in
- v sistemu se vodi elektronska evidenca vpogledov v tajne podatke.

7.2.2 Elektronska distribucija tajnih podatkov stopnje tajnosti INTERNO oziroma RESTREINT UE

Glede na to, da je številčno največ tajnih podatkov stopnje tajnosti INTERNO oziroma RESTREINT UE, distribucija teh tajnih podatkov do delovnih postaj zaposlenih najbolj olajša delo prejemnikom tajnih podatkov in Službi za tajne podatke.

Služba za tajne podatke prejme tajne podatke stopnje tajnosti INTERNO oziroma RESTREINT UE v papirnati obliki ali na pomnilniškem mediju. Distribucija tajnih podatkov med zaposlene se opravi na naslednje načine:

- tajne podatke zaposleni v Službi za tajne podatke na svojih delovnih postajah, kjer je dovoljeno uporabljati internet (UVTPKIS, 16. člen), obdelajo z optičnim bralnikom in jih vnesejo v obstoječ in nadgrajen sistem programa Lotus Notes, katerega uporabljajo vsi zaposleni na stalnem predstavništvu;[35]
- prejemnike se o prispelih tajnih podatkih ne obvesti več po elektronski pošti, saj za to ni potrebe;
- prejemniki na svojih delovnih postajah lahko obdelujejo tajne podatke (v vseh pisarnah stalnega predstavništva);
- prejemniki lahko zaprosijo Službo za tajne podatke za izdelavo kopije tajnega podatka v papirnati obliki;
- program avtomatsko barvno natisne diagonalno stopnjo tajnosti in številko kopije tajnega podatka in
- v programu Lotus Notes se vodi elektronska evidenca vpogledov v tajne podatke.

[35] V Republiki Sloveniji uporabljajo program Lotus Notes vsi organi državne uprave.

7.2.3 Elektronski prenos tajnih podatkov Službi za tajne podatke Ministrstva za zunanje zadeve Republike Slovenije

Prenos tajnih podatkov Službi za tajne podatke Ministrstva za zunanje zadeve lahko poteka s pomočjo:

- kurirske službe,
- kriptografskih naprav (kriptotelefaks) in
- informacijsko tehnološkega sistema.

Z informacijsko tehnološkim sistemom se lahko prenaša tajne podatke do stopnje tajnosti TAJNO oziroma SECRET UE.

Prenos tajnih podatkov iz ene službe v drugo poteka v naslednjih fazah:

- tajne podatke v papirnati ali v elektronski obliki se vnese v sistem na delovni postaji z optičnim bralnikom ali s pomnilniškim medijem (na primer zgoščenka);
- vodi se elektronska evidenca o prenosu tajnih podatkov (datum in čas prenosa, evidenčna številka tajnega podatka in stopnja tajnosti) in
- prejemnik tajnih podatkov jih lahko natisne ali pa shrani na pomnilniški medij (na primer USB-ključ).

7.3 PRIKAZ PREDNOSTI DELA Z INFORMACIJSKO TEHNOLOŠKIM SISTEMOM

7.3.1 Prednosti elektronske distribucije tajnih podatkov do stopnje tajnosti TAJNO oziroma SECRET UE

Elektronska distribucija tajnih podatkov do stopnje tajnosti TAJNO oziroma SECRET UE poteka do delovnih postaj v čitalnicah stalnega predstavništva (varnostna območja II. stopnje). Prednosti elektronske distribucije tajnih podatkov so:

- vodenje elektronske evidence zmanjša evidentiranje tajnih podatkov v delovodnikih;
- v delovodnikih se evidentirajo tajni podatki le v primeru, ko prejemnik zahteva izdelavo kopije tajnega podatka v fizični obliki; takrat je potrebno k tajnemu podatku pripeti tudi eventualen seznam vpogledov;
- zmanjša se fotokopiranje tajnih podatkov, kar zmanjša porabo papirja in arhiviranje tajnih podatkov, iz dveh razlogov:
  - tajni podatki se nahajajo v elektronski obliki (kopije niso izdelane več v fizični obliki) in
  - prejemnik si tajne podatke prebere v elektronski obliki (ni nujno, da prejemnik naroči izdelavo kopije v elektronski obliki);

- prejemnikom tajnih podatkov ni potrebno hoditi v čitalnico Službe za tajne podatke, saj si lahko tajne podatke preberejo v čitalnici, ki se nahaja v istem nadstropju stalnega predstavništva, kjer imajo pisarno; in
- poveča se sledljivost tajnih podatkov.

7.3.2 Prednosti elektronske distribucije tajnih podatkov do stopnje tajnosti INTERNO oziroma RESTREINT UE

Ker je največje število tajnih podatkov stopnje tajnosti INTERNO oziroma RESTREINT UE, prinaša elektronska distribucija tajnih podatkov omenjene stopnje tajnosti največ ugodnosti prejemnikom tajnih podatkov, saj na svojih delovnih postajah lahko ažurno prejemajo tajne podatke (takoj, ko jih v informacijsko tehnološki sistem vnese Služba za tajne podatke). Službam za tajne podatke ni potrebno več prekomerno kopirati in arhivirati tajnih podatkov stopnje tajnosti INTERNO oziroma RESTREINT UE.

Elektronska distribucija tajnih podatkov stopnje tajnosti INTERNO oziroma RESTREINT UE prinaša naslednje prednosti:

- vodi se le še elektronska evidenca tajnih podatkov (delovodniki se odpravijo);
- prejemnike tajnih podatkov ni potrebno več obveščati o prispetju tajnega podatka, saj lahko na svojih delovnih postajah obdelujejo tajne podatke;
- odpravi se več kot 90 odstotkov dela Službe za tajne podatke (evidentiranje v delovodnike, kopiranje tajnih podatkov, razvrščanje in urejanje tajnih podatkov ob vračilu prejemnikov ter arhiviranje tajnih podatkov) in
- povečanje sledljivosti tajnih podatkov.

Prejemniki tajnih podatkov lahko zaprosijo Službo za tajne podatke za izdelavo kopije tajnega podatka v papirnati obliki.

7.3.3 Prednosti elektronskega prenosa tajnih podatkov Službi za tajne podatke Ministrstva za zunanje zadeve Republike Slovenije

Informacijsko tehnološki sistem pri prenosu tajnih podatkov med službama za tajne podatke na stalnem predstavništvu in na Ministrstvu za zunanje zadeve odpravi potrebo po kurirski službi. Hitrost prenosa tajnih podatkov ni več odvisna od hitrosti dela kurirske službe, ampak od hitrosti vnosa tajnih podatkov v sistem in od hitrosti prenosa podatkov po zakupljeni telefonski liniji, kar pomeni ažurno distribucijo tajnih podatkov. V sistemu se vodi elektronska evidenca distribucije tajnih podatkov.

Informacijsko tehnološki sistem odpravi:

- pripravo tajnih podatkov, namenjeno kurirskemu prenosu (kopiranje tajnih podatkov in izdelava seznama tajnih podatkov);

- vodenje delovodnikov;
- plombiranje ovojnice;
- izdelavo kurirskega pisma (angl. courier letter);
- izdelavo pooblastila za prenos tajnih podatkov in
- stroške za potovanje kurirja (dnevnice, nastanitev, letalske karte oziroma stroški za gorivo osebnega vozila ipd.).

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih in Predpisi Sveta o varovanju tajnosti dopuščajo prenos tajnih podatkov stopnje tajnosti STROGO TAJNO oziroma TRÈS SECRET UE/EU TOP SECRET znotraj oziroma zunaj varnostnih območij po komunikacijskih in informacijskih sistemih, vendar je glede na občutljivost teh podatkov in glede na to, da so maloštevilni, primernejši fizični prenos z uporabo čitalnice oziroma s pomočjo kurirske službe.

8 URESNIČENI CILJI OZIROMA DOSEŽKI RAZISKAVE

V specialističnem delu sem z raziskovanjem uresničil naslednje cilje oziroma dosežke raziskave:

- opravljena je analiza in primerjava obstoječih pravnih predpisov Republike Slovenije in Evropske unije s področja varovanja tajnih podatkov;
- prikazana je ustanovitev Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju z opisom vseh postopkov in ukrepov;
- opisane so težave in pomanjkljivosti pri delu s tajnimi podatki v službi (ročno evidentiranje tajnih podatkov v osem delovodnikov; prekomerno kopiranje in distribucija tajnih podatkov; zasedenost blagajn; počasnost distribucije tajnih podatkov diplomatom; prenos tajnih podatkov Službi za tajne podatke Ministrstva za notranje zadeve poteka po kurirski službi);
- zasnovan je model organiziranosti in prikazane so možne rešitve za izboljšanje delovanja službe;
- prikazano je delovanje službe z modelom organiziranosti;
- razvit je informacijsko tehnološki sistem v Službi za tajne podatke, ki predstavlja nadgradnjo modela organiziranosti; in
- prikazano je delovanje službe z informacijsko tehnološkim sistemom.

Implementacija modela organiziranosti Službe za tajne podatke delno izboljša delo s tajnimi podatki. Izdelava distribucijske liste zmanjša število prejemnikov tajnih podatkov, kar zmanjša tudi kopiranje in arhiviranje tajnih podatkov. Služba za tajne podatke s pomočjo distribucijske liste hitreje določi upravičene osebe za dostop do tajnih podatkov (tajni podatki se distribuirajo prejemnikom z uporabo kratic Sveta Evropske unije; zmanjša se distribucija tajnih podatkov na način, da je potrebno tajni podatek prebrati in potem določiti upravičeno osebo do tajnega podatka). Poveča se tudi sledljivost tajnih podatkov zaradi uporabe prednatisnjene predloge z oznakama stopnje tajnosti in številke kopije tajnega podatka. Elektronska evidenca zmanjša čas evidentiranja tajnih podatkov in omogoča hitrejše iskanje tajnih podatkov po različnih iskalnih kriterijih. Interni akt vodje stalnega predstavništva poveča odgovornost pri delu s tajnimi podatki, saj se zaposleni seznanijo s posledico malomarnega in nevestnega dela s tajnimi podatki (prenehanje delovnega razmerja).

Informacijsko tehnološki sistem izboljša obdelavo tajnih podatkov (povečanje hitrosti distribucije, dostopnosti in prenosa tajnih podatkov; zmanjšanje evidentiranja, kopiranja in arhiviranja tajnih podatkov; zmanjšanje materialnih stroškov stalnega predstavništva). Prenos in arhiviranje tajnih podatkov poteka v celoti po elektronski poti. Elektronska evidenca zmanjša obseg evidentiranja tajnih podatkov.

Pri pisanju specialističnega dela sem pazil, da ne bi podrobno razkril sistem delovanja Službe za tajne podatke in s tem kršil pravne predpise s področja varovanja tajnih podatkov.

9 PREVERITEV HIPOTEZ

V uvodu specialističnega dela sem postavil tri hipoteze, ki jih bom v nadaljevanju pojasnil in jih na podlagi raziskovanja potrdil oziroma ovrgel:

- **Prva hipoteza:**

Obstoječa organiziranost Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju predstavlja težave pri poslovanju s tajnimi podatki.

Služba za tajne podatke evidentira tajne podatke ročno v osem delovodnikov, pri čemer je potrebno zapisati v delovodnike za vsak tajni podatek več kot deset podatkov. Tajni podatki se distribuirajo vsem! prejemnikom, ki delajo na določenem delovnem področju, čeprav nimajo potrebe po vedenju (angl. need to know). Zasnova modela organiziranosti Službe za tajne podatke uvede elektronsko evidenco tajnih podatkov, ki zmanjša število vnosov pri evidentiranju tajnih podatkov in olajša iskanje tajnih podatkov po različnih iskalnih kriterijih. Uvedba distribucijske liste, s pomočjo katere se tajni podatki distribuirajo na podlagi potrebe po vedenju, zmanjša kopiranje in arhiviranje tajnih podatkov. Izdaja internega akta s strani vodje stalnega predstavništva poveča odgovornost zaposlenih na stalnem predstavništvu pri delu s tajnimi podatki zaradi seznanitve z neustreznim delom s tajnimi podatki, ki lahko pripelje do prekinitve delovnega razmerja. Zaradi prikazane odprave organizacijskih ovir je prva hipoteza potrjena.

- **Druga hipoteza:**

Adekvatna informacijska podpora Službi za tajne podatke bi izboljšala poslovanje s tajnimi podatki.

Model organiziranosti Službe za tajne podatke delno odpravi težave pri poslovanju s tajnimi podatki, skoraj v celoti pa jih odpravi informacijsko tehnološki sistem službe. V informacijski sistem se pri evidentiranju tajnih podatkov ročno vnese manjše število potrebnih podatkov. Tajne podatke se vnese v sistem s pomočjo optičnega bralnika. Takoj po vnosu tajnih podatkov v sistem, imajo do tajnih podatkov dostop prejemniki na stalnem predstavništvu in Služba za tajne podatke Ministrstva za zunanje zadeve. Vnosi tajnih podatkov v sistem in dostopi prejemnikov v sistem pri branju tajnih podatkov se elektronsko evidentirajo. Vnos tajnih podatkov v sistem pomeni tudi elektronsko arhiviranje tajnih podatkov. Odpravijo se vpisi prejemnikov tajnih podatkov v delovodnike, kopiranje tajnih podatkov v papirnati obliki in kurirska služba za prenos tajnih podatkov. Z informacijsko tehnološkim sistemom se zmanjšajo tudi materialni stroški stalnega predstavništva. Navedeni postopki potrjujejo drugo hipotezo.

- **Tretja hipoteza:**

Pravni predpisi Republike Slovenije s področja varovanja tajnih podatkov otežujejo dostop do tajnih podatkov in delo s tajnimi podatki.

Nekateri pravni predpisi Republike Slovenije s področja varovanja tajnih podatkov določajo, da imajo dostop do tajnih podatkov osebe z dovoljenjem za dostop do tajnih podatkov in se morajo s temi podatki seznaniti zaradi "opravljanja funkcije ali delovnih nalog". V praksi to pomeni, da se tajni podatki distribuirajo vsem! osebam, ki opravljajo "funkcijo ali delovne naloge". Zaradi tega prihaja do prekomerne distribucije tajnih podatkov, kar prinaša dodatne probleme (povečan obseg evidentiranja, kopiranja in arhiviranja tajnih podatkov). Predpisi Sveta o varovanju tajnosti olajšajo delo s tajnimi podatki, saj se tajni podatki distribuirajo po načelu potrebe po vedenju (angl. need to know), ki je eno od temeljnih načel pri delu s tajnimi podatki in po katerem se distribuirajo tajni podatki ožjemu številu oseb. Uvedba distribucijske liste in informacijsko tehnološkega sistema v Službi za tajne podatke omogočata distribucijo tajnih podatkov po načelu potrebe po vedenju. Uredba o varovanju tajnih podatkov določa, da je potrebno evidentirati vsak tajni podatek. V skladu s Predpisi Sveta o varovanju tajnosti tajnih podatkov najnižje stopnje tajnosti RESTREINT UE (INTERNO) ni potrebno evidentirati. Glede na to, da je več kot 95 odstotkov tajnih podatkov najnižje stopnje tajnosti, evidentiranje teh tajnih podatkov otežuje delo s tajnimi podatki. Z uvedbo elektronskega evidentiranja tajnih podatkov in informacijsko tehnološkega sistema v Službi za tajne podatke se evidentira manj podatkov, kar izboljša delo s tajnimi podatki. Glede na navedeno, je potrjena tudi tretja hipoteza.

10 PRISPEVEK REZULTATOV RAZISKAVE K STROKI

V specialističnem delu sem prikazal načine izboljšanja dela s tajnimi podatki v Službi za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji, kjer največjo oviro predstavljata fizična obdelava tajnih podatkov (ročno evidentiranje tajnih podatkov v osem delovodnikov, distribucija tajnih podatkov po načelu opravljanja dela, prekomerno kopiranje in arhiviranje tajnih podatkov) in prenos tajnih podatkov s kurirsko službo.

Z zasnovanim modelom organiziranosti Službe za tajne podatke je prikazana rešitev izboljšanega poslovanja s tajnimi podatki, kjer se uvedeta elektronsko evidentiranje tajnih podatkov in distribucijska lista, s katero se tajni podatki distribuirajo prejemnikom po načelu potrebe po vedenju (angl. need to know), s čimer se delno odpravijo težave pri poslovanju s tajnimi podatki.

Informacijska podpora modelu organiziranosti Službe za tajne podatke predstavlja izgradnjo in implementacijo informacijsko tehnološkega sistema v Službi za tajne podatke. Informacijsko tehnološki sistem izboljša delo s tajnimi podatki prejemnikom tajnih podatkov in obema službama za tajne podatke na stalnem predstavništvu in na Ministrstvu za zunanje zadeve. Poveča se hitrost distribucije, dostopnost in sledljivost tajnih podatkov, zmanjša se evidentiranje, kopiranje in arhiviranje tajnih podatkov. Prenos tajnih podatkov med službama za tajne podatke poteka po elektronski poti (odpravi se kurirska služba). Informacijsko tehnološki sistem zmanjša tudi materialne stroške stalnega predstavništva.

11 UPORABNOST REZULTATOV RAZISKAVE

Rezultate raziskave predstavljajo novi postopki in metode dela pri poslovanju s tajnimi podatki v Službi za tajne podatke v okviru novega modela organiziranosti službe skupaj z nadgradnjo modela z informacijsko tehnološkim sistemom.

Rezultate raziskave bo lahko v okviru svojih pristojnosti uporabil Urad Vlade Republike Slovenije za varovanje tajnih podatkov s pomočjo strokovnjakov s področja tajnih podatkov in varnostno tehničnih služb, ki so usposobljeni za osebno, fizično, dokumentacijsko in informacijsko varnost. Urad lahko pomaga službam za tajne podatke pri posodobitvi sistema dela s tajnimi podatki (SUNOUVRSVTP, 2. člen).

V službah za tajne podatke se lahko vzpostavijo informacijsko tehnološki sistemi, ki bi informacijsko podprli obstoječe modele organiziranosti ter odpravili fizično obdelavo tajnih podatkov.

S predlaganim informacijsko tehnološkim sistemom, postopki in metodami pri poslovanju s tajnimi podatki bi se povečala ažurnost pri pridobitvi in prenosu tajnih podatkov, stroški poslovanja organov bi se zmanjšali, zmanjšalo bi se fizično delo v službah za tajne podatke, omogočena bi bila večja sledljivost tajnih podatkov, uvedeno bi bilo elektronsko evidentiranje in elektronsko arhiviranje tajnih podatkov. Prenos tajnih podatkov bi lahko potekal po elektronski poti (elektronska kurirska služba).

12 ZAKLJUČEK

V gospodarskem in političnem življenju se bije konkurenčen boj, kjer zmaga tisti, ki ima prednost pred nasprotnikom. Imeti prednost pred nasprotnikom, pomeni imeti potrebne informacije, ki jih je potrebno varovati. Razkritje določenih informacij bi lahko povzročilo škodo, kar pomeni, da jih je potrebno tudi ustrezno klasificirati. Take informacije imenujemo tajni podatki.

V specialističnem delu sem prikazal predpise Republike Slovenije in Evropske unije s področja varovanja tajnih podatkov in jih med seboj primerjal. Nacionalni predpisi bolj strogo obravnavajo tajne podatke v primerjavi s predpisi Evropske unije, saj je potrebno evidentirati tudi tajne podatke najnižje stopnje tajnosti, kar otežuje delo s tajnimi podatki tako prejemnikom tajnih podatkov kot tudi službam za tajne podatke. Druga slabost je preobsežna distribucija tajnih podatkov prejemnikom v skladu z nacionalnimi predpisi, saj je vezana na t. i. načelo "opravljanja dela". Po pravnih predpisih Evropske unije poteka distribucija tajnih podatkov glede na potrebo po vedenju osebe, kar je ožji pojem kot "opravljanje dela".

Nadalje sem prikazal postopek ustanovitve Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije v Bruslju s težavami, ki so se pojavljale, in možnosti za odpravo teh težav.

Zasnoval sem model organiziranosti službe za tajne podatke z ustreznimi postopki in ukrepi, ki izboljšajo delo s tajnimi podatki na stalnem predstavništvu. Z uvedbo distribucijske liste prejemajo tajne podatke osebe, ki opravljajo delovne naloge in imajo tudi potrebo po vedenju. Ročno evidenco tajnih podatkov v osmih delovodnikih nadomesti elektronska evidenca tajnih podatkov, ki omogoča ažurno spremljanje tajnih podatkov po več iskalnih kriterijih, hkrati pa zmanjša število fizičnih vnosov v evidenco s strani Službe za tajne podatke.

Informacijska podpora modelu organiziranosti uvede elektronsko poslovanje s tajnimi podatki. Razvil sem informacijsko tehnološki sistem, ki zaposlenim omogoča ažuren dostop do tajnih podatkov na delovnih postajah, hkrati pa zmanjša kopiranje tajnih podatkov ter s tem tudi obseg arhiviranja. Elektronski prenos tajnih podatkov med službama za tajne podatke na stalnem predstavništvu in na Ministrstvu za zunanje zadeve odpravi kurirsko službo na relaciji Ljubljana-Bruselj-Ljubljana, saj prenos tajnih podatkov poteka po zakupljeni telefonski liniji v šifrirani obliki, ki omogoča hiter prenos tajnih podatkov.

Informacijsko tehnološki sistem zmanjša materialne stroške stalnega predstavništva oziroma Ministrstva za zunanje zadeve zaradi zmanjšanja kopiranja tajnih podatkov in odprave kurirske službe. V Službi za tajne podatke bi bila lahko zaposlena le ena oseba.

Postavljene hipoteze, da obstoječa organiziranost Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju predstavlja težave pri poslovanju s tajnimi podatki, da bi adekvatna informacijska podpora Službi za tajne podatke izboljšala poslovanje s tajnimi podatki in da pravni predpisi Republike Slovenije s področja varovanja tajnih podatkov otežujejo dostop do tajnih podatkov in delo s tajnimi podatki, sem potrdil.

Ustrezna informacijska podpora obstoječim modelom organiziranosti služb za tajne podatke v organih državne uprave v Republiki Sloveniji bi izboljšala sistem poslovanja s tajnimi podatki, vendar je to bolj odvisno od volje politikov, Urada Vlade Republike Slovenije za varovanje tajnih podatkov in stroke kot pa od služb za tajne podatke.

LITERATURA IN VIRI

LITERATURA

1. ANTONČIČ, Marjan. Dostop do informacij javnega značaja in tajni podatki. Kaj prinaša novi zakon o dostopu do informacij javnega značaja. Inštitut za javno upravo. Ministrstvo za informacijsko družbo RS. Ministrstvo za notranje zadeve RS. Ljubljana, 2003, str. 88-95.
2. ANTONČIČ, Marjan. Nacionalni sistem varovanja tajnih podatkov: Zakon o tajnih podatkih. Slovenska uprava. 2001, let. 1, št. 2, str. 28-29.
3. ANTONČIČ, Marjan. Zakonska ureditev varstva tajnih podatkov v nekaterih državah, članicah Severnoatlantskega sporazuma. V: BELIČ, Igor (ur.). Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 13-34.
4. ANTONČIČ, Marjan. Zakonska ureditev varstva tajnih podatkov v nekaterih državah, članicah Severnoatlantskega sporazuma. Varstvoslovje. 2001, let. 3, št. 1/2, str. 19-32.
5. ARNEJČIČ, Beno. Tajnost, lojalnost in nacionalna varnost (socialno-psihološki vidiki odnosa posameznika do tajnih podatkov na nacionalnovarnostnem področju). V: BELIČ, Igor (ur.). Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 71-80.
6. ARNEJČIČ, Beno. Tajnost, lojalnost in nacionalna varnost: (socialno-psihološki vidiki odnosa posameznika do tajnih podatkov na nacionalnovarnostnem področju). Varstvoslovje. 2001, let. 3, št. 1/2, str. 49-56.
7. ANŽIČ, Andrej, TRBOVŠEK, Franc. Varnostno preverjanje oseb – omejitev dostopa do tajnih podatkov. Varstvoslovje. 2001, let. 3, št. 1/2, str. 42-48.
8. BAVEC, Cene (ur.). BUČAR, Maja (ur.). Zbornik B 6. mednarodne multi-konference Informacijska družba IS 2003, 13. do 17. oktober 2003. Institut "Jožef Stefan", Ljubljana, 2003, str. 149-150.
9. BELIČ, Igor. Informacijski terorizem. Varstvoslovje. 2001, let. 3, št. 4, str. 262-268.
10. BREZOVŠEK, Marjan, ČRNČEC, Damir. Tajnost v demokraciji. Teorija in praksa. 2004, let. 41, št. 3/4, str. 507-523.
11. BROŽIČ, Liliana. Tajni podatki in NATO. V: PAGON, Milan (ur.). Dnevi varstvoslovja, Visoka policijsko-varnostna šola, Ljubljana, 2002, str. 139.
12. BROŽIČ, Liliana. Varnostno potrdilo kot pogoj za zasedbo delovnega mesta. Kadrovske informacije. 2002, let. 3, št. 7, str. 30-32.
13. BROŽIČ, Liliana. Varnostno preverjanje oseb v Ministrstvu za obrambo (Primerjava preverjanja v ZDA in NATO s preverjanjem v MORS ali zakaj potrebujemo Zakon o tajnih podatkih). V: BELIČ, Igor (ur.). Javna predstavitev

mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 147-161.
14. BROŽIČ, Liliana. Varnostno preverjanje oseb v Ministrstvu za obrambo Republike Slovenije: (primerjava preverjanja v ZDA in NATO s preverjanjem v MORS ali zakaj potrebujemo Zakon o tajnih podatkih). Varstvoslovje. 2001, let. 3, št. 1/2, str. 57-67.
15. ČALETA, Denis. Varnostno preverjanje v Slovenski vojski. Bilten Slovenske vojske. 2003, let. 5, št. 1, str. 9-37.
16. ČALETA, Denis. Varovanje tajnih podatkov v demokratični družbi. Dignitas. 2008, let. 10, št. 37/38, str. 249-271.
17. ČERNETIČ, Metod, BROŽIČ, Liliana. Potrebe po novih znanjih – varovanje tajnih podatkov v Evropski uniji in zvezi NATO. V: RAJKOVIČ, Vladislav (ur.). URBANČIČ, Tanja (ur.). BERNIK, Mojca (ur.). ROZMAN, Ivan (ur.). HERIČKO, Marjan (ur.). VILFAN, Boštjan (ur.). ČERNETIČ, Metod. BROŽIČ, Liliana. Potrebe po novih znanjih – varovanje tajnih podatkov v Evropski uniji in zvezi NATO. Organizacija. 2003, let. 36, št. 8, str. 575-582.
18. ČERNETIČ, Metod, DEČMAN DOBRNJIČ, Olga. Planiranje izobraževanja in menedžment sprememb. V: RAJKOVIČ, Vladislav (ur.). URBANČIČ, Tanja (ur.). BERNIK, Mojca (ur.). Planiranje izobraževanja in menedžment sprememb. Organizacija. Kranj, 2006, let. 39, št. 8, str. 475-481.
19. ČRNČEC, Damir. Dostop do tajnih podatkov in varnostno preverjanje oseb. Varstvoslovje. 2004, let. 6, št. 1, str. 47-58.
20. ČRNČEC, Damir. Nova obveščevalna paradigma in Evropska unija. Varstvoslovje. 2009, let. 11, št. 1, str. 130-163.
21. ČRNČEC, Damir. Obveščevalno varnostna podpora mednarodnim operacijam in misijam. V: BRIC, Roman (ur.). Obveščevalno varnostna podpora mednarodnim operacijam in misijam, Ministrstvo za obrambo RS, Služba za odnose z javnostmi, Brdo pri Kranju, 2009, str. 1-20.
22. FOERSTEL, N. Herbert. Freedom of Information and the Right to Know: The Origins and Applications of the Freedom of Information Act. Greenwood Press, Westport, 1999.
23. GIDIERE, P. Stephen. The federal information manual: how the government collects, manages, and discloses information under FOIA and other statutes. American Bar Association, Chicago, 2006.
24. GOSTIČ, Štefan. Inšpekcijski nadzor. Varnost. 2006, let. 54, št. 1, str. 12-14.
25. GRILC, Peter. Pravo Evropske unije. Cankarjeva založba, Ljubljana, 2001.
26. HENIGMAN, Žarko. Kadrovska varnost – izziv varovanja tajnih podatkov = Personnel security – a challenge to classified information protection. Bilten Slovenske vojske. 2007, let. 9, št. 4, str. 167-186.
27. HUGHES, R. Gerald. Exploring intelligence archives: enquiries into the secret state. Routledge, London, New York, 2008.
28. IVANKO, Štefan. (Kako) napisati strokovno delo (del študijskega gradiva za "Upravni praktikum I"). Visoka upravna šola, Ljubljana, 1995.

29. IVANKO, Štefan. Upravni praktikum I (metodološki seminar o dejavnem in ustvarjalnem sodelovanju pri strokovnem in znanstvenem delu). Visoka upravna šola, Ljubljana, 2003.
30. KEČANOVIĆ, Bećir. Informacijska zasebnost na preizkušnji pri policiji. Pravna praksa. 2002, let. 21, št. 28/29, str. 9-11.
31. KEČANOVIĆ, Bećir. Varnostno preverjanje: policijski poseg v informacijsko zasebnost delavcev. V: BELIČ, Igor (ur.). Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 187-204.
32. KEČANOVIĆ, Bećir. Varnostno preverjanje: policijski poseg v pravice informacijske zasebnosti. Varstvoslovje. 2001, let. 3, št. 1/2, str. 85-94.
33. KOVAČ, Polonca. Izdaja na čas vezanih dovoljenj. Pravna praksa. 2008, let. 27, št. 22, str. 11-13.
34. KRIŽAJ, Marjana. Dostop do javnega arhivskega gradiva v nekaterih državah Evropske unije. Arhivi. 2007, let. 30, št. 1, str. 71-82.
35. KÜRBUS, Vinko. Uradna skrivnost – nesimpatična neizogibnost: vprašanje, ki je v naši državi več kot aktualno. Revija obramba. 2001, let. 33, št. 4, str. 22-25.
36. LALIĆ, Gordana. Varnostno preverjanje po Zakonu o tajnih podatkih. Pravna praksa. 2003, let. 22, št. 6/7, str. 20-22.
37. LUNEŽNIK, Bojan. Nadzor nad izvajanjem Zakona o tajnih podatkih. Slovenska vojska. 2004, let. 12, št. 10, str. 26-27.
38. MEKINA, Igor. Tajnost napada svobodi : državni zbor se pripravlja na sprejem zakona o tajnih podatkih. Mladina. 2001, let. 59, št. 11, str. 24-25.
39. MIKLAVČIČ, Marjan. Varnostno preverjanje oseb kot integracijski del kadrovske funkcije. V: BELIČ, Igor (ur.). Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 117-131.
40. MIKLAVČIČ, Marjan. Varnostno preverjanje oseb kot integracijski del kadrovske funkcije. Varstvoslovje. 2001, let. 3, št. 1/2, str. 95-102
41. MOUNT, Ellis. Top secret/trade secret: accessing and safeguarding restricted information. Neal-Schuman Publishers, New York, 1985.
42. PRAPROTNIK, Rok. Preverjanje ustavljeno. Dostop do tajnih podatkov: Ustavno sodišče začasno zadržalo izvajanje zakona o varovanju tajnih podatkov. Delo. 2003, let. 45, št. 115, str. 2.
43. PRAPROTNIK, Rok. Težave pri približevanju Natu. Ustavljeno varnostno preverjanje: premalo licenc za dostop do tajnih podatkov: vse odvisno od ustavnih sodnikov. Delo. 2003, let. 45, št. 116, str. 2.
44. RELYEA, Harold. Security classified and controlled information. Nova Science Publishers, New York, 2008.
45. REP, Roman. Varnostno preverjanje oseb. V: BELIČ, Igor (ur.). Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 215-219.

46. ROURKE, E. Francis. Secrecy and Publicity: Dilemmas of Democracy. The Johns Hopkins Press, Baltimore, 1966.
47. ROVŠEK, Jernej. Dostopnost informacij javnega značaja in dopustnost omejitev z vidika ustave in varstva človekovih pravic. V: BELIČ, Igor (ur.). Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 35-42.
48. SCHNEIER, Bruce, BANISAR, David. The electronic privacy papers: documents on the battle for privacy in the age of surveillance. J. Willey & Sons, New York, 1997.
49. STANIFORTH, Andrew. Anti-terrorism training: Intelligence. Police review. 2009, let. 117, št. 6.054, str. 31.
50. TRBOVŠEK, Franc. Varnostno preverjanje oseb – vloga obveščevalno varnostnih služb pri izvajanju zakona o tajnih podatkih. V: PAGON, Milan (ur.). Dnevi varstvoslovja, Visoka policijsko-varnostna šola, Ljubljana, 2002, str. 12.
51. VODOVNIK, Zvone. Delovnopravni položaj upravljalcev z državnimi tajnimi podatki (analiza zasnov Zakona o tajnih podatkih). V: BELIČ, Igor (ur.). Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 87-95.
52. WEISS JANŽEK, Silva. Informatika: osebni, tajni in drugi podatki. Ministrstvo za notranje zadeve RS, Policija, Ljubljana, 2008.
53. ŽIROVNIK, Janez. Dostop do tajnih podatkov v zvezi NATO in EU ter v izbranih tujih zakonodajah. Varstvoslovje. 2005, let. 7, št. 3, str. 291-303.
54. ŽIROVNIK, Janez. Varnostno preverjanje – pogoj za dostop do tajnih podatkov. V: BELIČ, Igor (ur.). Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, Ministrstvo za notranje zadeve RS, Ljubljana, 2001, str. 133-145.
55. ŽUMER, Vladimir. Čiščenje, shranjevanje in zloraba arhivskega gradiva. Dnevnik. 2003, let. 53, št. 117, str. 24-25.
56. ŽUMER, Vladimir. Dostop do javnih podatkov, informacij, dokumentov in arhivskega gradiva v Republiki Sloveniji. Arhivi. 2003, let. 26, št. 1, str. 14-21.
57. ŽUMER, Vladimir. Upravljanje dokumentarnega gradiva in elektronska hramba gradiva v digitalni obliki. Planet GV, Ljubljana, 2008.

PRAVNI IN DRUGI VIRI

1. Kazenski zakonik. Uradni list RS, št. 55/2008, 66/2008 – popravek in 39/2009.
2. Poročevalec Državnega zbora Republike Slovenije. Predlog zakona o tajnih podatkih. 2000, št. 10, str. 4.
3. Pravilnik Komisije o varnosti. Uradni list ES, št. L 317/1/2001, L 29/39/2005, L 31/66/2005, L 34/32/2006 in L 215/38/2006.
4. Predpisi Sveta Evropske unije o varovanju tajnosti. Uradni list ES, št. L 101/1/2001, L 63/48/2004, L 193/31/2005, L 346/18/2005 in L 164/24/2007.

5. Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja. Uradni list RS, št. 94/2006.
6. Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov. Uradni list RS, št. 6/2002.
7. Sklep Ustavnega sodišča RS o začasnem zadržanju drugega odstavka 25. člena Zakona o tajnih podatkih in II. dela vprašalnika za dostop do tajnih podatkov kot sestavnega dela Uredbe o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov št. U-I-79/03-7 z dne 8. 5. 2003. Uradni list RS, št. 48/2003.
8. Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja. Uradni list RS, št. 94/2006.
9. Uredba o notranjem nadzoru nad izvajanjem Zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi. Uradni list RS, št. 106/2002.
10. Uredba o upravnem poslovanju. Uradni list RS, št. 20/2005, 106/2005, 30/2006, 86/2006, 32/2007, 63/2007, 115/2007, 122/2007 – popravek, 31/2008 in 35/2009.
11. Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov. Uradni list RS, št. 71/2006 in 138/2006.
12. Uredba o varovanju tajnih podatkov. Uradni list RS, št. 74/2005.
13. Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih. Uradni list RS, št. 48/2007.
14. Ustava Republike Slovenije. Uradni list RS, št. 33I/1991-I, 42/1997, 66/2000, 24/2003, 69/2004, 69/2004, 69/2004 in 68/2006.
15. Zakon o javnih uslužbencih. Uradni list RS, št. 56/2002, 23/2005, 35/2005 – UPB1, 62/2005 – odločba US, 113/2005, 21/2006 – odločba US, 23/2006 – sklep US, 32/2006 – UPB2, 62/2006 – sklep US, 131/2006 – odločba US, 33/2007, 63/2007 – UPB3 in 65/2008.
16. Zakon o spremembah in dopolnitvah Zakona o tajnih podatkih (ZTP-A). Uradni list RS, št. 101/2003.
17. Zakon o tajnih podatkih. Uradni list RS, št. 87/2001, 101/2003, 135/2003 – UPB1, 28/2006 in 50/2006 – UPB2.
18. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih. Uradni list RS, št. 30/2006.

VIRI IZ INTERNETA

1. Bundesamt für Sicherheit in der Informationstechnik. Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) vom 31. März 2006. URL="http://www.bsi.bund.de/sicherheitsberatung/VSA.pdf". 31. 3. 2006.

2. Bwiti bvba. The Step by Step Guide to Brainstorming. URL="http://www.jpb.com/creative/brainstorming.php". 26. 9. 2009.
3. NATO. Nato Security Committee Directive on the Security of Information. URL="http://www.freedominfo.org/documents/AC_35-D_2002-REV2.pdf". 4. 2. 2005.
4. North Atlantic Council. Security Within the North Atlantic Treaty Organisation. URL="http://cryptome.org/nato-cm2002-49.htm". 17. 6. 2002.
5. Urad Vlade Republike Slovenije za varovanje tajnih podatkov. Delovna področja. URL="http://www.uvtp.gov.si/si/delovna_podrocja". 21. 9. 2009.

SEZNAM TABEL

SEZNAM UPORABLJENIH KRATIC

KZ	...	Kazenski zakonik
PKV	...	Pravilnik Komisije o varnosti
PSEUVT	...	Predpisi Sveta Evropske unije o varovanju tajnosti
SDPVOVVO	...	Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja
SUNOUVRSVTP	...	Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov
UIINPVTPVPDSII	...	Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja
UNNIZTPPINP	...	Uredba o notranjem nadzoru nad izvajanjem Zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi
URS	...	Ustava Republike Slovenije
UUP	...	Uredba o upravnem poslovanju
UVPIDDTP	...	Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov
UVTP	...	Uredba o varovanju tajnih podatkov
UVTPKIS	...	Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih
ZJU	...	Zakon o javnih uslužbencih
ZVDAGA	...	Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih
ZTP	...	Zakon o tajnih podatkih

PRILOGE

PRILOGA 1 – Primer kurirskega pisma
PRILOGA 2 – Primer evidence vstopov in izstopov v varnostno območje I. stopnje
PRILOGA 3 – Primer izjave za vstop v varnostno območje I. stopnje v slovenskem jeziku
PRILOGA 4 – Primer izjave za vstop v varnostno območje I. stopnje v angleškem jeziku
PRILOGA 5 – Primer izjave za vstop v varnostno območje I. stopnje v francoskem jeziku
PRILOGA 6 – Primer predloge za tajni podatek stopnje tajnosti ZAUPNO, kopija št. 22

PRILOGA 1 – Primer kurirskega pisma

PERMANENT REPRESENTATION
OF THE REPUBLIC OF SLOVENIA
TO THE EUROPEAN UNION

No.: 5/2009
Date: 5 May 2009

C O U R I E R L E T T E R

The Permanent Representation of the Republic of Slovenia to the European Union in Brussels herewith confirms that

Mr Janez Novak holder of the Diplomatic Passport No. DB0000001

is the carrier of a diplomatic letter.

The Permanent Representaion of the Republic of Slovenia to the European Union in Brussels kindly requests the authorities of the countries through which the carrier of the Courrier Letter is travelling to allow him free passage and to render him assistance, if necessary.

Signature:

Igor Senčar
Ambassador – Permanent Representative

PRILOGA 2 – Primer evidence vstopov in izstopov v varnostno območje I. stopnje

Republika Slovenija
Stalno predstavništvo Republike Slovenije pri EU v Bruslju

EVIDENCA VSTOPOV IN IZSTOPOV V VARNOSTNO OBMOČJE I. STOPNJE

ZAP. ŠT.	IME IN PRIIMEK	RS DOV.		EU DOV.		RAZLOG VSTOPA	DATUM	URA		PODPIS	
		ST.	ŠT.	ST.	ŠT.			PRIHOD	ODHOD	OBISKOVALEC	EVIDENT.

PRILOGA 3 – Primer izjave za vstop v varnostno območje I. stopnje v slovenskem jeziku

Ime in priimek	
Datum in kraj ter država rojstva	
Naslov prebivališča	
Organ oz. organizacija	
Delovno mesto	

I Z J A V A

Izjavljam, da sem bil/a pred vstopom v varnostno območje I. stopnje s strani pooblaščenega uslužbenca v celoti seznanjen/a s postopki in ukrepi, ki se izvajajo v tem območju, in da bom svoje delo izvedel/la izključno pod njegovim nadzorom. V zvezi s tem izjavljam še:

- da se zavedam pomena varnostnega območja in tajnih podatkov, ki se obravnavajo v njem;
- da sem pred vstopom v varnostno območje oddal/a vse elektronske naprave (mobitel, fotoaparat, kamera, snemalnik, MP3-predvajalnik ...);
- da ne bom poskušal/a kakorkoli neupravičeno pridobiti ali odtujiti tajnih podatkov;
- da se bom pri svojemu delu omejil/a le na najnujnejše postopke, ki zagotavljajo izpolnitev delovne obveznosti;
- da bom na zahtevo pooblaščenega uslužbenca, takoj prenehal/a z delom in po potrebi takoj zapustil/a varnostno območje;
- da bom varoval/a tajne podatke ne glede na to, kako bom zanje izvedel/a;
- da vsega videnega v varnostnem območju ne bom kakorkoli posredoval/a katerikoli osebi;
- DA SE ZAVEDAM KAZENSKE ODGOVORNOSTI (do 5 let zapora po 260. čl. KZ-1) ZA MOREBITNO POVZROČITEV RAZKRITJA TAJNIH PODATKOV;
- da pristajam na materialno odgovornost za škodo, ki bi jo povzročil/a s kršenjem katere od prej navedenih izjav.

V prostorih SPBR, dne_____

_____
(podpis osebe, ki podaja izjavo)

_____
(podpis pooblaščenega uslužbenca/ke)

Obvezna priloga: **KOPIJA OSEBNEGA DOKUMENTA**

PRILOGA 4 – Primer izjave za vstop v varnostno območje I. stopnje v angleškem jeziku

Name and surname	
Date, place and country of birth	
Address	
Body/Organisation	
Position	

DECLARATION

I declare that, before entering the security zone, level I, I have been notified by the competent officer of all procedures and measures applied in this zone, and that I will carry out my task exclusively under his/her surveillance. I furthermore declare as follows:

- I am aware of the significance of the security zone and classified information handled in the zone;
- Before entering the security zone, I have deposited all electronic devices (mobile phone, still camera, camera, recorder, MP3 player etc.);
- I will not try in any manner to obtain or impart classified information in an unauthorized way;
- In my activity I will restrain myself only to indispensable procedures, necessary for the accomplishment of my task;
- At the request of the competent officer, I will immediately terminate my work and, if requested, leave the security zone;
- I will protect classified information, regardless of the method in which I may have obtained it;
- I will not, in any way, disclose, whatever I see in the security zone, to anyone;
- I KNOW THAT I AM CRIMINALLY LIABLE FOR ANY POTENTIAL DISCLOSURE OF CLASSIFIED INFORMATION (prison sentence of not more than 5 years in accordance with Art. 260 of the Criminal Code);
- I shall bear material responsibility for any damage caused by infringing any of the above statements.

On the premises of the PRBR, on _____

_____

(Signature of the person making the declaration)

_____

(Signature of the competent officer)

Mandatory enclosure: **COPY OF IDENTIFICATION DOCUMENT**

PRILOGA 5 – Primer izjave za vstop v varnostno območje I. stopnje v francoskem jeziku

Prénom et nom	
Date, lieu et État de naissance	
Adresse	
Organisme/organisation	
Poste	

DÉCLARATION

Je déclare qu'avant l'entrée dans la zone de sécurité de 1er degré, j'ai été informé par l'agent responsable de toutes les procédures et mesures applicables dans cette zone, et que je remplirai ma tâche uniquement sous son contrôle. De plus, je déclare comme suit:

- Je comprends la signification de la zone de sécurité et des informations classifiées qui y sont traitées;
- Avant l'entrée dans la zone de sécurité j'ai déposé tous les appareils électroniques (téléphone portable, appareil photo, caméra, enregistreur, baladeur MP3 etc.);
- Je ne tenterai ni d'obtenir ni de communiquer les informations classifiées sans autorisation;
- Dans mon activité je me limiterai aux seules procédures indispensables à l'accomplissement de ma tâche;
- À la demande de l'agent responsable j'arrêterai mon activité immédiatement et, si nécessaire, quitterai la zone de sécurité sans délai;
- Je garderai les informations classifiées quelle que soit la manière de leur obtention;
- Je ne communiquerai aucun élément vu dans la zone de sécurité à qui que ce soit;
- JE SUIS CONSCIENT DE MA RESPONSABILITÉ PÉNALE POUR TOUT DÉVOILEMENT DES INFORMATIONS CLASSIFIÉES (jusqu'à 5 ans de prison selon les Art. 260 du Code Pénal);
- J'assumerai la responsabilité matérielle pour tout dommage causé par l'infraction à n'importe quelle des dispositions ci-dessus.

Fait à la RPBR, le _____

_____
(Signature du déposant)

_____
(Signature de l'agent responsable)

Pièce jointe obligatoire: **COPIE DU DOCUMENT D'IDENTITÉ**

PRILOGA 6 – Primer predloge za tajni podatek stopnje tajnosti ZAUPNO, kopija št. 22

IZJAVA O AVTORSTVU IN NAVEDBA LEKTORJA

S podpisom zagotavljam, da:

- je predloženo specialistično delo z naslovom Organiziranost in delovanje Službe za tajne podatke na Stalnem predstavništvu Republike Slovenije pri Evropski uniji izključno rezultat mojega lastnega raziskovalnega dela;
- je delo popravljeno v skladu s pripombami mentorja in članov komisije;
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženem delu, navedena oziroma citirana v skladu s fakultetnimi navodili;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del bodisi v obliki citata bodisi v obliki dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oziroma ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorskih in sorodnih pravicah, Uradni list RS, št. 139/2006);
- je elektronska oblika identična s tiskano obliko predloženega dela ter soglašam z objavo dela na fakultetnih straneh;
- da je delo lektorirala Marjeta Kristan.

Podpis: Sven Engelsberger