UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Mojca Kovač

Obravnavanje nacionalnih tajnih podatkov v informacijsko – komunikacijskem sistemu

diplomsko delo

Ljubljana, 2010

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Mojca Kovač

Mentor: doc. dr. Uroš Svete
Somentor: asis. dr. Matej Kovačič

Obravnavanje nacionalnih tajnih podatkov v informacijsko – komunikacijskem sistemu

diplomsko delo

Ljubljana, 2010

Mami Ireni in očetu Stanislavu.

Želela bi se zahvaliti svoji družini, ki mi je med študijem stala ob strani, me podpirala in zaupala vame, še posebej svojima sestrama Andreji in Janji za spodbudne besede in pozitivne misli med pisanjem diplomske naloge.
Iskrena hvala tudi mojemu mentorju doc. dr. Urošu Svetetu in somentorju asis. dr. Mateju Kovačiču za strokovna mnenja in konstruktivna navodila pri oblikovanju diplomske naloge.

OBRAVNAVANJE NACIONALNIH TAJNIH PODATKOV V INFORMACIJSKO – KOMUNIKACIJSKEM SISTEMU

V prvem delu diplomske naloge so predstavljeni nekateri pravni viri Republike Slovenije, ki določajo obravnavanje tajnih podatkov v informacijsko - komunikacijskem sistemu. Drugi, analitični del pa navaja predvsem bolj specifične primere samega obravnavanja tajnih podatkov v skupnem IKS. Predstavljeni so tudi določeni vidiki in standardi, ki urejajo to področje v RS. V samem uvodu je opredeljen pojem varnosti, tajnosti in tajnega podatka ter informacijsko - komunikacijskega sistema. Jasno je zastavljen tudi cilj diplomske naloge, ki izpostavlja trenutno problematiko med sodelovanjem med nacionalnimi organi in navaja potrebo po enotnem IKS. V osrednjem besedilu je bolj podrobno predstavljeno trenutno stanje IKS v RS in delovanje organov, ki so v povezavi z njim. Mnenja intervjuvancev, ki so povezani v sam sistem delovanja pa predstavljajo nekatere vidike in odprta vprašanja, ki jih je v Republiki Sloveniji še potrebno rešiti. Navedeno je tudi trenutno stanje sodelovanja med nacionalnimi organi ter izpostavljene nekatere pomankljivosti, katere so prisotne zaradi trenutnega stanja v državi.

Ključne besede: Nacionalni tajni podatki, varnostna kultura, obravnavanje nacionalnih tajnih podatkov, informacijsko - komunikacijski sistem

HANDLING OF NATIONAL CLASSIFIED INFORMATION IN INFORMATION – COMMUNICATION SYSTEM

The first part of this diploma presents some legal provisions and acts of the Republic of Slovenia, which determine the handling of national classified information in the information - communication system. The second, analytical part introduces more specific examples of protection of national classified information in the republic of Slovenia. The introduction defines the concept of security, classified information and information - communication system. The goal of this diploma emphasis the curent issue of cooperation beetween national authorities and cited the need for common information - communication system. In the main text there is more specificly presented the curent state of information - communication system in RS and the functioning of the authorities in connection with it. Opinions of interviewees which are part of this system presents some aspects and open questions about handling information and information - communication system in the RS and which are still need to be solved.

Keywords: national classified information, safety culture, handling of national classified information, information - communication system.

Kazalo

Seznam kratic

COMPUSEC	Varnost strojne opreme, programske opreme in varnost programsko - strojne opreme
COMSEC	Varovanje tajnosti v komunikacijskih sistemih
CRYPTOSEC	Varnost kriptografskih metod in naprav
EMSEC	Varnost pri elektromagnetnem sevanju elektronskih naprav
HKOM	Prostrano omrežje državnih organov
IKS	Informacijsko komunikacijski sistem
INFOSEC	Ukrepi za varovanje tajnosti v računalniških sistemih
KIV	Komisija za informacijsko varnost
MJU	Ministrstvo za javno upravo
MNZ	Ministrstvo za notranje zadeve
MORS	Ministrstvo za obrambo Republike Slovenije
MZZ	Ministrstvo za zunanje zadeve
NSA	(Nacional security authority) – Nacionalni varnostni urad
NVO	Nacionalni varnostni organ
OVS	Obveščevalno varnostna služba
SOVA	Slovenska obveščevalno varnostna agencija
TRANSEC	Varnost prenosnih sistemov
UVTP	Urad Vlade Republike Slovenije za varovanje tajnih podatkov

1 Uvod

Načelo tajnosti oblasti je v demokratičnih državah v veliki meri zamenjalo načelo javnosti oblasti, kar pa ne velja za nedemokratične, totalitarne oziroma avtoritarne režime. Popolne javnosti delovanja si tudi najbolj demokratična država ne more privoščiti, saj postane ranljiva za nedemokratične pritiske, postane neuspešna in neučinkovita ter kot takšna sama pomeni največjo grožnjo demokraciji (Brezovšek in Črnčec 2007).

Večina ljudi si pod pojmom nacionalni tajni podatki predstavlja določene skrivnosti, katere želi Vlada Republike Slovenije prikriti javnosti zaradi narave njenega delovanja in varovanja samih vitalnih interesov države. (ZTP, 2. člen) Vendar pa tukaj ne igra vloge le Vlada RS, ampak tudi različne organizacije tako vladne kot nevladne ter osebe ki zaradi opravljanja določene funkcije lahko dostopajo do teh podatkov.

Da bi država zavarovala svoje vitalne interese, ustavno ureditev, neodvisnost, ozemeljsko celovitost in obrambno sposobnost, je primorana v nekaterih primerih delovati tajno ali mimo oči javnosti, saj se lahko zgodi, da bi določene informacije prišle v roke »nepravi« osebi ali organizaciji. Tako bi bili ogroženi interesi in koristi same države in njenih državljanov.

Določitev nacionalnih podatkov in informacij za tajne zahteva določen postopek in posredovanje različnih organov, večkrat tudi medsebojno sodelovanje med njimi. Za čim lažje in hitrejše medresorsko sodelovanje so določeni organi že vzpostavili svoje lastne informacijsko - komunikacijske sisteme, preko katerih operirajo s tajnimi podatki. Zaželjeno pa je, da bi v roku parih let vzpostavili skupen informacijsko - komunikacijski sistem, ki bi jim to sodelovanje olajšal in znatno skrajšal določene postopke pri sami obravnavi nacionalnih tajnih podatkov.

Del sistema obravnavanja tajnih podatkov je tudi varovanje le teh. Pomen varovanja tajnih podatkov kaže na to, da vsi podatki ne morejo in niso prosto dostopni različnim posameznikom ali zainteresiranim organizacijam, ampak velja načelo, da se smejo s posameznimi informacijami in podatki seznaniti samo do njih upravičeni posamezniki. To predstavlja bistvo varnostne kulture varovanja tajnih podatkov. Komisija za informacijsko varnost, ki je bila imenovana na podlagi 15. člena Uredbe o varovanju tajnih podatkov v informacijsko - komunikacijskih sistemih pripravlja tehnične in normativne rešitve prav s tem namenom po zaščiti tajnih podatkov in posledično tudi vitalnih interesov države.

Države, ki imajo daljšo zgodovino in tradicijo, so tekom delovanja vzpostavile močne in izpopolnjene informacijsko - komunikacijske sisteme za obravnavanje tajnih podatkov, zato je imela Republika Slovenija zelo težko nalogo v procesu vključevanja v EU in NATO. Eden

temeljnih pogojev za vstop v te dve organizaciji je bil tudi vzpostavitev ustreznega sistema obravnavanja tajnih podatkov. Vendar ji je kjub svoji kratki zgodovini uspelo, saj se njen varnostni sistem v temeljnih načelih ne razlikuje od načel organizacij EU in NATO.

2 Teoretična, metodološka in hipotetična izhodišča

2.1 Metode dela in opredelitev ciljev preučevanja

Metode, katere sem uporabila v tej diplomski nalogi, se navezujejo na samo tematiko raziskovalnega dela. Preden sem sploh začela z raziskovanjem, sem zaradi lažjega dela najprej zbrala in pregledala določeno bibliografijo o temi, ki jo želim analizirati, saj sem se na ta način hotela prepričati, da ni bila moja željena tema že kadarkoli prej obravnavana oz. obdelana.

Z metodo zbiranja virov sem definirala temeljne pojme in nato dobila splošen vpogled v sam postopek obravnavanja nacionalnih tajnih podatkov znotraj informacijsko - komunikacijskih sistemov. S konceptualno analizo sem povezala posamezne pojme med sabo in na ta način ustvarila rdečo nit pri pisanju diplomskega dela.

Bibliografija na tem področju je zelo obširna, vendar sem se v diplomski nalogi nanašala izključno na sam Zakon o tajnih podatkih (Ur.l.RS, št. 50/06 - UPB2) in na Uredbo o varovanju tajnih podatkov (Ur.l.RS, št. - 74/05). Z analizo teh dveh primarnih virov, ki ju bom bolj natančno predstavila v nadaljevanju diplomske naloge, sem dobila splošen vpogled v sam proces delovanja različnih nacionalnih organov in uradov, ki sodelujejo pri obravnavanju nacionalnih tajnih podatkov.

Uredba o varovanju tajnih podatkov v informacijsko - komunikacijskih sistemih (Ur. l. RS, št. 50/06), izdana na podlagi petega odstavka 39. člena Zakona o tajnih podatkih, zajema splošne določbe, ki navajajo organizacijske in tehnične ukrepe ter postopke varovanja nacionalnih tajnih podatkov znotraj informacijsko - komunikacijskega sistema. Ta Uredba je edini primarni pravnomočni vir v RS, s pomočjo katerega sem lahko vsaj okvirno opredelila informacijsko - komunikacijski sistem, ki omogoča obravnavanje nacionalnih tajnih podatkov (Uredba o varovanju tajnih podatkov v informacijsko - komunikacijskih sistemih, Ur. l. RS, št. 50/06).

Preohlapno obravnavanje vsebinskih pojmov in preveč splošno definiranje posameznih izrazov mi je nemalokrat povzročalo preglavice predvsem pri iskanju sekundarne literature na

internetu, saj sem pri iskanju s ključnimi besedami velikokrat naletela na ogromno rezultatov, ki pa za mojo obravnavano temo niso bili kaj dosti uporabni.

Identifikacija raziskovalnega problema, katero sem določila s pomočjo analize primarne literature, mi je uspešno služila kot vodilo pri nadaljni raziskavi. Tako sem lahko določila, katera sekundarna literatura mi bo v največjo pomoč pri preverjanju hipoteze.

Tekom raziskovanja in prebiranja literature ter iskanja ažurnih virov in že obstoječih problemih sem ugotovila, da do določenih informacij, ki bi bile aktualne, predvsem pa bistvene za moj raziskovalni del diplomske naloge, kot študentka ne bom smela dostopati, kaj šele, da bi jih v nalogi omenjala. Prav zato sem za svojo naslednjo metodo izbrala intervju.

Intervju nam lahko omogoči neposreden dostop do empiričnih podatkov. Sama sem se v diplomski nalogi odločila za strukturiran intervju, pri čemer sem zastavljala odprta vprašanja, saj sem na ta način dopustila intervjuvancu, da ponudi tudi svoje videnje problema. S to metodo sem pridobila največ informacij in odgovorov, ki jih tekom analize različne literature nisem našla oziroma mi dostop do nje ni bil odobren.

Glede na dejstvo, da bom preučevala obravnavanje nacionalnih tajnih podatkov v informacijsko - komunikacijskem sistemu, bom opravila intervjuje s člani Komisije za informacijko varnost, ki jo sestvljajo predstavniki Ministrstva za javno upravo, Ministrstva za notranje zadeve, Ministrstva za obrambo, Ministrstva za zunanje zadeve in Urada Vlade Republike Slovenije za varovanje tajnih podatkov.

Vsem intervjuvancem bo ponujena možnost vnaprejšnje seznanitve z vprašanji in snemanje zvočnega zapisa med potekom intervjuja.

Na podlagi zbranih podatkov iz intervjujev in analize primarne in sekundarne literature ter literature pridobljene na internetu na koncu opravila še primerjalno analizo, pri kateri bom med sabo primerjala zbrane odgovore intervjuvancev.

Enoten informacijsko - komunikacijski sistem za tajne podatke v RS bi bil tehnično možen in zaželjen. Tudi EU in NATO imata svoje enotne sisteme, ne sicer za vse tajne podatke ampak samo za nekatera posamezna področja. V RS bi z enotnim IKS za obravnavanje tajnih podatkov rešili predvsem problem povezave med organi, kar trenutno predstavlja največjo oviro pri delovanju določenih institucij. Ker pa so določeni organi tekom svojega delovanja postali že precej samostojni in imajo že dodobra razvite IKS, bi bil enoten sistem za vse tajne podatke težko izvedljiv.

Cilj diplomske naloge je opredeliti vlogo in pomen izvedbe enotnega informacijsko - komunikacijskega sistema za obravnavanje nacionalnih tajnih podatkov v RS in s tem okrepiti in rešiti problem povezave med organi.

2.2 Opredelitev temeljnih pojmov

2.2.1 Varnost

Varnost je stanje, v katerem je zagotovljen uravnotežen fizični, duhovni in duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbene skupnosti in narave (Grizold 1999).

Anžič (2002, 455) predstavi varnost kot »imanentno prvino družbe, ki zajema stanje oziroma lastnost stanja in dejavnost oziroma sistem«. Sam pojem se nanaša tako na posameznika, na državo ter družbo v celoti, kot tudi na mednarodno skupnost. Sodobna varnostna paradigma namreč varnost obravnava v treh temeljnih okvirih in sicer kot nacionalno varnost, individualno varnost in mednarodno varnost.

Varnost je torej človekovo zavestno prizadevanje za vzpostavitev takšne civilizacijske in kulturne kategorije, ki bo zajemala vse vidike varnosti: politične, pravne, zdravstvene, gospodarske, socialne, kulturne in druge (Anžič 2002, 455).

Koncept varnosti se nanaša na zelo širok spekter človekovega delovanja. Pojavlja se na različnih stopnjah družbe in družbenih ureditev in zadeva tako posameznika kot tudi skupine in organizacije. V svoji diplomski nalogi se bom osredotočila predvsem na informacijsko varnost pri obravnavanju tajnih podatkov oziroma na varovanje tajnih podatkov v informacijsko - kumunikacijskih sistemih. Sama tema moje diplomske naloge pa zahteva tudi razčlenitev vidikov individualne, mednarodne in nacionalne varnosti, ki so medsebojno povezane in igrajo ključno vlogo tudi pri sooblikovanju informacijsko - komunikacijskih sistemov.

V resoluciji o izhodiščih zasnove nacionalne varnosti Republika Slovenija opredeli nacionalno varnost kot »stanje, v katerem je zagotovljeno uresničevanje človekovih pravic in temeljnih svoboščin, uravnotežen gospodarski, socialni in kulturni razvoj ter uresničevanje drugih življenskih interesov, delovanje demokratične, pravne in suverene ter ozemeljsko

enotne in nedeljive Republike Slovenije« (Resolucija o izhodiščih zasnove nacionalne varnosti Republike Slovenije, Uradni list RS, št. 71/93).

Grizold (1992, 65) opisuje nacionalno varnost kot varovanje državnega ozemlja (kopno, vode, zračni prostor), prebivalstva in njihove lastnine, ohranjanje nacionalne suverenosti ter zagotavljanje ustreznih razmer za uresničevanje temeljnih funkcij družbe. Medtem ko Anžič (1997, 37) poudarja, da »nacionalna varnost z ene strani res zagotavlja varnost svojim državljanom ter odpravlja vire njihovega ogrožanja, vendar hkrati preko svojih varnostnih organov posledično tudi sama postane vir ogrožanja individualne varnosti.«

Zavedati se je treba, da med nacionalno in individualno varnostjo obstajajo vedno neka nasprotujoča si dejstva. Lahko se zgodi, da je zunanji vidik nacionalne varnosti zagotovljen, vendar so državljani kljub temu individualno ogroženi, bodisi v odnosu med seboj bodisi s strani državnih organov. Absolutne varnosti ni. Država svojim državljanom zagotavlja nacionalno varnost z oblikovanjem nacionalno varnostnega sistema.

Brezovšek (2007, 17) navaja, da če je individualna potreba po varnosti, ki jo čuti posameznik, zadovoljena, sta mu omogočena kakovosten razvoj in posledično tudi obstoj. Individualna varnost nastopi vedno relativno, medtem ko se mednarodna varnost kaže kot notranji varnostni problem sistema držav in sveta kot celote. Je kolektivna dobrina tako za mednarodno globalno družbo kot tudi za posamezno državo ali zvezo držav.

3.člen Uredbe o varovanju tajnih podatkov v komunikacijsko - informacijskih sistemih opredeljuje informacijsko varnost kot sistem, ki zajema določanje in uporabo ukrepov varovanja tajnih podatkov, kateri se obravnavajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov.

2.2.2 Tajnost in tajni podatek

Tajnost: vrednota in zlo, tako opredeli Anžič (2000, 849) ta družbeni fenomen, ki so ga družboslovne, predvsem politološke, sociološke in obramboslovne znanosti skoraj v celoti zanemarile ali mu niso posvečale dovolj pozornosti, mogoče prav zaradi enačenja s pojmom skrivnosti.

SSKJ navaja tajnost kot značilnost tajnega (jamčiti tajnost, podatki morajo ostati v tajnosti), spet v drugem pomenu jo opredeli kot nekaj kar je tajno (podatki so tajnost, državna tajnost) ter izpostavi knjižnji sinonim za skrivnost. Skrivnost je tisto, kar kdo ve, kar mu je zaupano in se ne sme pripovedovati drugim. Za primer je podana vojaška, poslovna in uradna skrivnost (Brezovšek in Črnčec 2007, 96).

Anžič (2000, 852) se ne strinja in nam predstavi svoj vidik razumevanja tajnosti, in sicer kot nekaj znanega, kar se da razumeti in pojasniti. Vsebina tajnosti je znana, vendar jo njen »posestnik« (posameznik, institucija ali država) ne sme ali noče narediti dostopno javnosti. Tajnost pomeni obstoj znanih dejstev o družbenih, varnostnih, obrambnih, gospodarskih in drugih podatkih in informacijah, ki so posamezniku ali instituciji zaupana v uporabo in varovanje.

V sodobni demokratični državi lahko obstoj tajnosti opravičujejo tudi naslednji razlogi:

- obstoj nasprotujočih si interesov;
- izrecno pravno opredeljeni interesi;
- kršitev tajnosti mora predstavljati posamezniku ali družbi nevarno ali škodljivo ravnanje;
- tajnost mora biti namenjena varovanju, obrambi in zaščiti obstoja države, njene ustavne ureditve ali posebnim interesom pri varovanju človekovih pravic;
- s pravno normo morajo biti določeni podatki označeni kot tajni, imenovani morajo biti upravljalci tajnosti in ti podatki morajo imeti ustrezno stopnjo in vrsto tajnosti;

- določeni morajo biti ukrepi za varovanje tajnih podatkov, s katerimi se preprečuje njihovo prilaščanje, neopravičeno odstopanje, spreminjanje ali pridobivanje (Anžič 2000, 854).

Bistveno vsem tem razlogom je, da tajnost kot oblika skrivanja znanega, ne sme biti politizirana. Služiti bi morala univerzalnim, splošnim in posebnim interesom ter preprečevati možnosti škodovanja le tem (Anžič 2000, 854).

V sodobnih demokratičnih političnih sistemih je tajnost kompleksen pojav, ki vključuje pravico države do zasebnosti in do varovanja svojih tajnosti (Anžič 2000, 854).

2. člen Zakona o tajnih podatkih opredeljuje tajni podatek kot dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je potrebno, zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami in ki je v skladu s tem zakonom določeno in označeno za tajno (ZTP 2. Člen, 2006).

2.2.3 Informacijsko – komunikacijski sistem

Informacijsko - komunikacijski sistem ali telematika, kot so ga pred desetletjem arhaično poimenovali telekomunikacisti, je v začetni fazi integracije informacijskih in telekomunikacijskih sistemov imel dokaj specifičen in dobro opredeljen pomen. Šlo naj bi za skupek uporabniških storitev, ki so zasnovane na osnovi telekomunikacijskih sistemov (Vidmar 2002).

Izraz telematika, ki ga dandanes sploh več ne poznamo, je bil izrazit v sedemdesetih letih, predvsem v Evropi, medtem ko ga Amerika ni nikoli sprejela, kar je najbrž dodaten razlog, da njegova uporaba zamira. Vendar pa je sam izraz pomemben prav zato, ker se v njem prvič zrcalita potreba in ideja o integraciji informacijskih in telekomunikacijskih storitev (Vidmar 2002).

Vidmar (2002, 32) pravi, da je informacijsko - komunikacijski sistem multidisciplinaren in kompleksen integriran sklop različne tehnologije. Opredeli ga kot integracijo računalniškega informacijskega sistema in telekomunikacijskega sistema (Vidmar 2002, 57). V sebi združuje

različne metode in tehnologije s področja prenosnih naprav, telekomunikacisjkih sistemov, računalniških in informacijskih sistemov z vsemi podrobnostmi in specifičnostmi posamezne tehnologije in infrastrukture.

Vidmar (2002, 71) opredeli povezavo med uporabniki in sistemom kot implementacijo z množico informacijskih funkcij, ki omogočajo podatke zbirati, hraniti in do njih dostopati ter množico funkcij komunikacijskega sistema, ki omogočajo podatke prenašati med različnimi informacijskimi okolji.

V diplomski nalogi bom predstavila informacijsko - komunikacijski sistem, ki je predstavljen v Uredbi o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, elektromagnetno sevanje, varnostno območje, elektronsko varnostno območje in strojno opremo sistema, kakršno vsebuje nacionalni informacijsko - komunikacijski sistem.

Informacijsko - komunikacijski sistem, kot ga navaja Uredba o varovanju tajnih podatkov v komunikacijsko - informacijskih sistemih, je zadolžen za izvajanje fizičnih, organizacijskih in tehničnih ukrepov ter postopkov varovanja tajnih podatkov v samem procesu obravnavanja le teh v različnih vladnih in nevladnih organizacijah. Potrebno je vzpostaviti sistem minimalnih standardov, postopkov in tehničnih ukrepov, ki bi ustrezali stopnji tajnosti tajnih podatkov v komunikacijskih in informacijskih sistemih ter onemogoča njihovo razkritje nepooblaščenim osebam, katere bi lahko ogrozile vitalne interese države (Uredba o varovanju tajnih podatkov v informacijsko komunikacijskih sistemih 1.člen, 2005).

Ključne sestavine IKS so strežniki, delilniki in usmerjevalniki prometa, oprema za upravljanje in nadzor, aktivna oprema za prenos podatkov v nešifrirani obliki, oprema za šifrirno zaščito podatkov, varnostne pregrade, oprema za odkrivanje in zaščito pred vdori, oprema za izdelavo varnostnih kopij.

Vsa ta oprema mora biti odobrena s strani Urada Vlade RS za varovanje tajnih podatkov z varnostnim dovoljenjem za delovanje sistema. Vsak predstojnik organa ali organizacije mora pred začetkom obravnavanja tajnih podatkov v sistemu s pisnim sklepom potrditi izvajanje vseh ukrepov in postopkov za zagotovitev varnega delovanja sistema (Uredba o varovanju tajnih podatkov v informacijsko komunikacijjskih sistemih 4. Člen, 2007).

2.3 Hipoteze

V skladu z zastavljenim ciljem bom preverjala naslednjo hipotezo.

Za obravnavanje nacionalnih tajnih podatkov v Republiki Sloveniji bi bil potreben enoten informacijsko - komunikacijski sistem.

Izvedena hipoteza:

1. Enoten informacijsko - komunikacijski sistem za obravnavanje tajnih podatkov v Republiki Sloveniji bi okrepil sodelovanje med organi in rešil vprašanje povezljivosti med njimi.

3 Razvoj informacijsko - komunikacijske tehnologije in družbena odgovornost oblasti

Vsaka država z zakonom določi, kateri podatki so tajni. V Republiki Sloveniji to določa Zakon o tajnih podatkih RS, ki v svojem 5. členu opredeljuje, da se podatek lahko določi za tajen, če se nanaša na:

- varnost države,
- obrambo države in obrambne zadeve,
- mednarodno dejavnost in mednarodne odnose RS,
- obveščevalne in varnostne dejavnostidržavnih organov RS,
- sisteme, naprave, projekte in načrte, ki so pomembni za varnost in obrambo države,
- znanstvene, raziskovalne, tehnološke in gospodarske zadeve, ki so pomembne za varnost in obrambo države (ZTP 5. Člen, 2006).

Podatek, nanašujoč na prejšnji odstavek, se lahko določi za tajen samo, če je takšna določitev nujna zaradi zavarovanja interesov Republike Slovenije in če se lahko utemeljeno pričakuje, da bi se brez takšne določitve utegnile nastati škodljive posledice za varnost države in posledično tudi njenih državljanov (ZTP 10. Člen, 2006).

Po ZTP 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 ZTP morajo ravnati tudi dobavitelji, izvajalci gradenj ali izvajalci storitev, ki se jim tajni podatki posredujejo zaradi izvršitve naročil organa (Zakon o tajnih podatkih, Ur.l.RS, št. 50/06 - UPB2).

Zahteve glede delovanja javne in državne uprave se vedno bolj zaostrujejo, pričakovanja državljanov in gospodarskih subjektov pa se vedno bolj višajo, kar se kaže predvsem po zahtevah po manjšanju obsega sredstev za delovanje uprave ob hkratnemu ohranjanju obsega storitev (Žurga 2001).

Meja med dejansko in namišljeno potrebo po zasebnosti države je dostikrat nejasna ali težko določljiva, zato je potrebno s tem, ko se državi dopusti zaščita tajnosti zagotoviti dovolj močne vzvode, ki onemogočajo oziroma otežujejo zlorabo (Brezovšek in Črnčec 2007).

Kot navaja Bohinc (2005, 5) predstavlja jvnost dela državnih organov ter transparentnost njihovih odločitev in ukrepov temeljno sestavino novodobnih demokratičnih družbenih ureditev.

Z razvojem informacijske in telekomunikacijske tehnologije je nadzor nad prebivalci danes lažje dosegljiv kot kadarkoli prej v zgodovini. Tehnološko in informacijsko razviti lahko s pomočjo satelitov navigirajo civilni in vojaški promet, prisluškujejo in prestrezajo komunikacije, kjerkoli se jim zazdi. Internet omogoča prebiranje elektronskih sporočil, ki si jih posamezniki pošiljajo med sabo, med njimi tudi uradniki, ki imajo nemalokrat v obdelavi tajne podatke, pa so pri svojem delu z njimi nekorektni in ne upoštevajo navodil, kako ravnati s tako občutljivimi podatki.

Prav v ta namen člani KIV pred akreditacijo šifrirnih rešitev, katere se uporabljajo za šifrirno varovanje podatkov v IKS pregledajo določeno dokumentacijo, katero jim morajo organi, ki so v procesu akreditacije predložiti. Če je predložena dokumentacija popolna in ustreza normativom in kriterijem, kateri so enakovredni standardom po katerih akreditirajo šifrirne rešitve v državah EU, potem se organu, ki je v postopku akreditacije izda potrdilo o varnostni ustreznosti šifrirnih rešitev.

Varnostna določila Sveta EU zajemajo tudi posebno poglavje, ki obravnava varovanje tajnih podatkov s področja informacijske tehnologije in komunikacijskih sistemov ter postopke za odobritev dostopa do tajnih podatkov. Ta varnostna določila Sveta EU veljajo za Svet EU, Generalni Sekretariat Sveta EU in vse države članice. Definirajo pojem tajni podatki in oblike potencialnega ogrožanja tajnih podatkov. Določajo, da mora vsaka država članica imeti svoj

nacionalni varnostni urad. (Security regulations of the Council of the European Union) V RS po 43. členu Zakona o tajnih podatkih naloge NVO opravlja Urad Vlade Republike Slovenije za varovanje tajnih podatkov (ZTP 43. člen, 2006).

V zvezi NATO so 17. junija 2002 pričeli veljati novi varnostni standardi, med katerimi so sprejeli tudi Direktivo o informacijski varnosti (AC/35-D/2002) . Ta direktiva določa načine in postopke ravnanja na področju informacijske varnosti, predvsem s poudarkom na tehničnih rešitvah informacijske varnosti (Security within the Nort Atlantic Treaty organisation, document CM (2002)49).

Vendar pa sama varnostna ustreznost šifrirnih rešitev še ne zagotavlja popolne varnosti obravnavanja tajnih podatkov. Tudi varnostna kultura posameznega organa narekuje določene vrednote, ki so sestavni del organizacijske oziroma politične kulture. Na podlagi teh vrednot, ki morajo biti v organizaciji sprejete soglasno, zaposleni pa se morajo nanje čustveno navezati, lahko organizacija dosega željene rezultate.

Vršec (2003, 8) navaja, da varnostna kultura pomeni »zavest, da ima vsakdo pravico in dolžnost poskrbeti za lastno varnost in hkrati prispevati k varnosti bivalnega, delovnega, poslovnega in širšega okolja.«

Profesionalno in osebno dolžnost razvijanja varnostne kulture zaposlenih in ostalih državljanov imajo državne institucije, izobraževalne organizacije, lastniki premoženja, menedžerji in strokovnaki iz varnostnih ved.

Vsak organ je zato dolžan iz varnostnih potreb, povezanih z njegovo dejavnostjo, sprejetih mednarodnih obveznosti ter veljavnih predpisov in priporočil, ki urejajo področje informacijke varnosti, določiti informacijsko - komunikacijsko varnostno politiko obravnavanja tajnih podatkov.

4 Varnostna politika RS pri obravnavanju nacionalnih tajnih podatkov

V organu javne uprave je treba jasno določiti odgovornosti za zaščito posameznih sredstev in izvajanje posebnih varnostnih postopkov. Splošna navodila za razporeditev vloge posameznika pri zagotavljanju informacijske varnosti in njegovi odgovornosti morajo biti zapisana v smernicah varnostne politike organa javne uprave (Uredba o varovanju tajnih podatkov v informacijko komunikacijskih sistemih, 15. čl.).

Ker postaja informacijska tehnologija vse bolj temelj premoženja vsake organizacije, delovanje le teh pa je odvisno prav od njene zanesljivosti je pomembno, da so informacijsko komunikacijski sistemi v uporabi varni in zanesljivi. IKS mora biti varovan pred najrazličnejšimi grožnjami iz okolja. V ta namen pa v procesu akreditacije KIV pregleda dokumentacijo vseh šifrirnih rešitev, katere ima organizacija namen vpeljati v IKS za obravnavanje nacionalnih tajnih podatkov.

Ključni dejavniki za delovanje internega kontrolnega sistema varovanja IKS so:

- varnostna politika,
- implementirane interne kontrole,
- delovanje internega kontrolnega sistema,
- prepoznavanje, razumevanje in ovrednotenje tveganj,
- usposabljanje zaposlenih (Javornik 2000).

Kadar se v organ javne uprave vpeljujejo nove informacijske in telekomunikacijske tehnologije, morajo biti le te odobrene s strani poslovnega in tehničnega vidika, saj se na ta način zagotovi njihovo skladnost z informacijsko - varnostno politiko in njenimi zahtevami.
V vsakem organu v javni upravi je potrebno imenovati svetovalca za informacijsko varnost ali pa vsaj vzpostaviti osrednje mesto kot vir nasvetov, kar pripomore pri odločanju o pomembnih varnostnih vprašanjih ter pri pridobivanju znanja in potrebnih izkušenj (Uredba o varovanju tajnih podatkov v informacijko komunikacijskih sistemih, 15. čl.).
Vzpodbujati je potrebno stike z notranjimi in zunanjimi strokovnjaki ter krepiti odnose in sodelovanje med organi javne uprave saj lahko na ta način pripomoremo k večji povezljivosti med njimi. Ponudniki informacijsko - komunikacijskih storitev omogočajo organom javne uprave, da sledijo svetovnim trendom in zagotavljajo hitro reševanje problemov ob morebitni ogroženosti ali nevarnosti, saj se nemalokrat lahko zgodi, da se zaupni podatki razkrijejo nepooblaščenim osebam.

4.1 Sistem upravljanja z informacijsko varnostjo v javni upravi

V organu javne uprave je prav vsak posameznik odgovoren za informacijsko varnost. Prav v ta namen je vsak organ javne uprave dolžan vsem zaposlenim, pa tudi zunanjim uporabnikom zagotoviti ustrezno izobraževanje in usposabljanje za zagotavljanje le-te.

Sistem varovanja nacionalnih tajnih podatkov mora zagotavljati kontinuirano izvajanje fizičnih, organizacijskih in tehničnih postopkov, ki jih predvideva ZTP, po drugi strani pa mora zagotavljati operativnost v svojih postopkih, ki morajo biti čim manj moteči za posameznika in delovanje sistema (Čaleta 2003). Zavedati se namreč moramo, da še tako dober sistem varovanja tajnih podatkov, ne pomeni ničesar, če nimamo dobro usposobljenega kadra, ki upravlja s temi podatki (Korošec 2006).

V informacijski varnostni politiki morajo biti opredeljene splošne vloge in odgovornosti pri vpeljevanju oziroma ohranjevanju informacijske varnosti, po potrebi pa tudi natančnejše usmeritve glede odgovornosti za posamezna sredstva in varnostne postopke.
Z ločevanjem vlog in odgovornosti se zmanjša možnost zlorab in drugih oblik ogrožanja informacijske varnosti v organu javne uprave. Tako je priporočljivo, da nekatere naloge, kot je vodenje sistema, vnos podatkov, vodenje varovanja, ravnanje z omrežjem in druge, opravljajo različni ljudje.
Informacijska varnostna politika predstavlja formalen dokument, katerega sprejme predstojnik organa javne uprave oziroma upravni vodja in se nanaša na vse redno in pogodbeno zaposlene ter zunanje sodelavce.

Ključne sestavine dokumenta varnostne politike so:

- varovanje in kontrola dostopa do informacij,
- usklajenost z zakoni in predpisi,
- ustrezno usposabljanje zaposlenih z namenom povečanja zavedanja o pomembnosti varovanja informacij in sredstev organizacije,
- kazni zaradi neskladnosti (Derek 2002).

Organ javne uprave nabavlja določeno opremo in vrste storitev preko zunanjih izvajalcev oziroma dobaviteljev, ki lahko dobijo ob tem vpogled v podatke tajne narave. Za vse take primere jih je potrebno zavezati s podpisano izjavo o varovanju podatkov. Zato more biti le ta napisana z mislijo na končne uporabnike, z drugimi besedami, jasno in enostavno, da jo bodo razumeli tudi nevešči uporabniki. V njej mora biti zapisano, kaj se pričakuje in na koga se obrniti z morebitnimi vprašanji.
Informacijska varnostna politika velja tudi zunaj poslopja organa javne uprave in izven delovnih ur. Na veljavnost informacijske varnostne politike je potrebno paziti pri delu izven

organa na oddaljeni lokaciji oziroma pri delu na domu. Tudi tak način dela mora zadostiti vsem zahtevam informacijske varnostne politike, predvsem kar zadeva varovanje podatkov, preprečevanje elektronskega prisluškovanja in zavarovanje pred virusi in drugimi oblikami kibernapada.

Najpogostejše nevarnosti, ki ogrožajo informacijsko tehnologijo se kažejo kot okvara stojne in programske opreme, napake v računalniških programih, napačni podatki, neprimerne tehnične karakteristike, uporabniške napake, vohunstvo, prevare ter naključne napake in druge odpovedi (Laudon 2000).

Kadar vnašamo podatke preko internih aplikacij se verjetnost napak znatno poveča (Eckerson 2002).

Organizacija mora izdelati pravilnik uporabe informacijskih sredstev za vsa področja. Sestavi izjavo o varovanju informacij. S podpisom izjave se uporabniki zavežejo zgolj k uporabi v službene namene. Zlorabe podpisane izjave pa se temu primerno obravnavajo z disciplinskimi ukrepi (Rakovec 2005, 78).

4.2 Upravljanje z informacijsko - komunikacijskim sistemom

Da posega računalniška tehnologija v vsa področja življenja sem razjasnila že v prejšnjih poglavjih diplomskega dela. V nadaljevanju se bomo osredotočili predvsem na samo upravljanje informacijsko - komunikacijskih sistemov in njihovo sistematično reševanje problemov ter akreditacije le - teh.

Posledično z razvojem IKS so tudi informacijske rešitve postale vedno bolj kompleksne in težje obvladljive. Dandanes je tržišče že prenasičeno z najrazličnejšimi programskimi aplikacijami, ki kljub popolnosti in dovršenosti uporabniki informacijskih tehnologij še vedno potrebujejo pomoč in podporo. Potreba po podpori IT je tako velika, da je v smislu poslovne upravičenosti smiselna organizacija lastnega centra za podporo, kot nekakšen »back up« celotnemu sistemu.

Za uspešno upravljanje IKS je v prvi vrsti potrebno dobro poznavanje same infrastrukture. Organizacija sama mora izvesti oceno tveganj ter pripraviti in ukrepati za zmanjšeanje ali preprečevanje tveganj na sprejemljivo raven (Hajtnik 2002).

Uspešne organizacije danes najprej načrtujejo vloge ljudi in partnerjev ter procese. Šele nato pride v poštev postavitev tehnologije, ki jih podpira in avtomatizira. V učinkovitih organizacijah so te vloge in procesi usklajeni s poslovanjem, poslovnimi zahtevami in

poslovnimi procesi. Upravljanje infrastrukture IKT zajema celotno upravljanje in administracijo, zasnovo in načrtovanje, tehnično podporo ter uvajanje in delovanje informacijsko - telekomunikacijske infrastrukture.

4.2.1 Akreditacija informacijsko - komunikacijskih sistemov

15. člen Uredbe o varovanju tajnih podatkov v informacijko komunikacijkih sistemih navaja, da Vlada RS ustanovi medresorsko komisijo za informacijsko varnost, ki je sestavljena iz predstavnikov Ministrstva za javno upravo, Ministrstva za notranje zadeve, Ministrstva za obrambo, Ministrstva za zunanje zadeve, Slovenske obveščevalno varnostne agencije in Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Uredba o varovanju tajnih podatkov v informacijko komunikacijskih sistemih, 15. čl.).

Naloge Komisije za informacijsko varnost so:

- pripravlja tehnične in normativne rešitve za varovanje tajnih podatkov v komunikacijskih in informacijskih sistemih;
- določanje primernih načinov in postopkov za identifikacijo in overitev dostopa uporabnikov v komunikacijsko informacijske sisteme;
- potrjuje šifrirne sisteme, ki se lahko uporabljajo v komunikacijsko informacijskih sistemih;
- izdelava zahtev za povezovanje komunikacijsko informacijskih sistemov;
- priprava varnostnih zahtev za izvajanje zaščite proti neželenemu elektromagnetnemu sevanju.

Komisija uredi način svojega dela s poslovnikom, ki mora biti akreditiran s strani Vlade (Uredba o varovanju tajnih podatkov v informacijko komunikacijskih sistemih, 15. čl.).
V njem so opredeljene tehnične in normativne rešitve, za varovanje tajnih podatkov v informacijsko - komunikacijskih sistemih ter nekatere smernice za povezovanje teh sistemov med organi.
Določeni nacionalni organi imajo že sedaj dodobra izpopolnjene IKS, manjka jim le enoten sistem, ki bi omogočil povezavo med njimi in njihovim delovanjem. Enoten informacijsko - komunikacijski sistem za obravnavanje tajnih podatkov bi bil v RS zelo zaželjen. S

tehničnega vidika bi bila njegova vzpostavitev izvedljiva, prktično pa bi rešil trenutno vprašanje povezljivosti in sodelovanja med organi pri obravnavanju nacionalnih tajnih podatkov.

Povezovanje sistemov je dovoljeno le po nadzorovanih in posebej varovnih vstopno - izstopnih točkah, preko katerih potekajo vsi servisi in storitve. Z internetom so lahko povezani le tisti sistemi, v katerih se obrvnavajo tajnih podatki stopnje tajnosti INTERNO. Komisija v ta namen pripravi določene varnostne zahteve po katerih poteka proces povezovanja sistemov (Uredba o varovanju tajnih podatkov v informacijko komunikacijskih sistemih, 16. čl.).

4.3 Uporaba šifrirnih sistemov in kripto naprav

Člani komisije za informacijsko varnost so zadolženi za pregledovanje, ocenjevanje in potrjevanje varnostnih politik, postopkov in standardov. Istočasno so dolžni pregledovati in ocenjevati poročila notranjih in zunanjih revizij informacijske varnosti.

4.3.1 Postopek odobritve uporabe šifrirnih rešitev v Republiki Sloveniji

Šifrirne rešitve so šifrirna oprema in sistemi ter vanje vgrajeni moduli, ki se uporabljajo za šifrirno varovanje podatkov v informacijsko - komunikacijskih sistemih, v katerih poteka obravnavanje tajnih podatkov (Navodilo o postopku odobritve uporabe šifrirnih rešitev, 2. čl.).

V RS postopek odobritve izvaja Urad Vlade RS za varovanje tajnih podatkov ali drug, z zakonom določen organ, in sicer za vsako šifrirno rešitev posebej. UVTP izda dokument o varnostni ustreznosti sistema, ki upravljavcem dovoljuje uporabo šifrirno ovrednotenih rešitev.

Navodilo o postopku odobritve uporabe šifrirnih rešitev, ki je bilo izdano na podlagi četrtega odstavka 15. člena Uredbe o varovanju tajnih podatkov v informacijsko - komunikacijskih sistemih, v svojem 6. členu navaja, da se v postopku šifrirnega ovrednotenja preverja stopnja varnosti arhitekture in izvedbe šifrirnih rešitev. Šifrirno ovrednotenje se opravi na podlagi zahtevane dokumentacije, ki jo predpisuje potrdilo o varnostni ustreznosti.

V sistemih, v katerih poteka obravnavanje tajnih podatkov stopnje INTERNO, je naloga komisije, da pregleda vso zahteva dokumentacijo, pri šifrirnem ovrednotenju šifrirnih rešitev v sistemih, ki obravnavajo tajne podatke stopnje ZAUPNO, mora komisija poleg pregleda same dokumentacije izvesti še funkcionalni preizkus šifrirnih rešitev v celoti in posameznih šifrirnih mehanizmov. Pri obravnavanju tajnih podatkov stopnje TAJNO ali STROGO TAJNO pa je poleg navedenega v prejšnjem stavku potrebno izvesti še analizo možnosti kompromitiranja varnostno pomembnih parametrov, kar vključuje tudi penetracijske preizkuse.
Splošne varnostne zahteve šifrirnih rešitev:

- izvedeni morajo biti taki šifrirni primitivi, ki omogočajo zaščito tajnih podatkov,
- zaščitena mora biti pred nepooblaščenim ravnanjem ali uporabo,
- onemogočiti mora nepooblaščeno odkritje vsebine in varnostno pomembnih parametrov,
- onemogočiti mora nepooblaščeno in neugotovljivo spreminjanje šifrirnih modulov in algoritmov, vključno z nepooblaščenim spreminjanjem, nadomeščanjem, vrinjenjem ali izbrisom šifrirnih ključev in drugih varnostno pomembnih parametrov,
- med delovanjem mora biti vidno stanje, v katerem je,
- zagotovljeno mora biti pravilno delovanje varnostnih mehanizmov,
- zagotovljeno mora biti odkrivanje napak med delovanjem in vzpostavljen mehanizem, ki preprečuje kompromitiranje varnostno pomembnih parametrov.

Urad Vlade Republike Slovenije je pristojen za vodenje evidence šifrirnih rešitev, za katere je izdano potrdilo o varnostni ustreznosti.

5 Sinteza mnenj predstavnikov sodelujočih organov v komisiji za informacijko varnost

V diplomskem delu sem uporabila metodo strukturiranega intervjuja s odprtimi vprašanji, kar je intervjuvancem omogočilo, da prikažejo svoje videnje in mnenje o določenem problemu. S svojimi odgovori so mi predstavili stanje obravnavanja nacionalnih tajnih podatkov v IKS v

RS ter izpostavili tiste ključne pomankljivosti, ki si jih s skupnimi močmi prizadevajo odpraviti.

Vprašanja so se nanašala na naslednje obravnavane teme:

- sodelovanje intervjuvancev pri obravnavanju nacionalnih tajnih podatkov v informacijsko - komunikacijskem sistemu,
- ustanovitev enotnega IKS za obravnavanje nacionalnih tajnih podatkov,
- trenutno stanje IKS v Republiki Sloveniji,
- pomanjkljivosti regulative, ki urejajo področje obravnavanja tajnih podatkov,
- sodelovanje med organi pri obravnavanju nacionalnih tajnih podatkov,
- pristojnosti komisije za informacijsko varnost,
- primerjava RS, EU in NATO standardov pri akreditaciji IKS za obravnavanje nacionalnih tajnih podatkov.

Intervjuje sem opravila s predstavniki sodelujočih organov v Komisiji za informacijsko varnost in sicer so sodelovanje v intervjuje privolili g. Miha Habič iz MORSa, g. Franci Močilar iz MZZja, g. Dejan Žorž iz MNZja, g. Igor Eršte iz UVTPja, g. Damijan Marinšek iz MJUja, medtem, ko pa je predstavnik SOVE sodelovanje odklonil zaradi službene dolžnosti.
Predstavnik MORSa v Komisiji za informacijsko varnost, g. Miha Habič, zastopa stališča Ministrstva za obrambo RS ter predstavlja strokovna mnenja za katera meni, da so pomembna in pravilna pri obravnavi posameznih gradiv.
Z g. Habičem sem se dogovorila za intervju na podlagi dejstva, da mi kot član komisije lahko posreduje določene informacije, katere bi sama težko pridobila le iz analize sekundarne literature. Prav tako lahko njegove odgovore primerjam z odgovori ostalih intervjuvancev in na ta način pridem do zaključka raziskovalnega dela in ovržem ali sprejmem hipotezo oziroma raziskovalno vprašanje. Na ta način lahko z večjo gotovostjo ovrednotimo trenutno stanje obravnavanja tajnih podatkov v RS, saj s tem pridobimo merodajneše podatke za analizo obravnavanja nacionalnih tajnih podatkov.
Na začetku intervjuja mi je g. Habič predstavil njegovo vlogo in vlogo MORSa pri sodelovanju v medresorski komisiji z informacijsko varnost.
V nadaljevanju je na podlagi svojih izkušenj in strokovnosti ocenil trenutno stanje obravnavanja nacionalnih tajnih podatkov v RS in izpostavil dejstvo da je največja

pomanjkljivost prav premajhna ozaveščenost o relevantnosti tega problema ter grožnje o odtekanju tajnih podatkov.

Največja pridobitev RS z enotnim IKS bi bila po njegovem mnenju varna medsebojna komunikacija med organi, prav tako pa se strinja, da bi skupen IKS organom omogočil večjo povezljivost in boljše medresorsko sodelovanje pri obravnavanju nacionalnih tajnih podatkov (Habič 2010).

G. Franc Močilar, predstavnik MZZja v Komisiji za informacijsko varnost zastopa in predstavlja stališča organa ter skuša na ta način vplivati na dvig nivoja informacijske varnosti v RS. Mnenja, ki mi jih je v intervjuju predstavil g. Močilar so vzeta predvsem iz prakse obravnavanja nacionalnih tajnih podatkov v informacijsko - komunikacijskem sistemu med Ministrstvom za zunanje zadeve in Uradom Vlade RS za varovanje tajnih podatkov ter v sodelovanju z drugimi organi, ki so del Komisije za infomacijsko varnost.

Podobno kot g. Habič navaja, da je še vedno največji problem premajhno zavedanje o pomembnosti tega področja ter posledično s tem tudi premajhna konkretna podpora s strani države v obliki financ, kadrov.

Z enotnim IKS bi v RS rešili veliko odprtih vprašanj in poenostavili medsebojno izmenjavo nacionalnih tajnih podatkov med organi. Izpostavil je tudi relevantnost izmenjave podatkov v elektronski obliki, kar bi zelo poenostavili z ustanovitvijo enotnega IKS (Močilar 2010).

V nadaljevanju intervjuja je predstavil tudi postopek odobritve uporabe šifrirnih rešitev, katero KIV odobri na podlagi ustrezne dokumentacije, kjer so podrobno opisani tehnični, organizacijski in drugi mehanizmi predlagane rešitve. Kriteriji, po katerih KIV ocenjuje to dokumentacijo in ustreznost šifrirnih rešitev se ravnajo po EU in NATO standardih.

Eden od predstavnikov MNZja v Komisiji za informacijsko varnost je tudi g. Dejan Žorž, s katerim sem se dogovorila za intervju z namenom, da mi predstavi vlogo MNZja pri sodelovanju v tej komisiji ter izpostavi oziroma opredeli svojo podpredsedniško funkcijo.

Ker MNZ na področju, ki ga pokriva komisija nima primernih kadrov, ga zato zastopata predstavnika Policije.

Naloga g. Žorža je, da kot predstavnik Policije zastopa interese RS, Policije in MNZja. Prizadeva si tudi za primerno predstavitev mnenj in stališč policije pri obravnavanju tajnih podatkov v informacijsko - komunikacijskem sistemu.

Tekom intervjuja je primerjal trenutni sistem varovanja tajnih podatkov po zgledu zahodnih integracij in poudaril, da smo ob tem zanemarili obstoječo varnostno kulturo, medtem ko nove še nismo povsem realizirali. Sprejeta je bila le na »papirju«, v praksi pa še ne (Žorž 2010).

G. Žorž poudarja, da dokler ne bomo vzpostavili potrebnih institucij na ustreznem organizacijskem nivoju ter jih primerno kadrovsko, finančno in tehnično opremili, realno ne moremo pričakovati boljših rezultatov.

Tako kot g. Habič in g. Močilar se tudi sam strinja z vzpostavitvijo enotnega informacijsko - komunikacijskega sistema za obravnavanje nacionalnih tajnih podatkov, saj bi na ta način smiselno povezali resorje organov med sabo med samim prenosom tajnih podatkov, ter tako občutno zmanjšali stroške vzdrževanja sistema.

G. Žorž se strinja s trditvijo, da bi enoten informacijsko - komunikacijski sistem omogočil večjo povezljivost in boljše medresorsko sodelovanje pri obravnavanju nacionalnih tajnih podatkov ter izpostavi dejstvo, da bi skupen IKS omogočil elektronsko pošiljanje tajnih podatkov, kar bi omogočilo vse prednosti elektronskega poslovanja.

Razlog, zakaj RS še nima povsem izoblikovanih standardov za akreditacijo šifrirnih rešitev je po njegovem mnenju prav premalo sredstev in nezanimanje Vlade RS za to področje, saj je oblikovanje standardov proces, ki se razvija kar nekaj časa in za to potrebuje finančna sredstva.

Kot naslednjega intervjuvanca bi želela omeniti g. Igorja Eršteta, ki je kot predsedujoči zadolžen za sklic in vodenje sestankov Komisije za informacijsko varnost ter v veliki meri za vsebinsko pripravo gradiv oziroma za usklajevanje gradiva, ki ga Komisija na svojih sejah obravnava.

Tako kot njegovi kolegi, katere sem predhodno intervjuvala, navaja, da se še vedno premalo zavedamo relevantnosti problema obravnavanja nacionalnih tajnih podatkov ter da bi v bodoče bilo potrebno spremeniti varnostno ozaveščenost vseh, ki imajo dostop do tajnih podatkov.

Tudi sam je naklonjen vzpostavitvi enotnega informacijsko - komunikacijskega sistema za obravnavanje nacionalnih tajnih podatkov, saj bi tako pridobili varen in zanesljiv način medsebojnega izmenjevanja tajnih podatkov.

Postopek odobritve uporabe šifrirnih rešitev obravnava Komisija na svojih sestankih in če je potrebno, zahteva dopolnitev dokumentacije, katero ji mora organ predhodno predložiti. G. Igor Eršte kot predsedujoči v KIV navaja, da pri evalvaciji teh sistemov uporabljajo standarde EU in zveze NATO, saj imamo kot enakopravni člani teh zvez dotop do njihovih standardov, kar je zaenkrat dovolj (Eršte 2010).

Zaradi boljšega kritičnega ovrednotenja trenutnega sistema obravnavanja tajnih podatkov v informcijsko komunikacijskem sistemu v RS sem želela intervjuvati tudi predstavnika SOVE v KIV, vendar pa je sodelovanje v intervjuju zavrnil zaradi službene dolžnosti.

Kot zadnjega sodelujočega v intervjuju naj omenim še g. Damijana Marinška, edega od predstavnikov Ministrstva za javno upravo v KIV. Slednji mi je v intervjuju predstavil vlogo Ministrstva, ki je predvsem skrb za skupno omrežje državnih organov – HKOM. Poudaril je, da se bodo na tej infrastrukturi omrežja gradile rešitve za prenos tajnih podatkov.

Tudi g. Marinšek podobno kot ostali intervjuvanci poudarja, da je še vedno premajhna ozaveščenost eden glavnih problemov s katerimi se trenutno spopadajo na področju obravnavanja nacionalnih tajnih podatkov (Marinšek 2010).

Tako kot ostali intervjuvanci je tudi sam naklonjen vzpostavitvi enotnega informacijsko - komunikacijskega sistema in poudarja, da je ta rešitev nujno potrebna. Skupen IKS bi organom omogočil večjo povezljivost in sodelovanje na način enotnega obravnavanja nacionalnih tajnih podatkov v sklopu pošiljanja, hranjenja, uničevanja in dostopanja do le - teh.

Tako kot predsednik Komisije, g. Igor Eršte je tudi sam mnenja, da zaenkrat lastnih standardov za akreditacijo šifrirnih rešitev ne potrebujemo, saj so standardi EU in zveze NATO dovolj.

Tabela 5.1: Primerjava individualnih pogledov

INDIVIDUALNI POGLEDI/ INTERVJUJI	OCENA TRENUTNEGA STANJA	NAJVEČJE POMANKLJIVOSTI PRI OBRAVNAVANJU TP	PRIDOBITVE Z VZPOSTAVITVIJO ENOTNEGA IKS	RAZLOGI ZA NEIZOBLIKOVANE STANDARDE ŠIFRIRNIH REŠITEV V RS
g. Miha Habič (MORS)	Premajhna ozaveščenost o problematiki na tem področju	Nezadostna podpora (kadrovska, finančna)	Poenostavljena medresorska komunikacija.	Sodelovanje RS v mednarodnih asociacijah in upoštevanje tehnološkega razvoja šif. rešitev ter prekratka tradicija RS.
g. Franc Močilar (MZZ)	Premajhno zavedanje o relevantnosti obravnavanja TP	Premajhna konkretna podpora pri delovanju.	Poenostavljena medsebojna izmenjava podatkov.	Večina standardov (EU in NATO) je uporabnih tudi v RS. Pomanjkanje kadra (premalo strokovnjakov).
g. Dejan Žorž (MNZ)	Prenovljen sistem varovanja TP po zgledu zahodnih integracij in ob tem zanemarjena obstoječa varnostna kultura.	Premajhna kadrovska, finančna in tehnična podpora pri obravnavanju TP.	Manjši stroški vzdrževanja IKS.	Oblikovanje standardov je dolgotrajen proces, kateremu je potrebno nameniti bistveno več finančnih sredstev, kot pa jih ima sistem sedaj.
g. Igor Eršte (UVTP)	Izboljšanje stanja v zadnjih dveh letih. Vendar je še vedno premalo pozornosti nemenjene temu problemu.	Premajhna varnostna ozaveščenost oseb, ki imajo dostop do tajnih podatkov.	Varen in zanesljiv način medsebojnega izmenjevanja tajnih podatkov.	Zaradi članstva RS v EU in zvezi NATO imamo dodstop do njihovih standardov, zaradi česar je izoblikovanje lastnih v ta namen nesmiselno.
G Damijan Marinšek (MJU)	Premajhna ozaveščenost.	Majhnost in razdrobljenost državnih organov in s tem posledično večji stroški zagotavljanje varnostne kulture.	Varen in zanesljiv način medsebojnega izmenjevanja TP.	Zaradi članstva RS v zvezi NATO in EU izoblikovanje lastnih standardov ni potrebno.

6 Zaključek

Kar nekaj časa in truda je bilo potrebnega, da smo kot samostojna država dočakali povabilo v organizacijo EU in zvezo NATO. Izpolnili smo vse zahteve za članstvo v obeh integracijah, kot enakovreden partner pa bomo morali na določenih področjih še marsikaj storiti.

S sprejetjem Zakona o tajnih podatkih smo v RS zadostili zahtevam pogajalskih izhodišč za vstop v EU in tako združili posamezna področja obravnavanja tajnih podatkov, katera so bila delno že urejena v zakonih oziroma v podzakonskih aktih (Černetič in Brožič 2003).

Sistem varovanja tajnih podatkov se je v RS začel vzpostavljati v obdobju osamosvojitve, ko je država morala na novo urediti zakonodajo, kar je za tiste čase predstavljalo velik in odgovoren projekt (Kozlevčar 2007).

Trenutno stanje obravnavanja nacionalnih tajnih podatkov v RS se kaže v premajhni ozaveščenosti o problematiki na tem področju, nezadostni kadrovski in finančni podpori ter tehnični oskrbi. Vlada RS še vedno ne posveča dovolj pozornosti temu področju, kar se kaže predvsem pri samem obravnavanju nacionalnih tajnih podatkov, pa naj gre za varovanje, distribucijo ali arhiviranje le teh.

Nekateri nacionalni organi imajo že dodobra razvite svoje lastne informacijsko - komunikacijske sisteme v katerih obravnavajo tajne podatke, da pa bi v prihodnje okrepili sodelovanje državnih institucij. Na tem področju bi bilo potrebno v ta namen vzpostaviti skupen informacijsko - komunikacijski sistem za obravnavanje nacionalnih tajnih podatkov.

Vsi predstavniki organov, ki sodelujejo v KIV, so v intervjujih podali pozitivno menenje glede vzpostavitve enotnega informacijsko - komunikacijskega sistema za obravnavanje nacionalnih tajnih podatkov. G. Habič, predstavnik MORSa v KIV je pri tem izpostavil poenostavljeno medsebojno komunikacijo med organi, kar bi posledično zmanjšalo stroške za zagotavljanje ustrezne varnosti in medsebojno izmenjavo teh podatkov. Trenutna razdroljenost državnih organov terja največje organizacijsko tehnične stroške na področju zagotavljanja varnosti, pravi g. Damijan Marinšek, in obenem navaja, da je rešitev v obliki enotnega informacijsko - komunikacijskega sistema nujno potrebna in je že v fazi priprave javnega naročila.

V RS smo prenovili sistem varovanja tajnih podatkov po zgledu EU in zveze NATO in med tem zanemarili obstoječo varnostno kulturo. Več bi morali storiti na področju usposabljanja ustreznega kadra, saj trenutno primanjkuje strokovnjakov, ki bi pripomogli k razvoju informacijsko - komunikacijske tehnologije, ter varnostni ozaveščenosti tistih, ki imajo dovoljenje za dostop do tajnih podatkov.

Enoten IKS pa bi kot organizacijsko tehnična rešitev moral zagotoviti vsakemu državnemu organu ustrezno zasebnost, saj dovoljenje za dostop do tajnih podatkov še ne daje pravice videti vseh tajnih podatkov, navaja g. Habič. Tudi g. Močilar je podobnega mnenja in pravi, da bi pri načrtovanju takega sistema morali upoštevati tudi želje organov po njihovi avtonomnosti. G. Dejan Žorž se strinja z navedenim, navede pa tudi primer, da bi pokroviteljstvo nad sistemom prevzel centralni organ z ustreznimi pooblastili in bi ga nato s primerno vladno podporo ponudil vsem organom, tako ne bi prišlo do nasprotovanja s strani posameznih organov.

Skupen informacijsko - komunikacijski sistem bi organom omogočil večjo povezljivost in boljše medresorsko sodelovanje pri obravnavanju nacionalnih tajnih podatkov, se strinjajo vsi intervjuvanci, g. Žorž pa še dodaja, da bi enotnost IKS omogočila elektronsko pošiljanje, kar omogoča vse prednosti elektronskega poslovanja.

Za ustrezno obravnavanje tajnih podatkov uporabljajo posamezni organi med drugim tudi šifrirne rešitve, katere mora KIV predhodno odobriti. Komisija v ta namen izda navodilo o postopku odobritve uporabe šifrirnih rešitev, ki daje organom določene smernice pri pripravi ustrezne dokumentacije, katero morajo skupaj s predlogom posredovati na UVTP oziroma na KIV. RS zaradi svoje kratke zgodovine še nima povsem izoblikovanih standardov za evalvacijo teh sistemov, niti se ni na tem področju kaj dosti razvijalo, saj se pred KIV ni nihče resno ukvarjal z razvojem teh smernic. Vsi intervjuvanci so podobnega mnenja, da zaradi polnopravnega članstva v EU in zvezi NATO ne potrebujemo lastnih standardov za akreditacijo šifrirnih rešitev.

Pomen izvedbe enotnega IKS je okrepiti sodelovanje organov RS pri obravnavanju nacionalnih tajnih podatkov. Tako okrepljeno sodelovanje bi zagotovilo večjo varnostno kulturo ter s tem posledično tudi manjše kadrovske in tehnične stroške, ki nastajajo zaradi trenutnega kaotičnega stanja obravnavanja nacionalnih tajnih podatkov.

Enoten IKS bi zagotavljal poenostavljeno medresorsko komunikacijo, manjše stroške vzdrževanja IKS, hitrejšo izmenjavo podatkov ter manjše stroške zagotavljanja varnostne kulture.

Na podlagi literature, ki sem jo preučila med pisanjem diplome, in podatkov, ki sem jih pridobila med intervjuvanjem, lahko potrdim svojo zastavljeno hipotezo, da bi za obravnavanje nacionalnih tajnih podatkov v Republiki Sloveniji bil potreben enoten informacijsko - komunikacijski sistem, ki bi okrepil sodelovanje med organi in rešil vprašanje povezljivosti med njimi. Da bi se rešitev lahko realizirala pa bo zato potrebna konkretna

podpora Vlade RS, ki bo omogočila zadostno finančno, tehnološko in kadrovsko pomoč, da bo tak sistem lahko sploh funkcioniral.

7 Literatura

1. Anžič, Andrej. 1996. *Vloga varnostnih služb v sodobnih parlamentarnih sistemih – nadzorstvo*. Ljubljana: Enotnost.
2. ---1997. *Varnostni sistem Republike Slovenije*. Ljubljana: Uradni list RS.
3. ---2000. Tajnost: vrednota in zlo. *Teorija in praksa* 37 (5): 849 – 863.
4. Anžič, Andrej in Franc Trbovšek. 2003. Varnostno preverjanje v NATO po novih standardih: (povzetek). V *dnevi varstvoslovja*. Ur. Milan Pagon in Iztok Podbregar, 118 – 128. Ljubljana: visoka policijsko varnostna šola.
5. Bohinc, Rado. 2001. *Uvodni nagovor.* V javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, ur. Igor belič, 5 – 8. Ljubljana: ministrstvo za notranje zadeve.
6. Brezovšek, Marjan in Damir Čenčec. 2007. *Demokratična uprava in tajnost podatkov*. Ljubljana: Fakulteta za družbene vede.
7. Bučar, Bojko, Zlatko Šabič, Milan Brglez in Monika Kalin – Golob, ur. 2002. *Navodila za pisanje: seminarske naloge in diplomska dela*. Ljubljana: Fakulteta za družbene vede.
8. Čaleta, Denis. 2003. *Trend razvoja slovensko obveščevalno – varnostne skupnosti po vstopu v EU in NATO*. 4. Slovenski dnevi varstvoslovja. Ljubljana: Visoka policijsko varnostna šola.
9. Černetič, Metod in Liliana Brožič. 2003. *Potrebe po novhi znanjih – varovanje tajnih podatkov v Evropski uniji in zvezi NATO*. Organizacija 36 (8): 575 – 582.
10. Črnčec, Damir. 2003. *Tajnost podatkov: varnostno preverjanje in obveščevalno varnostne službe*. Magistersko delo. Ljubljana: Fakulteta za družbene vede.
11. Eckerson, Wayne W. 2002. *Data quality and the bottom line*. Achieving business success through a commitment to high quality data. The data warehousing.
12. Eršte, Igor. 2010. Intervju z avtorico. Ljubljana, 19. april.
13. Habič, Miha. 2010. Intervju z avtorico. Ljubljana, 12. april.
14. Hajtnik, Tatjana. 2002. *Priporočila za pripravo informacijske varnostne politike*. Ljubljana: Center Vlade za informatiko.
15. Hartman, Ervin. 2007. *Varovanje tajnih podatkov in varnostna kultura na obrambnem področju: protiobveščevalno – varnostni vidik:* specialistično delo. Ljubljana: Fakulteta za družbene vede.
16. Korošec, Sabina. 2006. *Varnostno preverjanje v Republiki Sloveniji: Diplomsko delo*. Ljubljana: Fakulteta za družbene vede.

17. Kozlevčar, Marjan. 2007. *Organizacijske in administrativne ovire pri delu s tajnimi podatki*: magistersko delo. Univerza v Ljubljani: Fakulteta za upravo.
18. Laudon Kenneth c. in Laudin Jane Price. 1995: *Information Systems – a problem solving approach.* Orlando: The Dryden Press.
19. Marinšek, Damijan. 2010. Intervju z avtorico. Ljubljana, 20. april.
20. Močilar, Franci. 2010. Intervju z avtorico. Ljubljana, 14. april.
21. *Navodilo o izvajanju zaščite pred nezaželenim elektromagnetnim sevanjem v komunikacijskih in informacijskih sistemih, v katerih se obravnavajo tajnih podatki*. Ur. l. RS 48/2007 (19. november 2008).
22. *Navodilo o postopku odobritve uporabe šifrirnih rešitev*. Ur.l. RS 48/2007 (23.december 2008).
23. Oliver, Derek J. 2002. *Pregledni seminar za pripravo na izpit CISA*. Ljubljana: Slovenski inštitut za revizijo.
24. *Resolucija o strategiji nacionalne varnosti Republike Slovenije* Ur.l. RS 27/2010 (26.marec 2010).
25. *Security Whithin The Nort Atlantic Treaty organisation (NATO). Document C-M (2002)49.*
26. *Security Regulations of the Council of the European Union. (2001/264/EC), L 101 (19. marec 2001). Sklep Sveta EU z dne 19. marec 2001 o sprejetju predpisov Sveta skupnosti o varovanju tajnosti.*
27. *Sklep o ustanovitvi, nalogah in organizaciji Urada RS za varovanje tajnih podatkov.* Ur.l.RS 6/2010 (25.januar 2010).
28. *Uredba o upravnem poslovanju*. Ur. l. RS 20/2005 (4. marec 2005).
29. *Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov*. Ur. l. RS 138/2006 (28.december 2006).
30. *Uredba o varovanju tajnih podatkov*. Ur.l.RS 74/2005- UPB (20. avgust 2005).
31. *Uredba o varovanju tajnih podatkov v informacijsko komunikacijskih sistemih*. Ur. l. RS 48/2007 (1.junij 2007).
32. *Urad Vlade Republike Slovenije za varovanje tajnih podatkov: Navodilo za delo s tajnimi podatki zveze NATO in EU*. Dostopno prek: http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Navodila-tuji-TP.pdf (04. junij 2009).

33. *Urad Vlade Republike Slovenije za varovanje tajnih podatkov. 2009a. Informacijska varnost.* Dostopno prek: http://www.uvtp.gov.si/si/delovna_podrocja/informacijska_varnost/ (27.april 2009).
34. *---2009b. Naloge in cilji*. Dostopno prek: http://www.uvtp.gov.si/si/o_vladni_sluzbi/naloge_in_cilji/ (27. maj 2009).
35. *Ustava republike Slovenije* (URS). Ur.l. RS/I 33/1991. (23.12.1991). Objavljena dne 28.12.1991, začela veljati 23.decembra 1991, z dnem razglasitve.
36. Vidmar, Tone. 2002. *Informacijsko – komunikacijski sistem*. Ljubljana: Pasadena.
37. *Zakon o dostopu do informacij javnega značaja (ZDIJZ).* Ur. l. RS 24/2003 (22. marec 2003).
38. *Zakon o tajnih podatkih (ZTP).* Ur. l. RS 50/2006 – UPB2 (16. maj 2006).
39. Žorž, Dejan. 2010. Intervju z avtorico. Ljubljana, 14. april.
40. Žurga, Gordana. 2001. *Kakovost državne uprave: pristopi in rešitve*. Ljubljana: Fakulteta za družbene vede.

8 Seznam prilog

Priloga A: Intervju z g. Miho Habičem

Ljubljana, MORS; 16.04.2010

1. **Kakšna je vloga MORSa v medresorski komisiji za informacijsko varnost?**

   Predstavnik Ministrstva za obrambo v Komisiji za informaicjsko varnost zastopa stališča Ministrstva za obrambo in je z ostalimi člani, ki so jih na osnovi uredbe imenovali drugi državni organi, enakopraven .

2. **Lahko prosim na kratko opišete oziroma opredelite vašo vlogo, kot predstavnik MORSa v medresorski komisiji za informacijsko varnost.**

   Kot predstavnik Ministrstva za obrambo zastopam stališča ministrstva oziroma predstavljam strokovna stališča za katera menim, da so pri obravnavi posameznih gradiv, ki jih komisija obravnava, pomembna oziroma pravilna.

3. **Kako bi vi opisali trenutno stanje obravnavanja nacionalnih tajnih podatkov v RS? Kje so po vašem mnenju največje pomankljivostiP**

   Premajhna ozaveščenost o pomembnosti tega ter grožnjah odtekanja tajnih podatkov. Nepripravljenost temu področju posvetiti večjo pozornost (kadrovsko, finančno, …)

4. **Kakšno je vaše mnenje o enotnem informacijsko - komunikacijskem sistemu za obravnavanje nacionalnih tajnih podatkov?**

   Pozitivno. S tem bi poenostavili medsebojno komunikacijo.

5. **Kaj bi RS pridobila z vzpostavitvijo enotnega IKS. Tehnično bi bil izvedljiv in s strani organov zelo zaželjen, vendar se poraja vprašanje »v kolikšni meri bi se posamezni organi strinjali z enotnim IKS?«**

   Možnost varne medsebojne komunikacije.
   Kakršna koli tehnična rešitev pa bi morala vsakemu državnemu organu zagotoviti ustrezno zasebnost saj nenazadnje dovoljenje za dostop do tajnih podatkov še ne daje pravice videti vseh tajnih podatkov.

6. **Skupen IKS bi organom omogočil večjo povezljivost in boljše medresorsko sodelovanje pri obravnavanju nacionalnih tajnih podatkov. Se strinjate z navedeno trditvijo?**

   DA

7. **KIV v skladu s svojimi pristojnostmi izda tudi navodilo o postopku odobritve uporabe šifrirnih rešitev. Lahko, na kratko opišete kako poteka ta postopek odobritve. Na podlagi katerih kriterijev ocenjujete predloženo dokumentacijo? EU in NATO standardi?**

   Vlagatelj posreduje zahtevo za odobritev na Komisijo (UVTP). Pri tem tudi priloži potrebno tehnično dokumentacijo ali jo tudi v samem postopku po potrebi dopolni. Komisja gradivo obravnava s tem, da vsaj zaenkrat komisija za izhodišča evalvacije uporablja priznanen mednarodne standarde. NATO dokumentacija je vsaj z mojega stališča ena od pomembnejših. Seveda pa se uporabljajo tudi drugi standardi (EU v kolikor obstajajo, FIPS, …).

8. **Zakaj, po vašem mnenju RS še nima povsem izoblikovanih svojih standardov za akreditacijo šifrirnih rešitev?**

   Mogoče zaradi tega, ker na tem področju v R Sloveniji ni tako dolge tradicije kot v nekaterih drugih državah.
   Glede na dejstvo, da se v mednarodnih asocijacijah katerih članica je tudi Slovenija (EU, NATO) izdelujejo tudi takšni dokumenti in ob upoštevanju tehnološkega razvoja

šifrirnih rešitev najverjetneje ne obstaja upravičen razlog za izdelavo povsem lastnih standardov.

Priloga B: Intervju z g. Francijem Močilarjem

Ljubljana, MZZ; 16.04.2010

1. **Kako poteka sodelovanje MZZja v komisiji za informacijsko varnost?**

   MZZ v komisiji za informacijski varnost sodeluje enakopravno z ostalimi člani. Imamo enega člana in enega nadomestnega člana, tako kot ostali resorji. Vsi člani komisije dobro sodelujemo.

2. **Lahko prosim na kratko opišete oziroma opredelite vašo vlogo, kot predstavnik MZZja v medresorski komisiji za informacijsko varnost.**

   Kot predstavnik MZZ-ja v komisiji predstavljam in zastopam stališča MZZ-ja in hkrati, z ostalimi člani, skušam tudi vpivati na dvig nivoja informacijske varnosti v RS.

3. **Kako bi vi opisali trenutno stanje obravnavanja nacionalnih tajnih podatkov v RS? Kje so po vašem mnenju največje pomankljivosti?**

   Za nacionalne tajne podatke je bilo narejenega že ogromno dela. Precejšen korak naprej je bilo sprejetje Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih v letu 2007. Največji problem je po mojem mnenju še vedno premajhno zavedanje o pomebnosti tega področja ter posledično premajhna konkretna podpora temu področju, v obliki financ, kadrov itd.

4. **Kakšno je vaše mnenje o enotnem informacijsko - komunikacijskem sistemu za obravnavanje nacionalnih tajnih podatkov?**

   Enotni sistem za obravnavanje nacionalnih tajnih podatkov bi rešil veliko problemov ter poenostavil medsebojno izmenjavo teh podatkov.

5. **Kaj bi RS pridobila z vzpostavitvijo enotnega IKS. Tehnično bi bil izvedljiv in s strani organov zelo zaželjen, vendar se poraja vprašanje »v kolikšni meri bi se posamezni organi strinjali z enotnim IKS?«**

   Z enotnim IKS bi mnogim organom spoh omogočili izmenjavo tajnih podatkov v elektronski obliki, vsem organom pa olajšali medsebojno izmejavo. Seveda bi morali pri načrtovanju tega sistema upoštevati tudi želje organov po njihovi avtonomnosti.

6. **Skupen IKS bi organom omogočil večjo povezljivost in boljše medresorsko sodelovanje pri obravnavanju nacionalnih tajnih podatkov. Se strinjate z navedeno trditvijo?**
   Se popolnoma strinjam.

7. **KIV v skladu s svojimi pristojnostmi izda tudi navodilo o postopku odobritve uporabe šifrirnih rešitev. Lahko, na kratko opišete kako poteka ta postopek odobritve. Na podlagi katerih kriterijev ocenjujete predloženo dokumentacijo? EU in NATO standardi?**

   Predlagatelj mora v postopek odobritve priložiti tudi ustrezno dokumentacijo, kjer so podrobneje opisani tehnični, organizacijski in drugi mehanizmi predlagane rešitve. Kot kriterije za oceno ustreznost uporabljamo EU in NATO standarde ter tudi druge standarde s tega področja, kot so ISO/IEC družina standardov 27000, Common Criteria, FIPS itd.

8. **Zakaj, po vašem mnenju RS še nima izoblikovanih svojih standardov za akreditacijo šifrirnih rešitev?**

   Seveda ni potrebno, da Slovenija napiše svoje standarde, saj je večina standardov uporabnih tudi v RS. Sicer je glavni razlog kadrovski, ker so za to potrebni strokovnjaki. Tudi člani komisije bi radi marsikaj naredili, a nam pomanjkanje časa zaradi drugih stalnih obveznosti to onemogoča.

Priloga C: Intervju z g. Dejanom Žoržem

Ljubljana, MNZ; 14.04.2010

1. **Kakšna je vloga MNZja v medresorski komisiji za informacijsko varnost?**

MNZ v komisiji zastopata predstavnika Policije, saj MNZ na področju ki, ga pokriva komisija nima primernih kadrov. Predstavnika v komisiji zastopata interese RS, Policije in MNZ.

2. **Lahko prosim na kratko opišete oziroma opredelite vašo vlogo, kot predstavnik MNZja v medresorski komisiji za informacijsko varnost.**

Osebno imam podpredsedniško funkcijo, vendar v praksi delujem enakopravno z drugimi predstavniki. Kot predstavnik Policije seveda skrbim za primerno predstavitev mnenja Policije v komisiji.

3. **Kako bi vi opisali trenutno stanje obravnavanja nacionalnih tajnih podatkov v RS? Kje so po vašem mnenju največje pomankljivosti?**

V RS smo prenovili sistem varovanja podatkov zaupne narave po zgledu zahodnih integracij. Ob tem smo zanemarili obstoječo varnostno kulturo in nove še nismo vzpostavili. Pomemben del inštitucij, ki se je ukvarjal s tem področjem, je po razpadu SFRJ ostal izven RS. Zaradi različnih razlogov novih nismo uspeli vzpostaviti oziroma smo jih vzpostavili le "na papirju". Dokler ne bomo vzpostavili potrebnih inštitucij na ustreznem organizacijskem nivoju in jih primerno kadrovsko, finančno in tehnično opremili, realno ne moremo pričakovati boljših rezultatov.

4. **Kakšno je vaše mnenje o enotnem informacijsko - komunikacijskem sistemu za obravnavanje nacionalnih tajnih podatkov?**

Menim, da je to primerna in celo priporočljiva rešitev, vendar mora tak sistem striktno izpolnjevati vrsto varnostnih zahtev.

5. **Kaj bi RS pridobila z vzpostavitvijo enotnega IKS. Tehnično bi bil izvedljiv in s strani organov zelo zaželjen, vendar se poraja vprašanje »v kolikšni meri bi se posamezni organi strinjali z enotnim IKS?«**

Podatke višjih stopenj tajnosti je potrebno prenašati med sorazmerno malo točkami, Te točke se nahajajo v različnih resorjih, zato je smiselno resorje med seboj povezati z enotnim sistemom. S skupnim sistemom se tudi zmanjšajo stroški vzdrževanja.
V primeru, da bi pokroviteljstvo nad sistemom prevzel centralni organ s pravimi in dovolj pristojnostmi ter ga s primerno vladno podporo ponudil vsem organom, ne bi prišlo do nasprotovanja s strani posameznih organov. Trenutno takega centralnega organa ni.

6. **Skupen IKS bi organom omogočil večjo povezljivost in boljše medresorsko sodelovanje pri obravnavanju nacionalnih tajnih podatkov. Se strinjate z navedeno trditvijo? Prosim utemeljite.**

Organi lahko tajne podatke višjih stopenj med seboj pošiljajo elektronsko zaščiteno ali po kurirski pošti. IKS bi omogočil elektronsko pošiljanje, ki omogoča vse prednosti elektronskega poslovanja.

7. **KIV v skladu s svojimi pristojnostmi izda tudi navodilo o postopku odobritve uporabe šifrirnih rešitev. Lahko, na kratko opišete kako poteka ta postopek odobritve. Na podlagi katerih kriterijev ocenjujete predloženo dokumentacijo? EU in NATO standardi?**

Postopek odobritve poteka v skladu z Navodilom o postopku odobritve uporabe šifrirnih rešitev. Odvisno od rešitve se izvedejo različni postopki, ki so navedeni v navodilu, od odobritve na podlagi že pridobljene akreditacije do analize delovanja posameznih komponent rešitve. V vsakem primeru je potrebno najprej pridobiti ustrezno dokumentacijo na podlagi katere je možno pridobiti informacije o rešitvi in njenem delovanju.

8. **Zakaj, po vašem mnenju RS še nima povsem izoblikovanih svojih standardov za akreditacijo šifrirnih rešitev?**

Oblikovanje standardov je proces. RS je z postopki odobritve uporabe bolj sistematično pričela šele z Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, ki je bila izdana v letu 2007. Proces bi potekal hitreje, če bi vlada RS za to področje namenila več sredstev.

Priloga Č: Intervju z g. Igorjem Erštetom

Ljubljana, UVTP; 19.04.2010

1. **Kakšna je vloga UVTP ja v medresorski komisiji za informacijsko varnost?**

   Predstavnik UVTP vodi Komisijo za informacijsko varnost in nekako predstavlja gonilno silo Komisije. Drugače pa je v enakopravnemu položaju z ostalimi člani in zastopa mnenje UVTP. UVTP za potrebe Komisije opravlja strokovno administrativna dela (po potrebi se vključijo ostali organi).

2. **Lahko prosim na kratko opišete oziroma opredelite vašo vlogo, kot predsedujoči v komisiji za informacijsko varnost.**

   Kot predsedujoči sem zadolžen za sklic in vodenje sestankov Komisije za informacijsko varnost ter v veliki meri za vsebinsko pripravo gradiv oz. usklajevanje gradiva, ki ga komisija obravnava.

3. **Kako bi vi opisali trenutno stanje obravnavanja nacionalnih tajnih podatkov v RS? Kje so po vašem mnenju največje pomanjkljivosti.**

   Čeprav se je stanje v zadnjih dveh – treh letih izboljšalo, imamo še vedno nekako »mačehovski« odnos do nacionalnih tajnih podatkov. Predvsem je potrebno spremeniti odnos oz. varnostno ozaveščenost vseh, ki imajo dostop do tajnih podatkov. Temu problemu je potrebno v vseh organih nameniti večjo pozornost.

4. **Kakšno je vaše mnenje o enotnem informacijsko - komunikacijskem sistemu za obravnavanje nacionalnih tajnih podatkov?**

   Pozitiven!

5. **Kaj bi RS pridobila z vzpostavitvijo enotnega IKS. Tehnično bi bil izvedljiv in s strani organov zelo zaželjen, vendar se poraja vprašanje »v kolikšni meri bi se posamezni organi strinjali z enotnim IKS?«**

   Varen in zanesljiv način medsebojnega izmenjevanja tajnih podatkov. Osebno menim, da bi se ob pravilni postavitvi in upravljanju IKS ter seveda ob predhodnem »medsebojnem dogovoru« in dostopa do tajnih podatkov posameznega organa na podlagi potrebe po vedenju, organi z postavitvijo enotnega IKS strinjali.

6. **Skupen IKS bi organom omogočil večjo povezljivost in boljše medresorsko sodelovanje pri obravnavanju nacionalnih tajnih podatkov. Se strinjate z navedeno trditvijo? Prosim argumentirajte.**

   Da. Menim, da je dosedanja praksa na področju izmenjevanja tajnih podatkov pokazala, da tak IKS potrebujemo.

7. **KIV v skladu s svojimi pristojnostmi izda tudi navodilo o postopku odobritve uporabe šifrirnih rešitev. Lahko, na kratko opišete kako poteka ta postopek odobritve. Na podlagi katerih kriterijev ocenjujete predloženo dokumentacijo? EU in NATO standardi?**

   Predlagatelj predlog skupaj z zahtevano dokumentacijo posreduje na UVTP oz. Komisijo za informacijsko varnost. Komisija predlog obravnava na svojem sestanku in po potrebi zahteva dopolnitev dokumentacije oz. izvedbo drugih del. Evalvacija oz. postopek šifrirnega ovrednotenja poteka na podlagi priznanih mednarodnih standardov. Pri tem so seveda najpomembnejši standardi zveze NATO in EU.

8. **Zakaj, po vašem mnenju RS še nima povsem izoblikovanih svojih standardov za akreditacijo šifrirnih rešitev?**

   S to problematiko se zadnjih dvajset let, razen MORS-a in SOVE (oboji le za lastne potrebe), do ustanovitve Komisije za informacijsko varnost nihče ni ukvarjal. V Sloveniji na tem področju, razen dveh – treh manjših proizvajalcev tudi nimamo omembe vredne industije oz. izvoznikov. Ker imamo kot člani zveze NATO in EU dostop do njihovih (naših) standardov smatram, da izoblikovanje svojih standardov ni smiselna.

Priloga D: Intervju z g. Damijanom Marinškom

Ljubljana, MJU; 20.04.2010

1. **Kakšna je vloga MJUja v medresorski komisiji za informacijsko varnost?**

Predstavnika MJU v KIV sodelujeta kot tvorna člana skupine. S svojim znanjem in pokrivanjem področja dela se s kolegom Markom Erjavcem vključujeva v delo skupine. MJU skrbi za omrežje javne uprave – HKOM. Na infrastrukturi tega omrežja se bodo gradile rešitve za prenos tajnih podatkov.

2. **Lahko prosim na kratko opišete oziroma opredelite vašo vlogo, kot predstavnik MJUja v medresorski komisiji za informacijsko varnost.**

Sam nimam neke posebne vloge, v skupini sodelujem enakovredno z drugimi člani KIV. Pri svojem delu zastopam stališča MJU.

3. **Kako bi vi opisali trenutno stanje obravnavanja nacionalnih tajnih podatkov v RS? Kje so po vašem mnenju največje pomankljivosti?**

Premajhna ozaveščenost o pomembnosti tega ter grožnjah odtekanja tajnih podatkov. Majhnost in razdrobljenost državnih organov povečuje stroške za zagotavljanje ustrezne varnosti tako organizacijsko kot tehnološko.

Se pa vsaj na tehničnem področju pripravlja ustrezna rešitev,ki bo podpirala obravnavo tajnih podatkov v informacijsko - komunikacijskih sistemih.

4. **Kakšno je vaše mnenje o enotnem informacijsko - komunikacijskem sistemu za obravnavanje nacionalnih tajnih podatkov?**

Rešitev je v nujno potrebna in je v fazi priprave javnega naročila.

5. **Kaj bi RS pridobila z vzpostavitvijo enotnega IKS. Tehnično bi bil izvedljiv in s strani organov zelo zaželjen, vendar se poraja vprašanje »v kolikšni meri bi se posamezni organi strinjali z enotnim IKS?«**

Varen in zanesljiv način medsebojnega izmenjevanja tajnih podatkov. Osebno menim, da bi se ob pravilni postavitvi in upravljanju IKS ter seveda ob predhodnem »medsebojnem dogovoru« in dostopa do tajnih podatkov posameznega organa na podlagi potrebe po vedenju, organi z postavitvijo enotnega IKS strinjali.

6. **Skupen IKS bi organom omogočil večjo povezljivost in boljše medresorsko sodelovanje pri obravnavanju nacionalnih tajnih podatkov. Se strinjate z navedeno trditvijo? Prosim utemeljite.**

Da. Predvsem pa bi enoten sistem na enoten način urejal obravnavanje tajnih podatkov, pri tem gre za pošiljanje, hranjenje, uničevanje in dostop do teh podatkov.

7. **KIV v skladu s svojimi pristojnostmi izda tudi navodilo o postopku odobritve uporabe šifrirnih rešitev. Lahko, na kratko opišete kako poteka ta postopek odobritve. Na podlagi katerih kriterijev ocenjujete predloženo dokumentacijo? EU in NATO standardi?**

Predlagatelj predlog skupaj z zahtevano dokumentacijo posreduje na UVTP oz. KIV. KIV predlog obravnava na svojem sestanku in po potrebi zahteva dopolnitev dokumentacije oz. izvedbo drugih del. Evalvacija oz. postopek šifrirnega ovrednotenja poteka na podlagi

priznanih mednarodnih standardov. Pri tem so seveda najpomembnejši standardi zveze NATO in EU.

8. Zakaj, po vašem mnenju RS še nima povsem izoblikovanih svojih standardov za akreditacijo šifrirnih rešitev?

Do ustanovitve Komisije za informacijsko varnost se na nacionalnem nivoju nihče ni ukvarjal s tem področjem razen MORS za vojaške potrebe in SOVA za potrebe obveščevalne službe. Do ustanovitve Komisije za informacijsko varnost se na nacionalnem nivoju nihče ni ukvarjal s tem področjem razen MORS za vojaške potrebe in SOVA za potrebe obveščevalne službe. Izoblikovanje lastnih standardov ni smiselno, saj ima RS kot polnopravna članica dostop do le teh.

Priloga E: Vzorec potrdila o varnostni ustreznosti

Vzorec potrdila o varnostni ustreznosti

Glava izdajatelja potrdila

Izdajatelj potrdila na podlagi prvega odstavka 4. člena Navodila o postopku odobritve uporabe šifrirnih rešitev izdaja

POTRDILO O VARNOSTNI USTREZNOSTI

za šifrirno napravo/sistem _____ _____

proizvajalca

_____,

ki se bo uporabljala v sistemu _____

_____

za prenos tajnih podatkov do stopnje tajnosti

STOPNJA TAJNOSTI

Potrdilo velja od _____

do/za dobo _____

Številka:
Datum:

Pečat podpis predstojnika

Številka dokumenta:

Priloga F: Seznam zahtevane dokumentacije za akreditacijo šifrirnih rešitev

Zahtevana dokumentacija

1. Opis varnostnih funkcij, ki jih šifrirna rešitev izvaja.

2. Opis šifrirne rešitve (modula), in sicer:
   a. specifikacija strojnih, programskih in strojno-programskih sestavnih delov, specifikacija drugih sestavnih delov, ki niso varnostno pomembni, in opis materialnega videza;
   b. specifikacija fizičnih vhodov/izhodov in logičnih vmesnikov z določenimi vhodnimi/izhodnimi potmi;
   c. specifikacija ročnih in logičnih kontrol šifrirnih rešitev, specifikacija fizičnih in logičnih kazalnikov statusa;
   d. specifikacija vseh varnostnih funkcij in načinov delovanja;
   e. bločni diagram vseh pomembnejših strojnih ali/in programskih podsklopov s poudarkom na sestavinah, kjer so varnostno pomembni parametri;
   f. specifikacija vseh varnostno pomembnih parametrov, kot so šifrirni algoritmi, generatorji naključnih števil, razni šifrirni protokoli, šifrirni ključi (tajni in javni), avtentikacijski podatki (pin, geslo), in drugi varnostno pomembni parametri, katerih razkritje bi lahko ogrozilo varnost šifrirne rešitve;
   g. specifikacija varnostne politike uporabe in delovanja šifrirnega modula.

3. Opis vlog in funkcij pooblaščenih uporabnikov šifrirne rešitve ter opis avtentikacijskega mehanizma, in sicer:
   a. specifikacija vseh avtoriziranih vlog, ki jih podpira šifrirna rešitev;
   b. specifikacija vseh funkcij, servisov in operacij;
   c. specifikacija avtentikacijskih mehanizmov, opis avtentikacijskih podatkov in inicializacije.

4. Opis modela končnih stanj.

5. Opis fizične varnosti:
   a. specifikacija fizične materialne zaščite;
   b. specifikacija postopka brisanja varnostno pomembnih parametrov, če šifrirna rešitev omogoča vzdrževalni dostop;
   c. specifikacija okoljskih parametrov (temperatura, vlažnost, napajanje, ...) operativnega delovanja.

6. Opis operativnega okolja:
   a. specifikacija operativnega okolja glede na možnost spreminjanja funkcionalnosti že delujoče šifrirne rešitve;
   b. specifikacija operacijskega sistema.

7. Opis upravljanja šifrirnih ključev:
   a. specifikacija vseh šifrirnih ključev ali sestavnih delov, s pomočjo katerih ključi nastajajo;
   b. specifikacija vseh generatorjev naključnih števil;
   c. specifikacija načinov za generiranje šifrirnih ključev;
   d. specifikacija načinov za vzpostavljanje šifrirnih ključev;
   e. specifikacija postopka vnosa in iznosa šifrirnih ključev;
   f. specifikacija načinov shranjevanja šifrirnih ključev;
   g. specifikacija postopka brisanja šifrirnih ključev.

8. Opis samopreizkušanja:
    a. specifikacija postopka samopreizkušanja, vključno s preizkušanjem pri zagonu in vsemi pogojnimi preizkusi;
    b. specifikacija stanj, ko samopreizkušanje ni uspešno, in postopek za vzpostavitev ponovnega normalnega operativnega delovanja;
    c. specifikacija vseh varnostno kritičnih funkcij, ki se pri zagonu šifrirne rešitve preverijo;
    d. specifikacija mehanizma izključitve varnostnih funkcij šifrirne rešitve, če ta obstaja.

9. Opis varnostnega jamstva življenjskega cikla šifrirne rešitve:
    a. specifikacija postopkov za varno generiranje, namestitev in zagon šifrirne rešitve, vključno z morebitno nadgradnjo z novimi različicami;
    b. specifikacija, ki povezuje razvito šifrirno rešitev z navedenimi varnostnimi funkcijami;
    c. specifikacija izvorne programske kode in bločna predstavitev posameznih varnostno pomembnih programskih podsklopov;
    d. specifikacija strojne opreme in bločna predstavitev posameznih varnostno pomembnih strojnih podsklopov;
    e. specifikacija (za vse programske, strojne in strojno-programske sestavne dele) vhodnih parametrov, vseh funkcij, ki se izvedejo na podlagi vhodnih parametrov, ter pričakovanih rezultatov, ko se te funkcije izvedejo;
    f. specifikacija za navodila kriptoadministratorju:
        i. administrativne funkcije, varnostni dogodki, varnostni parametri, fizični in logični vmesniki, ki jih bo uporabljal;
        ii. postopek za varno upravljanje šifrirne rešitve;
        iii. predpostavke, ki so varnostno pomembne glede na ravnanje uporabnika šifrirne rešitve;
    g. specifikacija za navodila uporabniku:
        i. odobrene varnostne funkcije, fizični in logični vmesniki, ki jih bo uporabljal;
        ii. naloge, ki zagotavljajo varno delovanje šifrirne rešitve.