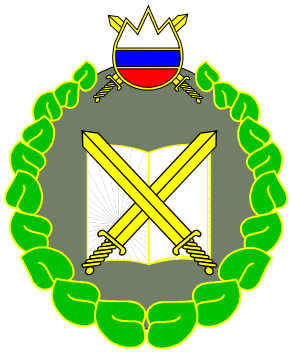
ŠOLA ZA ČASTNIKE
XVII. GENERACIJA

SPECIALIZACIJA NZP



Zaključna naloga

VARNOSTNA ZAGOTOVITEV V CNKZP

Kandidat: nvu VII Grega OSOJNIK

Mentor: st Goran VAREK

Ljubljana, september, 2007

POVZETEK

V zaključni nalogi z naslovom Varnostna zagotovitev Centra za nadzor in kontrolo zračnega prostora Brnik (v nadaljevanju CNKZP) je predstavljen sistem varovanja tajnih podatkov, ki predstavlja temelj za postavitev ustreznega varnostnega sistema.

16. bataljon za nadzor zračnega prostora (v nadaljevanju 16.BNZP) in z njem CNKZP sta bili eni prvih enot Slovenske vojske, ki sta bili interoperabilni ter operativni znotraj Severno atlantske zveze (NATO-North Atlantic Treaty Organisation). To pomeni, da poleg obdelovanja, hranjenja, pošiljanja in uničevanja nacionalnih tajnih podatkov, enako postopata ob delu s tajnimi podatki zveze NATO. Celovit in ustrezen sistem varovanja tajnih podatkov je tako bistvenega pomena za operativnost CNKZP, ki mu omogoča delo znotraj NATO integriranega sistema zračne obrambe (NATINADS–NATO Integrated Air Defence System).

Predstavljeni so vsi organi in njihove vloge pri vzpostavitvi ustreznega sistema varovanja tajnih podatkov, tako na nacionalni, kot tudi na mednarodni ravni. V sklopu zaključne naloge so predstavljeni nekateri izredni dogodki, ki se lahko pojavijo in ukrepi, kateri morajo biti izvajani ob pojavu teh dogodkov.

KLJUČNE BESEDE

Varovanje tajnih podatkov, fizična varnost, kadrovska varnost, varnost informacij, varnost informacijskih in komunikacijskih sistemov, zakoni in uredbe, načrt varovanja tajnih podatkov.

SUMMARY

In presented work Security system establishment for Control and Reporting Center Brnik (CRC Brnik) is described and presented system of security for accessing classified data, which represents the foundaments for establishment of appropriate security system.

The 16th airspace surveillance battalion and CRC Brnik, as a part of this battalion, were one of the first NATO interoperable and operative units, within Slovenian Armed Forces (SAF). That means that both units are accessing, keeping, distributing and destroying classified data of national interest and also those concerning NATO. Advanced and suitable system for protection of classified data, from being accessed by unauthorised person, is essential for everyday work of CRC Brnik, as a part of NATINADS (NATO Integrated Air Defence System).

Work includes detailed presentation of all national and some of international security organisations and agencies and their interaction, influence and obligations within the establishment of security system for protecting classified data. There is also a part, which is presenting possible actions and scenarios in case of environmental or other disasters, with suitable and recommended actions being taken.

KEY WORDS

Protection of classified data, physical security, personnel security, security of information, communications and informations systems security, law and regulations, plan for security protection of classified data.

KAZALO

1 UVOD

1.1 IZHODIŠČE ZAKLJUČNE NALOGE

V zaključni nalogi je podrobno razdelan in predstavljen sistem varnostne zagotovitve v Centru za nadzor in kontrolo zračnega prostora. Predstavljene bodo varnostne zahteve in standardi North Atlantic Treaty Organization (v nadaljevanju NATO) za Center za nadzor in kontrolo zračnega prostora (v nadaljevanju CNKZP) ter podobne objekte stacionarnega tipa. Opisani bodo dogodki, ki lahko ogrožajo varnost v CNKZP ter analiza postopkov v primeru teh izrednih dogodkov (požar, poplava, potres, ...).

1.2 NAMEN IN CILJI RAZISKAVE

Namen raziskave je podati splošen opis sistema varnostne zagotovitve za objekte z višjimi varnostnimi zahtevami, med katere spada tudi Center za nadzor in kontrolo zračnega prostora RS na Brniku. Cilj je podrobno predstaviti vse pravne podlage in normative, kateri omogočajo postavitev temeljev in podajajo osnovne smernice za nadgradnjo varnostnega sistema objektov stacionarnega tipa do željene varnostne stopnje. V raziskavi in analizi bodo vključeni tako nacionalni, kot tudi NATO predpisi in varnostne zahteve za omenjene tipe stacionarnih objektov.

1.3 METODE DELA

Pri izdelavi zaključne naloge bodo uporabljene analitična metoda dela in metoda dialoga, intervjuja z strokovnimi osebami s področja varnostne zagotovitve s strani enote, katera izvaja naloge zagotavljanja ustreznih varnostnih pogojev za CNKZP.

1.4 STRUKTURA ZAKLJUČNE NALOGE

Zaključna naloga je sestavljena iz večih poglavij, katera so v smiselnem vrstnem redu, tako da bralcu zaključne naloge v jedru naloge podajo ustrezne odgovore na zastavljena vprašanja in teme podane v izhodišču zaključne naloge. Zaključek naloge vsebuje sintezo ugotovitev in podaja izhajajoče smernice.

2 SPLOŠNO O RAVNANJU S TAJNIMI PODATKI IN OPREDELITEV OSNOVNIH POJMOV

Eden od pogojev za uspešno in učinkovito delovanje države predstavlja tudi zmožnost delovanja sistema in izvajanje dela sistemskih aktivnosti, za določen čas v tajnosti. Za dosego tega cilja je potrebno delovanje takega sistema opredeliti z ustreznimi varnostnimi zahtevami, kar se doseže z implementacijo zakonov in predpisov s področja varnosti. Državni organi z njihovo pomočjo varujejo svoje tajne podatke. Zmožnost ščitenja nacionalnih podatkov in interesov, kaže tudi zmožnost varovanja podatkov mednarodnih organizacij (zveze NATO in Evropske unije) ter tako predstavlja enega od pogojev za sodelovanje znotraj mednarodnih organizacij, katerih članica je tudi Republika Slovenija.

Proces vključevanja Republike Slovenije v zvezo NATO in Evropsko unijo je normativno urejanje varnostnega področja in področja varovanja tajnih podatkov še pospešil. Področje je precej široko, vendar podrobno razdelano tako na nacionalni ravni, kot tudi na ravni zveze NATO. Predpisi in zahteve slednje so za delovanje CNKZP še posebej pomembni, vendar morajo biti uskljajeni z nacionalnimi predpisi in zahtevami. V nadaljevanju so predstavljeni nekateri osnovni pojmi, kateri so bistveni za nadaljnje razčljenjevanje zastavljene izhodiščne teme, varnostne zagotovitve za delovanje CNKZP.

2.1 KAJ JE TAJNI PODATEK?

Tajni podatek je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami, in ki je v skladu s tem zakonom določeno in označeno za tajno (Zakon o tajnih podatkih – v nadaljevanju ZTP. Uradni list RS, št. 87/01). Podobna definicija tajnih podatkov je zapisana tudi v dokumentih Evropske unije in zveze NATO.

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 (ZTP. Uradni list RS, št. 87/01).

Varovanje tajnih podatkov je lahko učinkovito samo, če je vzpostavljen celoten sistem označevanja, določanja in dostopa do tajnih podatkov. Natančneje to pomeni, da je treba zagotoviti: ustrezno fizično in tehnično varovanje (vzpostavitev varnostnih območij); dosledno spoštovanje načela potrebe po vedenju; ustrezne postopke pridobitve varnostnega dovoljenja (potrdila); postopke za izdelavo, prenos, varovanje in uničevanje tajnih podatkov; vzpostavitev (pod)registrov; varovanje informacijskih sistemov in posredovanje tajnih podatkov drugim državam in mednarodnim organizacijam. Vse to je sistemsko urejeno v ZTP, ki ga je državni zbor sprejel leta 2001 in prvič dopolnil leta 2003. Zakon se je zgledoval po ureditvi tega področja v državah z dolgo demokratično tradicijo. Vsakdo, ki mu je zaupan tajni podatek ali njegova vsebina, ga je dolžan varovati v skladu z veljavnimi predpisi (Črnec, 2004, 18).

Kadar je treba podatek označiti kot tajen, se mu določi ustrezna stopnja tajnosti. Z sprejetjem ZTP je v Sloveniji poenotena terminologija, ki se uporablja pri ravnanju s tajnimi podatki. Določen je enovit sistem označevanja podatkov, oziroma razvrščanje stopenj tajnih podatkov. V Sloveniji imamo primerljiv sistem označevanja z Evropsko unijo in zvezo NATO. Ti uporabljata štiristopenjski sistem označevanja tajnih podatkov: STROGO TAJNO, TAJNO, ZAUPNO in INTERNO. Za poenotenje standardov in koordinacijo vseh aktivnosti je bil ustanovljen Urad za varovanje tajnih podatkov.

Oznake in stopnje tajnosti tajnih podatkov po NATO klasifikaciji in primerljive slovenske oznake:
NATO UNCLASSIFIED–Brez stopnje tajnosti (ne sme izven NATO strukture)
NATO RESTRICTED–INTERNO
NATO CONFIDENTAL-ZAUPNO
NATO SECRET-TAJNO
NATO COSMIC TOP SECRET(ATOMAL)-STROGO TAJNO

2.2 DOSTOP DO TAJNIH PODATKOV

Dokument, kateri določa predpise, aktivnosti in ukrepe za dostopanje do tajnih podatkov je Uredba o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov. Posamezniku je omogočen dostop do tajnih podatkov šele, ko je ustrezno varnostno preverjen in je to preverjanje uspešno prestal.

Ta uredba določa način in postopek varnostnega preverjanja oseb, ki morajo zaradi opravljanja funkcij, nalog ali delovnih dolžnosti v organu dobiti dovoljenje za dostop do tajnih podatkov, ter postopek izdaje in preklica tega dovoljenja, če ni določen že z ZTP (Uradni list RS, št. 87/01, 1.člen Uredbe o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov).

Do tajnih podatkov stopnje INTERNO ima dostop vsak zaposlen v organu, če podpiše izjavo s katero se zavezuje, da pozna predpise kateri urejajo varovanje tajnih podatkov in da bo ravnal s tajnimi podatki v skladu s temi predpisi (3.člen ZTP). Dovoljenje za dostop do tajnih podatkov stopnje ZAUPNO, TAJNO in STROGO TAJNO se pridobi po uspešno opravljenem varnostnem preverjanju ter podpisani izjavi o seznanjenosti z ZTP in predpisi, ki urejajo varovanje tajnih podatkov. Dostop do tajnih podatkov je mogoč ob izpolnjevanju dveh pogojev. Prvi pogoj je, da oseba poseduje ustrezno dovoljenje za dostop do tajnih podatkov, izdan s strani poooblaščenega organa. Drugi pogoj je izkazana potreba po vedenju (upravičen interes). Takoimenovani ”need to know” pomeni, da mora oseba izkazati upravičen interes za dostop do tajnih podatkov, ker brez vpogleda v določene tajne podatke ne more opravljati svoje funkcije ali delovnih nalog (glej Črnec, 2004, 19).

V praksi to pomeni da oseba, katera poseduje dovoljenje za dostop do tajnih podatkov stopnje STROGO TAJNO in dela v določenem uradu ali službi, nima dostopa do podatkov katerekoli stopnje tajnosti in kateregakoli oddelka urada ali službe. Izkazana mora biti upravičenost interesa za dostop do tajnih podatkov. Nekatere države zveze NATO so postavile še rigidnejše zahteve in poleg teh dveh pogojev zahtevajo še takoimenovano listo dostopa do tajnih podatkov (access list). Ob izpolnjevanju prvih dveh pogojev morajo biti vse osebe, katere

izkažejo upravičenost interesa in posedujejo dovoljenje za dostop do tajnih podatkov, še na listi dostopa, katero izda pristojni organ.

Varnostno preverjanje oseb je zbir aktivnosti, postopkov in ukrepov s pomočjo katerih se ugotovi primernost posameznikov za delo na varnostno občutljivem delovnem mestu ali za ravnanje s tajnimi podatki. Dokument kateri določa in ureja postopke za preverjanje oseb je Uredba o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov (Ur. list RS, št. 110/03). Priloge uredbe so soglasja in vprašalniki za različne vrste preverjanja. Sama vsebina varnostnega preverjanja je določena v 25.členu ZTP. V Sloveniji se omenjeni postopki izvajajo od leta 2001 in sicer od sprejetja ZTP. ZTP opredeljuje varnostno preverjanje oseb kot poizvedbo, ki jo pred izdajo dovoljenja za dostop do tajnih podatkov opravi pristojni organ in namen katere je zbiranje podatkov o morebitnih varnostnih zadržkih.

V Sloveniji varnostno preverjanje opravlja več organov in služb. V Ministrstvu za obrambo (v nadaljevanju MO) opravlja varnostno preverjanje Obveščevalno-varnostna služba (v nadaljevanju OVS) MO. To opravlja za zaposlene v MO in Slovenski vojski, ter za osebe, ki bodo pri svojem delu uporabljale tajne podatke z obrambnega področja. Policija opravlja varnostno preverjanje za svoje zaposlene, Slovenska varnostno–obveščevalna agencija za svoje zaposlene, za vse ostale, ki potrebujejo dovoljenje za dostop do tajnih podatkov, pa Služba za tajne podatke Ministrstva za notranje zadeve.

Glede na predvideni dostop osebe do tajnih podatkov različnih stopenj tajnosti, pristojni organ opravi različno obsežno varnostno preverjanje. Osnovno za dostop do tajnih podatkov stopnje ZAUPNO, razširjeno za dostop do tajnih podatkov TAJNO in razširjeno varnostno preverjanje, z varnostnim poizvedovanjem za dostop do tajnih podatkov stopnje STROGO TAJNO. Osnovno preverjanje vsebuje preverjanje posameznikovih navedb v osnovnem vprašalniku za varnostno preverjanje ter podatkov iz evidenc in drugih zbirk podatkov upravljalcev zbirk podatkov. Pri razširjenem varnostnem preverjanju kandidat izpolni še posebni vprašalnik, podatki se lahko preverijo pri referenčnih osebah zgolj ob pojavu varnostnega zadržka. Ob izvajanju razširjenega preverjanja z varnostnim poizvedovanjem, po izpolnitvi osnovnega, posebnega in prvega dela dodatnega vprašalnika, lahko organ, zgolj v primeru pojava varnostnega zadržka, preveri podatke pri drugih osebah, organih ali organizacijah, ki o preverjeni osebi kaj vedo (22.d člen ZTP). Ta dikcija omogoča ti. ”terensko preverjanje”.

Zveza NATO in Evropska unija ne izvajata varnostnih preverjanj, ampak je to v domeni držav članic. Nacionalno dovoljenje za dostop do tajnih podatkov je podlaga za pridobitev osebnega potrdila za dostop do tajnih podatkov zveze NATO (PSC-Personal Security Certificate). Ključna kriterija za verodostojnost posameznika sta nedvomno lojalnost (državi, organizaciji) in zanesljivost (na delovnem mestu in izven njega). Dvom v lojalnost in zanesljivost je glavno merilo potrjevanja varnostnih zadržkov. Prav tako je poleg teh kriterijev upoštevanih še več ostalih kriterijev. Eden izmed teh kriterijev je tudi neposedovanje dvojnega državljanstva, kar je predstavljalo za nekatere posameznike s področje Slovenije manjši problem. Razlog zato je iskati v dejstvu, da je po razpadu Jugoslavije bilo mnogo državljanov Slovenije, kateri so bili v družinskih skupnostih iz mešanih zakonov in posledično z dvojnim državljanstvom.

2.3 VAROVANJE TAJNIH PODATKOV

To področje je v Sloveniji urejeno z sprejemom Uredbe o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov (Ur. list RS, št.70/02). Uredba je bila sprejeta v letu 2002 in predstavlja osnovne zahteve za postavitev sistema varovanja tajnih podatkov, od njihovega označevanja, hranjenja in do prenosa. Določa načine in oblike označevanja tajnih podatkov ter fizične, organizacijske in tehnične ukrepe, katerih namen je onemogočiti dostop ali razkritje tajnih podatkov. Fizični ukrepi vsebujejo neposredno fizično varovanje tajnih podatkov ter varovanje prostorov ali objektov. Organizacijski ukrepi vsebujejo pripravo, izdelavo, hranjenje in uničevanje tajnih podatkov. Tehnični ukrepi so ukrepi varovanja tajnih podatkov ter varovanja prostorov ali objektov, v katerih se tajni podatki nahajajo, s pomočjo tehničnih sredstev in sistemov.

Uredba določa, da se lahko tajni podatki ne glede na stopnjo tajnosti obdelujejo in hranijo v določenem, vidno označenem in zaščitenem prostoru, objektu ali območju. V Sloveniji so, primerljivo z zvezo NATO, vzpostavljena tri varnostna območja, kjer se obdelujejo in hranijo tajni podatki ustrezne stopnje tajnosti. V varnostnem območju III.stopnje se obdelujejo in hranijo tajni podatki stopnje INTERNO, v varnostnem območju II.stopnje se obdelujejo in hranijo tajni podatki stopnje ZAUPNO, v varnostnem območju I.stopnje pa se obdelujejo in hranijo tajni podatki stopnje TAJNO in STROGO TAJNO, praviloma se hranijo v ločenih prostorih (po Črnec, 2004, 19).

Nadzor vstopa in izstopa v varnostna območja je točno opredeljen z ZTP (Ur. list RS, št. 87/01) in z Uredbo o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov (Ur. list RS, št.70/02). Kriteriji se glede na stopnjo varnostnega območja ustrezno zvišujejo, se pravi so progresivno restriktivni. Pogoji vstopa v najstrožje varovano območje I.varnostne stopnje so najbolj restriktivni. Osebe lahko vstopajo v tako območje samo, če so tam zaposlene ali druge osebe, vendar morajo imeti vsi dovoljenje za dostop do tajnih podatkov najmanj stopnje TAJNO. Izkazati morajo upravičen interes (need to know), prihod zunanjega obiskovalca pa mora biti ustrezno najavljen. Vsi vstopi preko varnostne točke se evidentirajo, preveriti je potrebno identiteto posameznika, izkazan upravičen interes in dovoljenje, kjer je potrebno (nekatere članice NATO) pa mora biti oseba na listi dostopa. Vnos mehanskih in elektronskih naprav (mobilni telefoni, fotoaparati, diktafoni) v prostore I.varnostne stopnje je potrebno preprečiti, v območju mora biti prisotna oseba odgovorna za obdelavo, hranjenje in dostopanje do tajnih podatkov.

Vsi prostori I.varnostnega območja, vključno z kontrolno točko in potjo do nje morajo biti nadzorovani z video sistemom. Vsakih šest mesecev ali po vsakem posegu v prostoru mora biti opravljen protiprisluškovalni pregled prostorov območja I.varnostne stopnje. Tajni podatki stopnje TAJNO in tajni podatki stopnje STROGO TAJNO se lahko hranijo v istem prostoru, vendar morajo biti hranjeni v ločenih blagajnah. Blagajna za tajne podatke stopnje TAJNO mora biti ognjevzdržna, z vgrajeno ključavnico in sistemom protivlomnega javljanja. Blagajna za hranjenje tajnih podatkov stopnje STROGO TAJNO mora imeti poleg prej naštetih zahtev, nameščen še protitrgalni senzor. Strogi kriteriji veljajo tudi za prenos tajnih podatkov, tajne podatke stopnje TAJNO lahko prenaša ena oborožena oseba, stopnje STROGO TAJNO pa dve oboroženi osebi (Črnec, 2004, 19).

Naloga vsakega organa, enote ali službe je, da ustrezno spoštuje in izvaja določila zakona ter podzakonskih predpisov. Način izvedbe je razviden iz načrta varovanja tajnih podatkov (v nadaljevanju NV). NV je sestavljen iz splošnega in posebnega dela, natančneje opredeljuje ukrepe varovanja, opis objektov, odgovornost posameznikov in postopke ob nepredvidenih dogodkih ali razkritju tajnega podatka. Načrte je potrebno stalno dopolnjevati in nadgrajevati. Tak načrt varovanja mora biti v vseh objektih I. in II. varnostnega območja in zato ima izdelanega tudi CNKZP. Načrt mora biti označen in hranjen ustrezno glede na stopnjo oznake tajnega podatka.

Z uvedbo ZTP in ostalih podzakonskih aktov ter določil je veliko sprememb tudi na področju pridobivanja poslov v takoimenovani namenski industriji. Za pridobitev poslov je veliko odvisno tudi od izpolnjevanja pogojev varnostne zagotovitve pri hranjenju, obdelovanju, varovanju in prenosu tajnih podatkov. Podjetja, katera bodo hotela pridobiti posle zaupne narave, bodisi za potrebe MO ali zveze NATO, bodo dolžna izpolnjevati tudi vse predpisane varnostne kriterije. Izpolnjevati bodo morala vse fizične, organizacijske in tehnične zahteve za varovanje tajnih podatkov ustreznih stopenj. Dolžna bodo varnostno preveriti vse osebe z dostopom do tajnih podatkov, ki morajo podpisati izjavo o seznanjenosti, podjetje pa mora zagotoviti, da bo dovolilo vpogled samo osebam, ki izpolnjujejo kriterij upravičenosti interesa. Ko pooblaščeni državni organ izvede nadzor podjetju, ki izpolnjuje vse prej naštete zahteve, izda varnostno potrdilo. Veljavno varnostno potrdilo je pogoj za pridobitev posla, ki vključuje tajne podatke v kakršnikoli obliki.

2.4 VARNOSTNA POLITIKA ZVEZE NATO

Za polnopravno članstvo v katerikoli mednarodni organizaciji je nujno potrebna uvedba standardizirane ureditve varnostne politike. To usklajevanje je morala opraviti tudi Slovenija ob vstopu v Evropsko unijo (01.05.2004) in zvezo NATO (29.03.2004). Usklajevanja je bilo potrebno izvesti na vseh področjih, od varnostnega preverjanja ali zagotavljanja ustreznih postopkov in ukrepov za varovanje tajnih podatkov. Kljub upoštevanju vseh fizičnih, organizacijskih in tehničnih ukrepov brez ustrezne varnostne kulture vseh, ki ravnajo s tajnimi podatki, ni učinkovitega sistema varovanja tajnih podatkov.

Izdano nacionalno dovoljenje je podlaga za pridobitev dovoljenja za dostop do tajnih podatkov zveze NATO. Pomembnost varnostnega področja za uspešno delovanje zveze NATO je razvidno iz dokumentov, ki urejajo varnostno področje zveze. Postopki ravnanja s tajnimi podatki so natančno predpisani, kot tudi način njihovega označevanja, posredovanja, hranjenja, uničevanja in dostopa. NATO je v letu 2002 izdal ključne dokumente s področja varovanja tajnih podatkov, ki so nadgradili prej obstoječi varnostni sistem zveze NATO. Dopolnjene rešitve so bile nadgrajene v skladu z novimi varnostnimi izzivi.

Severnoatlantski svet (North Atlantic Council-v nadaljevanju NAC) je 26.03.2002 potrdil sprejetje dokumentov C-M(2002)49 Security within NATO–Varnost znotraj zveze NATO in C-M(2002)50 Protection Measures for NATO Civil and Military Bodies, deployed NATO Forces and Installations (Assets) against Terrorist Threats–Varnostni ukrepi NATO civilnih in vojaških organov, aktiviranih NATO Sil in objektov proti terorističnim grožnjam. Oba dokumenta sta nasledila dokument C-M (55)15(Final). C-M(2002)49 zavezuje vse stranke iz dokumenta in civilno vojaške organe-NATO, da ščitijo in varujejo tajne podatke, ki izvirajo iz

zveze ali jih države članice posredujejo drugi državi članici v okviru programa/projekta ali pogodbe NATO. Ščitijo in varujejo se tudi tajni podatki, zaupani nenatovskim organom ali posameznikom (Črnec, 2004, 20).

Sprejete so bile tudi naslednje direktive, ki skupaj s prejšnima dokumentoma predstavljajo varnostno politiko NATO:

- AC/35-D/2000 Directive on Personnel Security (Kadrovska varnost);
- AC/35-D/2001 Directive on Physical Security (Fizična varnost);
- AC/35-D/2002 Directive on Security of Information (Varnost informacij);
- AC/35-D/2003 Directive on Industrial Security (Industrijska varnost);
- AC/35-D/2004 Primary Directive on INFOSEC (Varnost informacijskih sistemov);
- AC/35-D/2005 INFOSEC Management Directive for CIS (Communications Informations System) (Direktiva za upravljanje varnosti komunikacijsko informacijskih sistemov).

Poleg omenjenih dokumentov je izredno pomemben dokument, kateri opredeljuje osnovne varnostne zahteve AD 70-1(ACO (Allied Command Operations – Operativa Združenega Poveljstva) Security Directive (Varnostna Direktiva), number (št.) 70-1 izdan s strani NAC. Dokument AD 70-1 je sestavljen iz šestih delov, ki vsak opredeljujejo določeno varnostno področje:

- PART 1: GENERAL (SPLOŠNO);
- PART 2: PHYSICAL SECURITY AND COUNTER TERRORISM/SABOTAGE (Fizična varnost in zaščita pred terorističnimi dejanji in sabotažami);
- PART 3: SECURITY OF INFORMATION (Varnost informacij);
- PART 4: PERSONNEL SECURITY (Kadrovska varnost);
- PART 5: INFOSEC (Varnost informacijskih sistemov);
- PART 6: SECURITY PROCEDURES (Varnostni postopki).

Vsi zgoraj omenjeni dokumenti predstavljajo osnove za izdelavo in postavitev ustreznih varnostnih sistemov znotraj članic zveze NATO. Ti omogočajo ščitenje in varovanje tajnih podatkov vseh stopenj, znotraj vseh kategorij varnostnih območij, ter s tem posledično omogočajo varen pretok tajnih podatkov v vseh oblikah, znotraj vseh organov zveze NATO. CNKZP je NATO integrirana enota v sklopu NATO Integrated Air Defence System-NATO integrirani sistem zračne obrambe(v nadaljevanju NATINADS) in je kot del zveze NATO dolžan za operativno izvajanje nalog v sklopu zveze izvajati vse varnostne ukrepe predpisane s strani NATO.

3. PODROČJA IZVAJANJA UKREPOV ZA VAROVANJE TAJNIH PODATKOV

Dokumenti, ki opredeljujejo varnostne postopke, ukrepe in aktivnosti v CNKZP so določeni z zakoni, uredbami in predpisi na nacionalni ravni. Ti se nahajajo na ustrezni lokaciji (v blagajni), v varnostni mapi , kjer se hranijo vedno ažurirane izdaje zakonov in podzakonskih aktov. Te predstavljajo osnovne reference in usmeritve za doseganje željenega varnostnega nivoja v objektih stacionarnega tipa, kot je CNKZP. Vsi ti postopki, aktivnosti in predpisi se izvajajo z namenom doseganja višje, oziroma opredeljene stopnje varnosti na definiranem varnostnem območju. Slovenska zakonodaja opredeljuje varnostne zahteve za objekte stacionarnega tipa, v grobem, predvsem na tri področja. Področje fizične, organizacijske in tehnične varnosti. Na nacionalni ravni so pomembni predvsem dokumenti, kot so:

- Zakon o tajnih podatkih (ZTP).
- Uredba o varovanju tajnih podatkov.
- Uredba o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov.
- Uredba o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov.

Iz zgoraj omenjenih predpisov izhajata spodnja predpisa, ki sta interna, vendar obvezna:

- Hišni red Centra za nadzor in kontrolo zračnega prostora (interni dokument).
- Načrt varovanja tajnih podatkov (interni dokument s stopnjo tajnosti).

Terminologija NATO in Evropske skupnosti se v nekaterih delih nekoliko razlikujeta od slovenske opredelitve. V NATO opredelitvi so ukrepi za varovanje tajnih podatkov razdeljeni na sledeča področja izvajanja ukrepov varovanja tajnih podatkov:

- kadrovska varnost,
- fizična varnost,
- varnost informacij,
- varnost informacijskih sistemov,
- industrijska varnost.

Na podlagi teh skupin bodo v nadaljevanju skozi terminologijo NATO (preglednost in opis področij) predstavljeni ukrepi in dejavnosti s področja varovanja tajnih podatkov, ki jih določa slovenska zakonodaja.

Ukrepi sprejeti in predpisani v nekem organu in temeljijo na neki veljavni zakonski podlagi, morajo zajeti vse zaposlene, ki imajo dostop do tajnih podatkov, ter vse objekte in naprave, kjer se ti podatki obdelujejo, hranijo in prenašajo. Zakon predpisuje le minimalne ukrepe za varovanje tajnih podatkov. To pomeni da se lahko organ, glede na pomembnost tajnih podatkov, ki jih varuje, odloči za restriktivnejše ukrepe, ob oceni da je to nujno potrebno.

3.1 KADROVSKA VARNOST

Glavni cilj in namen kadrovske varnosti je zagotavljati ustrezen sistem varnostnega preverjanja za vse zaposlene, ki bodo imeli v organu dostop do tajnih podatkov stopnje ZAUPNO in višje. Po opravljenem varnostnem preverjanju, se zaposlenemu na podlagi ugotovitev, izda dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti. Po

končanem postopku varnostnega preverjanja se odobri dostop do tajnih podatkov. V kategorijo oseb, ki bodo imele pri svojem delu dostop do tajnih podatkov je potrebno šteti tudi kurirje, osebje za čiščenje, varnostno osebje in ostale osebe za katere obstaja verjetnost, da bodo pri svojem delu imeli stik s tajnimi podatki.

V vsakem organu, kateri obdeluje, hrani in prenaša tajne podatke stopenj ZAUPNO, TAJNO in STROGO TAJNO, se mora vzpostaviti evidenca dovoljenj za dostop do tajnih podatkov za vse osebe v organu, ki imajo taka dovoljenja. V enoti mora biti vzpostavljen organ, kateri je pooblaščen za sprožanje postopkov pridobitve novih dovoljenj za dostop do tajnih podatkov. Pomembni in natančno določeni so tudi postopki preklica dovoljenja za dostop do tajnih podatkov, ob ugotovljenih zakonsko določenih dejstev za tak preklic.

Pomemben ukrep na področju kadrovske varnosti je upravičenost interesa, oziroma NATO termin ”need to know”. To pomeni, da ima oseba dostop do tajnega podatka samo takrat, ko se mora s tajnim podatkom seznaniti, zaradi opravljanja funkcije ali delovnih nalog. Nobena oseba, ne glede na položaj, čin ali stopnjo dovoljenja za dostop do tajnih podatkov, se ne sme seznaniti s tem tajnim podatkom, če ne izkaže upravičen interes za vpogled vanj. Pomemben del izvajanja ukrepov zagotavljanja kadrovske varnosti je dvig varnostne kulture. Sem spada predvsem zavedanje o pomembnosti pravilnega ravnanja s tajnimi podatki. To zavedanje se lahko doseže skozi ustrezen sistem izobraževanja in izvajanja nadzorov, z namenom opozarjanja na morebitne nepravilnosti ter odmike od predpisanih minimalnih varnostnih zahtev. Sistem izobraževanja mora biti stalen in izdelan na podlagi ažuriranih predpisov in zahtev tako s strani nacionalnih zakonov in zakonskih podaktov, kot tudi s strani zveze NATO in njenih direktiv ter predpisov.

Pomembno področje zagotavljanja kadrovske varnosti je izdelava ustreznih postopkov za dostop do tajnih podatkov v izrednih primerih, kot so dostop do tajnih podatkov v primeru nastopa izrednih dogodkov. To so primeri dostopa, zaradi nujnih vzdrževalnih dejavnosti v varnostnem območju, dostopi v primeru izrednih situacij (primer požara ali drugih izrednih dogodkov), ter sodelovanje in prisotnost oseb brez ustreznega dovoljenja za dostop do tajnih podatkov na konferencah ali sestankih. V vseh primerih mora biti razvidno kdo je oseba, ki je odobrila dostop do tajnih podatkov v omenjenih situacijah. Pomembno vlogo na področju kadrovske varnosti igra tudi protiobveščevalna zaščita oseb in delovnih mest, na katerih se osebe srečujejo s tajnimi podatki različnih stopenj tajnosti (glej Čaleta, 2003, 102).

3.2 FIZIČNA VARNOST

Ukrepi fizične varnosti, ki jih predvideva ZTP, so namenjeni preprečitvi nepooblaščenega dostopa do tajnih podatkov. Ti ukrepi temeljijo na postavitvi varnostnih območij ustrezne stopnje v vseh organih, ki obdelujejo in shranjujejo tajne podatke. Ukrepi fizične varnosti so odvisni od različnih faktorjev:

- stopnje tajnosti podatkov, ki se obdelujejo;
- količina in oblike informacij ali tajnih podatkov (zapisi na papirju ali na prenosnih medijih);
- stopnje dovoljenj za dostop do tajnih podatkov oseb, zaposlenih v tem organu, ter upravičenost inetresa za vpogled v tajne podatke;

- ocene ogroženosti, v kateri se predvidevajo vsi vidiki kriminalnega, subverzivnega, terorističnega in ogrožanja s sabotažami.

Učinkovit sistem varnostne zagotovitve se doseže samo z učinkovito povezavo vseh področij varnostnega sistema. Pomembno vlogo igra tudi pravilna ocena varnostnih tveganj, ki ob pravilnih ocenah groženj sistemu varovanja tajnih podatkov, v povezavi z ugotovljenimi pomanjkljivostmi sistema, omogoča sprejemanje ustreznih ukrepov fizičnega varovanja.

Osnovne naloge in ukrepi fizičnega varovanja so določitev varnostnih območij in preprečitev nepooblaščenega dostopa do tajnih podatkov, ter izdelava sistema za odkrivanje in zaznavanje nepoobčlaščenega dostopa v varnostno območje in ustrezno alarmiranje z kratekim odzivnim časom moštva, namenjenega varovanju in intervenciji. Ukrepe, kateri sestavljajo področje fizičnega varovanja. bi lahko razdelili na ukrepe varovanja s tehničniimi sredstvi (tehnični sistemi varovanja, video nadzor, protivlomni in protipožarni sistemi, elektronski omejilniki vstopa), ukrepe varovanja z moštvom in gradbene ukrepe. Ukrepi varovanja z moštvom predstavljajo ustrezno varovanje na vstopno–izstopnih točkah, določitev intervencijskih sil za posredovanje v izrednih dogodkih (nasilni vstop v varnostno območje, požar ali druge naravne nesreče). Gradbeni ukrepi so pomembni predvsem za varnostna območja obdelovanja in hranjenja tajnih podatkov najvišjih stopenj (TAJNO, STROGO TAJNO). S temi ukrepi lahko že v začetni fazi močno izboljšamo varnost na določenem varnostnem območju, ter postavimo solidne temelje za nadaljnjo nadgraditev varnostnega sistema. Značilno za gradbene ukrepe je, da jih je lažje in končno ceneje upoštevati ob gradnji novih objektov, kot kasneje ob adaptaciji starih objektov (po Čaleta, 2003, 104).

3.3 VARNOST INFORMACIJ

Tajni podatki zahtevajo nekatere varnostne ukrepe, ki se redno izvajajo v sistemu varovanja tajnih podatkov. Potrebno je zagotoviti ukrepe za določanje stopnje tajnosti podatkom, njihovo označevanje in zagotovitev jasne razpoznavnosti ter določitev trajanja tajnosti (časovna opredelitev tajnosti podatka). Pomembno vlogo pri teh postopkih ima originator. Ta določi stopnjo tajnosti podatka, ki ga je izdelal in označil kot tajnega. Obenem je odgovoren tudi za posredovanje tega podatka drugim, ki morajo biti po njegovi oceni seznanjeni z njim. Samo originator lahko podatku zniža, spremeni ali umakne stopnjo tajnosti. Ob nastanku tajnega podatka določi način znižanja ali prenehanje njegove tajnosti. Določitev ustrezne stopnje tajnosti podatka določa kakšno bo njegovo bodoče hranjenje, obdelava in razpošiljanje ter končno uničenje, kot tudi določanje zahtev za dostop do dotičnega tajnega podatka. Zaradi teh dejstev moramo biti previdni pri določanju previsoke ali prenizke stopnje tajnosti podatka, ki laho posledično vpliva na učinkovitost sistema varovanja.

To področje zahteva izdelavo ustreznega sistema preverjanja upravičenosti stopenj tajnosti podatkov, katere so določene na dokumentih s temi podatki. NATO predpisuje, da po petih letih v svojih dokumentih s področja informacijske varnosti pregleda, če je določena stopnja tajnosti podatkov v dokumentih še primerna, ali se lahko zniža ali odvzame. ZTP določa:

- da mora biti vsak dokument ob določitvi stopnje tajnosti vidno in v neskrajšani obliki označen s stopnjo tajnosti, z načinom prenehanja tajnosti, s podatki o pooblaščeni osebi, ki je določila stopnjo tajnosti, podatki o organu, če ta ni razviden iz glave dokumenta, in z datumom določitve tajnosti;

- dokumenti stopnje TAJNO in STROGO TAJNO morajo imeti poleg naštetih zahtev še podatke o zaporedni številki izvoda dokumenta, skupnem številu strani dokumenta, morebitnih prilogah ali spremljajoči dokumentaciji.

Poleg omenjenih določil ZTP točno določa oblikovne in ostale zahteve za unificirano izdelavo dokumentov z različnimi stopnjami tajnosti. Določa tudi postopke multipliciranja dokumentov s tajnimi podatki in ostale postopke obdelovanja, dostopanja, prenosa in uničenja dokumentov z tajnimi podatki (glej Čaleta, 2003, 105).

3.4 VARNOST INFORMACIJSKIH SISTEMOV

Določila varnosti informacijskih sistemov opredeljujejo minimalne standarde za varovanje tajnih podatkov, ki se pošiljajo, obdelujejo ali shranjujejo v komunikacijsko-informacijskih sistemih (KIS) ali omrežjih. Pri zagotavljanju varnosti informacijskih sistemov je zelo pomembna vzpostavitev ustrezne in učinkovite varnostne organizacije KIS, v kateri ima vsaka raven natančno določene pristojnosti in dolžnosti v smislu tajnosti, samostojnosti in uporabnosti tajnih podatkov, ki so shranjeni, procesirani ali obdelovani v KIS ali omrežjih. Noben KIS ali omrežje ne sme biti uporabljen za shranjevanje in procesiranje tajnih podatkov ali informacij, če za to ni ustreznega dovoljenja akreditacijskega organa v državi (Čaleta, 2003, 106).

V nacionalnem sistemu KIS ali omrežju, ki bo avtonomno in samostojno, bo akreditacijske dejavnosti izvajal nacionalni organ, čeprav bodo v teh sistemih ali omrežjih obdelovali tudi NATO tajne podatke. Če bosta KIS ali omrežje povezana v NATO sistem, bo akreditacijo poleg nacionalnega organa izvajal tudi ustrezen akreditacijski organ zveze NATO. Pomembno je, da so vse elektronske naprave, ki se uporabljajo za obdelavo in hranjenje tajnih podatkov ustrezno preverjene in certificirane. NATO in Evropska unija obravnavata to področje, kot zelo pomembno. To je razvidno tudi iz dejstva, da je večina podatkov o organizaciji teh sistemov nedostopnih državam, ki niso njune polnopravne članice (Čaleta, 2003, 107).

3.5 INDUSTRIJSKA VARNOST

Z ukrepi industrijske varnosti se zagotavlja ustrezne normative, ki v organih omogočajo izvajanje nekaterih storitev zunanjih izvajalcev, ki bodo za svoje delo potrebovali dostop do tajnih podatkov. Ti normativi in ukrepi so zelo pomembni v postopku pogajanja za sklenitev ustreznih pogodb, ki določajo tudi zahteve in dolžnosti izvajalcev posla pri ravnanju s tajnimi podatki ali dostopu do njih, kadar jih bodo potrebovali za izpolnitev pogodbe. Industrijska varnost zajema naslednja področja:

- usmeritve za pogajanja o sestavi pogodbe, ki vsebujejo podrobnosti, kadar bo za izvedbo storitve treba posredovati nekatere tajne podatke;
- varnostne zahteve za pogodbenike, ki bodo za svoje delo dobili dostop do nekaterih tajnih podatkov;
- dovoljenje za dostop do tajnih podatkov za pogodbenike, ki bodo za opravljanje storitev potrebovali tajne podatke;
- transport dokumentov z določeno stopnjo tajnosti, predvsem v partnersko državo;
- mednarodne obiske iz partnerskih držav;

- primer oseb, ki bodo poslane v partnersko državo za izvedbo projektov, ki vsebujejo tajne podatke in so v matični državi že pridobile ustrezna dovoljenja za dostop do teh podatkov.

Pomembno je dejstvo, da mora služba, ki bo v organu sestavljala pogodbe in pripravljala projekt, dobiti pisno soglasje originatorja tajnega podatka, da se ta lahko posreduje organizaciji ali podjetju za izvedbo storitve. Podjetje ali organizacija mora po sklenitvi pogodbe posredovati dokumentacijo za pridobitev ustreznih dovoljenj za dostop do tajnih podatkov. Osebe iz organizacije ali podjetja, ki sodelujejo v pogajanjih za sestavo pogodbe in projektne dokumentacije, ki vsebuje tajne podatke pa morajo imeti dovoljenje za dostop do tajnih podatkov že ob začetku pogajanj. Iz dokumentacije, ki jo posreduje organizacija, mora biti razvidno:

- identiteta in zahtevana stopnja dostopa do tajnih podatkov za vse izvajalce in podizvajalce, ki bodo sodelovali v projektu;
- za posameznike mora biti razvidno, do kakšne ravni in s kakšno količino tajnih podatkov se bodo seznanjali pri izpolnjevanju pogodbene storitve za organ.

Organ pred posredovanjem tajnih podatkov za izvedbo naročila pozove odgovorno osebo v organizaciji, naj predloži podatke, iz katerih bo mogoče ugotoviti uresničevanje ukrepov za varovanje tajnih podatkov, določenih v pogodbi med naročnikom in organizacijo, ki bo izvjala storitev. Organ lahko na podlagi pridobljenih podatkov pozove organizacijo, naj izpolni manjkajoče ukrepe za varovanje tajnih podatkov in za to določi ustrezen časovni rok. Organ mora organizaciji nuditi ustrezno strokovno pomoč. Šele ob ugotovitvi izpolnjevanja vseh zahtev, se organizaciji posreduje tajne podatke, nujne za izvedbo storitve. Organ lahko tudi med opravljanjem storitve preverja ukrepe in postopke za varovanje tajnih podatkov, vendar samo v delu, ki se nanaša na izvajanje konkretne storitve (Čaleta, 2003, 107).

3.6 NACIONALNI ORGANI POMEBNI ZA VARNOSTNO ZAGOTOVITEV CNKZP

Organi, enote ter izvajalci, ki so vključeni v izvajanje aktivnosti, postopkov, predpisov z namenom izpolnjevanja varnostnih zahtev pri delu CNKZP so:

- Urad za varovanje tajnih podatkov (v nadaljevanju UVTP),
- Obveščevalno varnostna služba Ministrstva za obrambo (OVS MO),
- 16.BNZP,
- CNKZP.

Vsaka od omenjenih ustanov ima v varnostnem sistemu svoje naloge in funkcije, katere so določene z predpisi in stalno nadzirane ter ustrezno verificirane s strani določenih organov. Ti organi preverjajo izvajanje vseh predpisanih aktivnosti, postopkov in predpisov za izpolnjevanje ter doseganje nivojev vseh varnostnih zahtev. Za doseganje standardov, predpisov in pravilno izvajanje vseh varnostnih postopkov so odgovorni znotraj 16. BNZP varnostni častnik in štabni odsek S-2.

4. VARNOSTNE ZAHTEVE IN STANDARDI NATO ZA CNKZP

Poleg vseh omenjenih dokumentov na nacionalni ravni mora CNKZP izvajati in upoštevati predpise, zahteve ter standarde zveze NATO. Ti dokumenti in izpolnjevanje njihovih zahtev so ključni za pridobitev akreditacije evalvacijske skupine pooblaščene s strani zveze NATO. Brez njihove akreditacije in pridobitve certifikata ustreznosti (Certificate of Compliance), CNKZP ne mora opravljati svojega dela v sklopu NATINADS. Vsi dokumenti morajo biti usklajeni na nacionalni ravni in NATO ravni. Zveza NATO ima rahlo drugačen sistem opredeljevanja varnostni zahtev od slovenskih nacionalnih predpisov. NATO predpisi posamezna področja bolj razdelijo in sicer na več segmentov, kot so kadrovska varnost, fizična varnost, varnost informacij, industrijska varnost in varnost informacijskih sistemov.

4.1 DIREKTIVA AD 70-1

Direktiva AD 70-1 (ACO (Allied Command Operations – Operativa Združenega Poveljstva) Security Directive (Varnostna Direktiva), number (št.) 70-1 izdan s strani Severnoatlantskega sveta (North Atlantic Council). Direktiva AD 70-1 je sestavljen iz šestih delov, ki vsak opredeljujejo določeno varnostno področje:

- PART 1: GENERAL (SPLOŠNO);
- PART 2: PHYSICAL SECURITY AND COUNTER TERRORISM/SABOTAGE (Fizična varnost in zaščita pred terorističnimi dejanji in sabotažami);
- PART 3: SECURITY OF INFORMATION (Varnost informacij);
- PART 4: PERSONNEL SECURITY (Kadrovska varnost);
- PART 5: INFOSEC (Varnost informacijskih sistemov);
- PART 6: SECURITY PROCEDURES (Varnostni postopki).

Direktiva je izdana s strani Supreme Headquarters Allied Powers Europe (Vrhovno poveljstvo Združenih Sil Evrope) v Belgiji (v nadaljevanju SHAPE). Dokument je klasificiran s stopnjo tajnosti NATO Unclassified, kar pomeni da nima stopnje tajnosti, vendar se mora nahajati znotraj NATO strukture. Dokument predstavlja krovni dokument glede varnostnih zahtev in standardov predpisanih za objekte stacionarnega tipa s strani zveze NATO, med katere spada tudi CNKZP. Dokument je razdeljen na šest delov. Vsako izmed šestih poglavij opredeljuje posamezno področje varnostne zagotovitve.

4.1.1 Prvi del: Splošno

Prvi del dokumenta je splošni del in je razdeljen na dve poglavji. Prvo poglavje predpisuje osnovne predpise in minimalne standarde varnostne zagotovitve, katera mora biti prenešena na vse nivoje ACO (Allied Command Operations-Operativa Združenega Poveljstva). Vse članice zagotavljajo, da bodo implementirale predpise in minimalne standarde, z ciljem doseganja skupnega standarda zaščite tajnih podatkov v vsaki članici, poveljstvu, agenciji in formaciji ACO. To pomeni zagotavljanje zanesljivega dostopa, obdelave, hranjenja, prenosa in uničenja tajnih podatkov.

Ukrepi in predpisi implementirani v vsaki ACO formaciji (poveljstva, centri, agencije in elementi podrejeni SACEUR-Supreme Allied Commander Europe-Vrhovni poveljnik NATO za Evropo) morajo odražati zagotovitev varnosti v kadrovski organizaciji, fizični varnosti, varnosti informacij, varnosti informacijskih sistemov (INFOSEC–Information Systems Security), komunikacijski varnosti (COMSEC–Communications Security) z namenom doseganja minimalnih predpisanih standardov. Ti morajo biti prilagojeni lokalnim okoliščinam in operativnim zahtevam.

Vsaka odgovorna oseba je odgovorna za varnost in dolžna pripraviti varnostni načrt območja in izdati navodila za implementacijo zahtev te Direktive. Vsaka oseba pooblaščena za dostop do tajnih podatkov je dolžna osvojiti ustrezno varnostno kulturo. Naloga varnostnega častnika je organiziranje izobraževanja s področja varnostne tematike in opozarjati na nepravilnosti pri izvajanju varnostnih postopkov. Vsaka velika odstopanja od predpisanih minimalnih standardov s to Direktivo, morajo biti ugotovljena in poročana s strani organov J2 (INTEL) SHAPE.

Drugo poglavje prvega dela določa in predpisuje postopke organiziranja varnostnega sistema, odgovornosti in načrtovanje varnostnega sistema. Opredeli vlogo NATO vojaškega komiteja (v nadaljevanju NAMILCOM–NATO Military Commitee) in sicer je ta odgovoren za izvrševanje vseh vojaških nalog ter je posledično odgovoren za vse varnostne zadeve znotraj NATO vojaške strukture. Odgovoren je za obdelavo vseh inšpekcijskih varnostnih poročil in je obveščen o vseh resnih varnostnih pomanjkljivostih. SACEUR je odgovoren NAMILCOM za vse varnostne zadeve znotraj ACO. To vključuje odgovornost za vzpostavitev varnostne organizacije, izvrševanje varnostnih programov v skladu z NATO varnostno politiko, ter zagotavljanje periodičnega nadzora izvajanja varnostnih predpisov na vseh nivojih poveljevanja. Zaradi zagotovitve delovanja SACEUR prenese svojo varnostno pooblastilo na ACOS J2 SHAPE.

4.1.2 Drugi del: Fizična varnost in protiteroristični ukrepi/sabotaže

4.1.2.1 Fizična varnost

Fizična varnost predstavlja le del varnostnega sistema, ki mora biti podprt z ustrezno kadrovsko varnostjo, varnostjo informacij in ukrepi zaščite informacijskih sistemov.
Glavni namen fizičnega varovanja je preprečiti nepooblaščen dostop do NATO tajnih podatkov. Drugi del te Direktive opredeljuje predvsem fizično varnost z namenom zaščite pred špijonažo, vrinjanjem, sabotažo in terorističnimi dejanji. Varnostni elementi, kot so ograje in ostale prepreke, služijo za zaščito pred različnimi grožnjami, zato jih je potrebno vključiti v organizacijo in načrtovanje varnostnega sistema. Prvo poglavje opredeljuje osnovne fizične varnostne ukrepe z namenom preprečevanja groženj špijonaže in vrinjanja. Drugo poglavje opredeljuje zaščito pred terorističnimi dejanji in sabotažami znotraj držav članic zveze NATO. Tretje poglavje se osredotoča na zaščito pred terorističnimi dejanji in sabotažami izven območja držav članic zveze NATO.

Varnostne zahteve so opredeljene različno in so odvisne od različnih faktorjev. Eden od teh je tudi velikost enote, saj varnostne zahteve za manjše premično, terensko poveljstvo niso enake kot tiste za veliko štabno poveljstvo nivoja korpusa (ali Združenega Poveljstva Sil). Upošteva

se še faktorje, kot so nivo klasifikacije in kategorije informacij, količina hranjenih informacij (tiskovina, informacije zapisane na različnih medijih), varnostni certifikati zaposlenih in izkazan upravičen interes zaposlenih, način shranjevanja tajnih podatkov ter ocena stopnje ogorženosti področja za možne teroristične napade in sabotaže.

4.1.2.1.1 Varnostna območja

Definiranje varnostnih območij predstavlja osnovni pogoj za določitev nadaljnih zahtev zaščite območja, kjer se hranijo, obdelujejo in prenašajo tajni podatki. Temeljno določilo pri uvajanju fizične varnosti in sistema varnostnih območij je predpis, ki določa da se morajo tajni podatki stopnje tajnosti NATO ZAUPNO ali višje obdelovati in hraniti v varnostnih območjih. Taka varnostna območja morajo biti organizirana in načrtovana, kot to določajo predpisi te Direktive. Namen koncepta varnostnih območij je ustvariti kontrolni sistem za preprečitev nepooblaščenega dostopa do NATO tajnih podatkov.

Varnostna območja I.stopnje so organizirana in načrtovana tako, da omejujejo, iz praktičnih razlogov, dostop do tajnih podatkov (operativni centri in registri dokumentov). Za vzpostavitev takih območij se zahteva:
- točno določena in zaščitena vhodno-izhodna točka, skozi katero so kontrolirani vsi vstopi in izstopi v območje,
- sistem kontrole vstopov, ki omogoča vstop samo tistim ustrezno preverjenim in posebno pooblaščenim,
- specifikacijo nivoja in kategorije tajnih podatkov, kateri se normalno hranijo in do katerih se dostopa na varnostnem območju.

Varnostna območja II.stopnje so območja, kjer se obdelujejo in hranijo tajni podatki stopnje tajnosti NATO ZAUPNO ali višje v taki obliki, da se jih lahko zaščiti z interno vzpostavljeno kontrolo, z namenom preprečitve dostopa nepooblaščenim osebam (objekti z pisarnami v katerih se redno obdelujejo in hranijo tajni podatki stopnje tajnosti NATO ZAUPNO ali višje). Za vzpostavitev takih območij se zahteva:
- točno določena in zaščitena vhodno-izhodna točka, skozi katero so kontrolirani vsi vstopi in izstopi v območje,
- sistem nadzora vstopov, ki omogoča vstop brez spremljave samo tistim, ki posedujejo ustrezno dovoljenje ali posebno odobritev. Za vse ostale osebe mora biti priskrbljeno spremstvo ali enakovreden nadzor, z namenom preprečitve nepooblaščenega dostopa do NATO tajnih podatkov in nekontroliranega vstopa na območje.

Administrativna območja so pridodana območja območjem I. ali II.stopnje, ki zahtevajo manj stroge varnostne ukrepe. Tam kjer so vzpostavljena je potrebno vzpostaviti vidni parameter znotraj katerega obstaja možnost nadzora osebja in vozil. Najvišji dovoljeni nivo tajnih podatkov, ki se obdelujejo in hranijo v administrativnem območju, je stopnje tajnosti NATO INTERNO. Taka območja niso obvezna, vendar lahko znatno pripomorejo k dvigu varnosti na območju.

4.1.2.1.2 Kontrola vstopov v varnostna območja

Glede na predpise Direktive mora biti vstop v varnostna območja I. in II. varnostne stopnje nadzorovan z sistemom elektronske ali osebne prepoznave. Sistem vstopov mora izpolnjevati in upoštevati sledeče pogoje:

- Vsi stalno zaposleni morajo biti ustrezno varnostno preverjeni. Po določilih Direktive AD 70-1 vsaj do stopnje NATO TAJNO.
- Obiskovalci z ustreznim varnostnim potrdilom imajo lahko odobren začasen dostop brez spremstva.
- Obiskovalci brez ustreznega varnostnega potrdila ne smejo imeti dostop v varnostno območje. Izjemoma je lahko odobren vstop takim osebam, kadar so izvedeni vsi poostreni ukrepi z namenom preprečitve nepooblaščenega dostopa do tajnih podatkov zveze NATO.
- Pogodbeni izvajalci (vključujoč vzdrževalce in čistilce) morajo ali pridobiti ustrezno varnostno potrdilo ali biti s spremstvom ves čas. Varnostno potrdilo mora biti izdano za stopnjo podatkov do katerih lahko nenamenoma dostopijo. Sistemski administratorji morajo biti preverjeni do najvišjega nivoja, katerega obdeluje sistem.
- Občasno je neizogiben obisk delegacij ali posameznikov ne-NATO organizacij, ki sodelujejo z zvezo NATO. Zato jim mora biti omogočen dostop v varnostna območja, razen varnostnega območja I.stopnje. V takem primeru morajo biti primeri odobritev dostopa obravnavani s strani NATO Office of Security (v nadaljevanju NOS) z SHAPE J2. V primerih, ko je dostop do varnostnega območja I.stopnje neizogiben, se omenjeno območje predela do obsega, ko se lahko klasificira, kot varnostno območje II.stopnje.

Sistemi avtomatske kontrole vstopov v varnostna območja so lahko vpeljani v varnostna območja I. ali II. stopnje. Podprti so lahko z avtomatizirano identifikacijo in so lahko obravnavani kot nadomestilo, vendar ne popolna zamenjava za varnostnike. Tak dostop je lahko daljinsko voden z določenega mesta in mora izpolnjevati določene pogoje, kot so:

- Avtomatska dostopna vrata morajo fizično onemogočati dostop, polzapore niso dovoljene.
- Nadzornik mora imeti vzpostavljen CCTV (Closed Circuit Television-Video prenos zaprtega tokokroga) in sistem daljinskega zvočnega komuniciranja.
- Nadzornik sistema mora imeti možnost kontroliranja avtomatskega dostopa z namenom preprečitve avtomatskega dostopa, kadar in če je to potrebno.
- Sistem prehoda je podprt z unikatnim PIN (Personal Identification Number-Osebna identifikacijska številka) sistemom dostopa.

Naključne fizične preiskave se lahko izvaja ob vsakem izstopu in vstopu iz varnostnega območja, z namenom preprečitve nepooblaščenega iznosa tajnih podatkov. Pred vsakim vstopom in izstopom je potrebno obiskovalcem to tudi naznaniti.

Uporaba varnostnih propustnic v varnostnih območjih je dodatno varnostno merilo. Vsaka varnostna priponka mora vsebovati serijsko številko in podrobnosti o imetniku (podpis ni zahtevan). Izpolnjevati mora še nekatere zahteve kot so: biti mora unikatna za organizacijo, vendar brez izdajanja identitete organizacije, v kodiranem načinu mora razkrivati varnostno območje in dostop do tajnih podatkov, katerega omogoča, ne sme biti na vpogled izven varnostnega območja, propustnice se ne smejo uporabljati v namen identifikacije posameznikov, propustnice osebja katero ne poseduje ustreznih NATO varnostnih pooblastil, se mora popolnoma razlikovati od tistih z varnostnimi pooblastili NATO.

Na varnostnem območju se lahko uvede varnostna služba z ustrezno izurjenimi varnostniki, ki lahko izven delavnega časa zaposlenih, izvajajo obhode na določen čas, oziroma periodo. Ustrezni sistemi detekcije vdorov (IDS–Intrusion Detection Systems) lahko nadomestijo varnostnike in varnostne obhode, ne morejo pa nadomestiti dežurne varnostne službe, ki se mora izvajati ves čas. Najmanj dva varnostnika morata biti vedno na razpolago za intervencijo na lokaciji, vendar mora biti intervencija izvedena brez vpliva njune odsotnosti na zmanjšanje varnosti na drugih lokacijah.

4.1.2.1.3 Shranjevanje NATO tajnih podatkov

Naslednji standardi so navedeni po Direktivi AD 70-1, kot minimalni za shranjevanje NATO tajnih podatkov:

- Dokumenti stopnje tajnosti COSMIC TOP SECRET in vsi stopnje ATOMAL (NATO STROGO TAJNO in vezani na atomsko orožje-ATOMAL) morajo biti hranjeni v ojačanem prostoru, v blagajni ali kontejnerju razreda A, z vgrajeno kombinacijsko ključavnico standarda razreda A.
- Dokumenti stopnje tajnosti NATO SECRET ali CONFIDENTAL (NATO TAJNO ali ZAUPNO) morajo biti hranjeni v ojačani sobi, v blagajni ali kontejnerju razreda A ali B z napravo za zaklepanje ekvivalentnega razreda.
- Dokumenti stopnje tajnosti NATO RESTRICTED (INTERNO) morajo biti hranjeni vsaj v pohištvu z sistemom zaklepanja razreda C, ki se nahajajo v zakljenjenih pisarnah ali stavbah. Posebno pozornost je potrebno nameniti ob iznosu in ravnanju s podatki stopnje tajnosti NATO INTERNO izven varnostnih območij z namenom preprečitve dostopa in vpogleda nepooblaščenih oseb.

Varnostne blagajne in kontejnerji predstavljajo zadnjo zaščito pred nepoooblaščenim dostopom do tajnih podatkov. Delimo jih na več razredov, ko so potrjeni in preverjeni s strani držav članic zveze NATO:

- Razred A je potrjen s strani nacionalnih organov za hranjenje dokumentov do stopnje tajnosti NATO COSMIC TOP SECRET, znotraj varnostnega območja I. in II. stopnje.
- Razred B je potrjen s strani nacionalnih organov za hranjenje dokumentov do stopnje tajnosti NATO SECRET in CONFIDENTAL, znotraj varnostnega območja I. in II. stopnje.
- Razred C je potrjen s strani nacionalnih organov za hranjenje dokumentov do stopnje tajnosti NATO RESTRICTED in sicer gre za pisarniško pohištvo z ustreznim sistemom zaklepanja.

4.1.2.2 Protiteroristični ukrepi/sabotaže

Ukrepi fizičnega varovanja se v glavnem nanašajo na splošne nevarnosti in ukrepe za zmanjšanje le teh. Ti ukrepi morajo biti vedno upoštevani. To poglavje obdeluje grožnje teroristične narave in sabotaže znotraj držav članic NATO, trejtje pa izven držav članic NATO. Možne teroristične grožnje in sabotaže NATO civilnim in vojaškim organom se opredeljujejo skozi šest tipov groženj:

- Splošna varnost osebja.
- Onemogočanje osnovnih zalog in služb, ki bodo preprečile ali zmanjšale učinkovitost misije.

- Fizične poškodbe.
- Onemogočanje izvajanja misije.
- Onemogočanje svobode gibanja.
- Onemogočanje spolšne varnosti in stabilnosti znotraj ozemlja članic NATO zveze.

Grožnje lahko izvirajo iz:
- Strani terorističnih organizacij (skupine ali posamezniki), ki si lahko izberejo NATO, kot tarčo napadov.
- Sabotaž z povzročitvijo škode lastnini, nezmožnosti delovanja posameznikov in/ali povzročitev izgube osnovnih zalog in služb.
- Organiziranega kriminala.
- Vnašanja civilnih nemirov.

Tipi groženj nasilja, ki lahko doletijo NATO objekte so različni in opredeljeni v tem poglavju. Gre za tipe groženj od bombnih napadov z avtomobili bombami, demonstracije, napadov z lahkim orožjem, ubojev, ugrabitve, operacije proti ključnim sistemom informacijske tehnologije do uporabe bioloških, kemičnih in radioloških naprav.

Odgovornosti za varnost objektov in osebja, ki deluje v zvezi NATO pripada državi gostiteljici, oziroma sodelujoči državi. Ta se zavezuje, da bo o vseh zaznanih morebitnih grožnjah obveščala poveljstvo združenih sil in storila vse potrebno, da zaščiti ogrožene objekte. Pri tem morajo biti upoštevani vsi zahtevani standardi in predpisi zveze NATO.

Varnostni ukrepi morajo biti izvajani tako, da zagotavljajo varovanje pred možnostmi fizičnih poškodb, onesposobitvijo ključnih zmožnosti in služb, ter pred poškodbami in smrtjo osebja. Večina varnostnih ukrepov sprejetih za varnost in zaščito NATO tajnih podatkov nudi zaščito tudi pred sabotažami in terorističnimi dejanji. Poveljnik združenih sil je odgovoren, da predpiše in uvede dodatne ukrepe, če je to potrebno. Kljub vsemu morajo biti načrtovani varnostni ukrepi, ki opravičujejo stopnjo zaščite glede na operativno vrednost objektov in sistemov.

Pri načrtovanju je potrebno upoštevati načrt NATO objektov in izdelati ustrezen Notranji načrt varovanja. Primeri vseh elementov, ki jih je potrebno upoštevati za implementacijo NV, so navedeni v aneksu A. Varnostni ukrepi, vključujoč fizično varnost, so navedeni v aneksu B. NV mora biti upoštevan in izvajan periodično, z namenom zagotavljanja njegove učinkovitosti. Poveljniki so odgovorni za izvajanje urjenja osebja, z namenom odzivanja na različne situacije z podano oceno ogroženosti. Vaje morajo vključevati tudi alarmiranje osebja izven običajnega delovnega časa. Ustreznost NV in zapisi o opravljenih vajah morajo biti pregledani med izvajanjem inšpekcijskega pregleda s strani ACO varnostne inšpekcije. Rezultati ugotovitev komisije morajo biti vključeni v inšpekcijskem poročilu.

Standardni NATO opozorilni sistem je uveden za vse organizacije znotraj združenega poveljstva. Ta opozorilni sistem ima štiri ločene stopnje nad normalno, ki so: alpha, bravo, charlie in delta. Vsaka od stopenj poudarja osnovne minimalne ukrepe, ki jih je potrebno izvajati ob razglasitvi ustrezne stopnje ogroženosti.

Stopnja ogroženosti Alpha se razglasi ob splošni ogroženosti možnega terorističnega napada na organizacijo NATO in njeno osebje.

Stopnja Bravo se uvede ob povečani grožnji in bolj predvidljivi teroristični aktivnosti. Zagotovljena mora biti zmožnost večtedenska vzdrževanje te stopnje varnostnih ukrepov, brez ogorožanja operativnosti in brez ogrožanja odnosov z lokalnimi oblastmi.

Stopnja Charlie se razglasi ob nastopu incidenta ali ob prejetju obveščevalnih podatkov, da je katera izmed terorističnih groženj proti NATO organizaciji ali osebju neizogibna verjetnost. Vzdrževanje te stopnje varnostnih ukrepov bo verjetno otežila delo in mirnodobne aktivnosti enot in osebja.

Stopnja Delta se razglasi na mestu nastopa terorističnega dejanja ali ob prejemu obveščevalnih podatkov, da je tak napad na lokacijo ali osebo verjeten. Ponavadi to stopnjo razglasijo, kot lokalno opozorilo in nakazuje zmožnost napada v 24-ih urah. Dodatek 1 k aneksu B opisuje vse ukrepe sprejete ob razglasitvi posamezne stopnje ogroženosti.

4.1.3 Tretji del: Varnost informacij

Ta del opredeljuje varnost informacij skozi štiri poglavja:
- sistem registrov,
- varnostne klasifikacije in označevanje dokumentov z tajnimi podatki,
- priprave, prenos in uničenje dokumentov z vsebino tajnih podatkov,
- postopki objave dokumentov.

4.1.3.1 Sistem registrov

Sistem registrov zagotavlja nadzor tajnih podatkov zveze NATO. Registri za hranjenje tajnih podatkov stopnje STROGO TAJNO in njihove kontrolne točke, so lahko locirani poleg registrov za hranjenje in obdelavo tajnih podatkov stopnje NATO TAJNO in nižje. Pogoj je, da so podatki stopnje tajnosti STROGO TAJNO, fizično in administrativno ločeni od tajnih podatkov stopnje TAJNO ali nižje. Glavni namen uvedbe ločenega sistema hranjenja, obdelave, prenosa in uničenja tajnih podatkov stopnje STROGO TAJNO, je zagotoviti ustrezen nivo varnosti podatkov omenjene stopnje. Sistem registrov je postavljen tako, da iz centralnega registra v SHAPE-u upravljajo in razpošiljajo ves material stopjne tajnosti NATO ATOMAL v podregistre mednarodnih organizacij. Vsak od teh podregistrov je zadolžen za vzpostavitev varnostnega sistema z kontrolnimi točkami prve in druge stopnje.

Kontrolne točke izvajajo sprejem, kontrolo in omejeno razpošiljanje za aktivnosti, kot je opredeljeno za:
- Kontrolne točke 1. kategorije so ustanovljene za delo v manjših mednarodnih zveznih štabih ali za aktivnosti locirane zunaj matične mednarodne organizacije.
- Kontrolne točke 2. kategorije so ustanovljene znotraj matične mednarodne organizacije ali njenih aktivnosti, ter služijo enemu ali večim štabnim elementom.

V vsakem takem registru delujeta tudi COSMIC Control Officer (v nadaljevanju CCO) in/ali COSMIC ATOMAL Control officer (v nadaljevanju CACOs), ki sta odgovorna za ažuriranje vseh prejetih, hranjenih in razposlanih zapisov stopnje tajnosti STROGO TAJNO in ATOMAL. Skrbita tudi za skladnost dokumentov z predpisi te Direktive in Direktive 35-4 in ustrezno razpošiljanje v skladu z seznamom pooblaščenih prejemnikov. Ažurirata tudi Listo

registra dostopov osebja pooblaščenega za dostopanje do tajnih dokumentov stopnje STROGO TAJNO in ATOMAL in sta obenem odgovorna za ustrezno fizično varovanje teh dokumentov.

4.1.3.2 Varnostne klasifikacije in označevanje dokumentov s tajnimi podatki

Pri klasifikaciji in označevanju dokumentov, kateri vsebujejo tajne podatke je naloga originatorja zapisa dokumenta, da določi njegovo stopnjo tajnosti v skladu z določili Direktive AD 70-1:

- STROGO TAJNO (COSMIC TOP SECRET-CTS). Podatki in gradivo, katerega nepooblaščeno razkritje bi pomenilo izredno veliko škodo za zvezo NATO.
- TAJNO (NATO SECRET-NS). Podatki in gradivo, katerega nepooblaščeno razkritje bi predstavljalo povzročitev velike škode zvezi NATO.
- ZAUPNO (NATO CONFIDENTAL-NC). Podatki in gradivo, katerega nepooblaščeno razkritje bi bilo škodljivo zvezi NATO.
- INTERNO (NATO RESTRICTED-NR). Podatki in gradivo, katerega nepooblaščeno razkritje bi bilo škodljivo interesom ali učinkovitosti zveze NATO.
- Podatki brez oznake tajnosti (UNCLASSIFIED) niso del varnostne obravnave, katera obdeluje področje varovanja tajnih podatkov stopnje INTERNO in višje. Potrebno je biti previden pri podajanju stopenj tajnosti, da ne pride do nezaželjenega razkritja tajnih podatkov.

Označevanje z oznako NATO mora biti na vseh izvodih tajnih dokumentov (razen stopnje STROGO TAJNO) pripravljenih v zvezi NATO. Mora biti vsebovan tudi na vseh dokumentih brez stopnje tajnosti, če ti izvirajo iz združenega poveljstva. Oznaki COSMIC in NATO označujeta, da dokument ne sme biti prenešen izven strukture NATO, razen s strani originatorja, oziroma z njegovo odobritvijo. Oznaka STROGO (COSMIC) mora biti na vseh dokumentih stopnje STROGO TAJNO namenjenim razpošiljanju znotraj zveze NATO. Edina izjema so primeri, ko morajo biti iz operativne nujnosti taki dokumenti razposlani enotam, ki nimajo registra ustrezne stopnje tajnosti. V tem slučaju se oznaka STROGO (COSMIC) izpusti, vendar se mora zagotoviti ravnanje z dokumenti stopnje tajnosti STROGO TAJNO. Oznaka ATOMAL mora biti na vseh dokumentih z tajnimi podatki o atomskem orožju, ki so jih posredovale ZDA ali Velika Britanija.

V primeru pod ali nadklasifikacije stopnje tajnosti dokumenta mora prejemnik dokumenta na to opozoriti originatorja. V primeru, da se originator odloči spremeniti stopnjo tajnosti mora o tem obvestiti vse prejemnike dokumenta. Pooblastila za označevanje stopnje tajnosti STROGO TAJNO mora imeti minimalno število oseb. Poveljnik združenih sil izda seznam teh oseb. Ponovna klasifikacija tajnih podatkov je lahko izvedena s strani pisarne originatorja, naslednika ali višje oblasti.

4.1.3.3 Priprave, prenos in uničenje dokumentov z vsebino tajnih podatkov

To poglavje je precej obširno in govori o ustrezni pripravi, oznakah in prenosu ter uničenju vseh vrst tajnih podatkov, kot so: pisni dokumenti, karte, mape, risbe, zapisi na trakih, komunikacijsko-informacijski izdelki za hranjenje, platnice dokumentov (STROGO TAJNO –rdeče, TAJNO–modro, ZAUPNO–zelen, INTERNO–rumeno), projekcije in ostalo. Poglavje obravnava tudi postopke za: označevanje strani in podrobnosti okoli štetja strani, zapisovanje

datumov in označevanje kopij, dodatne kopije in prevode, izvlečke, mikrofilme in postopke reprodukcije z mikrofilmov.

Poglavje obravnava tudi postopke prenosa tajnih podatkov. Točno določa kako se izvaja postopke in določa minimalne zahteve za izvajanje teh postopkov. Določeni so postopki za prenos tajnih podatkov na nacionalni ravni in mednarodni ravni. V nadaljevanju so predstavljeni standardi za prenos na nacionalni ravni, kjer so opredeljene zahteve za prenos tajnih podatkov glede na stopnjo tajnosti:

- Tajni podatki STROGO TAJNO ali ATOMAL se lahko prenašajo samo z uradno določenimi kurirji ali kurirsko službo. Osebno prenašanje tajnih podatkov te stopnje je prepovedano.
- Tajni podatki TAJNO ali ZAUPNO se lahko prenašajo samo z uradno določenimi kurirji ali kurirsko službo, ali izjemoma z drugim določenim osebjem. Dodatno lahko izvajajo take prenose nacionalno registrirane ali zavarovane poštne službe pod nacionalnimi določili.
- Tajni podatki stopnje INTERNO se lahko prenašajo znotraj katerekoli države članice zveze NATO z uradno kurirsko ali sporočilno službo. Tajni podatki stopnje ZAUPNO se lahko prenašajo z osebo, ki je ustrezno varnostno preverjena in seznanjena z varovanjem tajnih podatkov pred javnostjo in nepooblaščenimi osebami.

V Direktivi so opredeljeni tudi vsi postopki za posebne prenose, prenose na mednarodni ravni ter zahteve in minimalni standari za osebne prenose. Posebno poglavje obravnava postopke in zahteve za uničenje tajnih podatkov. Navaja uporabo rezalnikov, oziroma trgalnikov za pisne dokumente in obenem opozarja na problem ustreznega končnega odlaganja teh ostankov dokumentov. Uničenje z zažiganjem je temeljit način in le malo pepela ostaja, glede na količino zažganega materijala. Specificira točne zahteve za vse možne aparate za uničenje dokumentov in opredeljuje posebno direktivo z navodili za uničenje kripto materijala.

4.1.3.4 Postopki objave dokumentov s tajnimi podatki

Poglavje opredeljuje postopke izdajanja in prenosa NATO tajnih podatkov ne-NATO mednarodnim organizacijam. Velja za tajne podatke do stopnje STROGO TAJNO. NAC je najvišji organ za izdajanje tajnih podatkov ne-NATO prejemnikom teh podatkov. Ta prenos podatkov poteka po principu originatorja in poteka, kot sledi:

- Do navezujočega komiteja za tajne podatke do stopnje in vključujoč NATO ZAUPNO.
- Do NAMILCOM za tajne podatke do stopnje in vključujoč NATO TAJNO, za tajne podatke originatorja NAMILCOM, komiteje pod njem in za vse agencije in poveljstva v NATO vojaški strukturi.
- Podatki ATOMAL, katerekoli stopnje tajnosti ne smejo biti izdani katerikoli državi/organizaciji, ki ni vključena v trenutni verziji dokumenta C-M(64)39 in C-M(68)41.

4.1.4 Četrti del: Kadrovska varnost

Del Direktive AD 70-1, ki opredeljuje področje kadrovske varnosti je razdeljen na poglavji o dostopu do tajnih podatkov NATO in o poglavju o varnostnem izobraževanju.

4.1.4.1 Dostopanje do tajnih podatkov NATO

Dostop do tajnih podatkov NATO je omogočen samo zaposlenim, kateri za opravljanje svojega dela potrebujejo dostop do tajnih podatkov. Pri tem dostopajo samo do tajnih podatkov, za katere izkažejo upravičenost interesa. Pred odobritvijo do dostopa tajnih podatkov stopnje ZAUPNO in višje mora biti osebje ustrezno varnostno preverjeno in dobiti ustrezen certifikat. Pogoj za izdajo NATO varnostnega certifikata je pridobitev nacionalnega in upoštevanje sledečih zahtev za izpeljavo varnostnih poizvedovanj:

- Ne sme preteči pet let od datuma zahtevka za varnostno preverjanje za pripadnike vojske in civilnih služb.
- Ne sme preteči več kot devet mesecev od zahtevka za preverjanje za vse ostalo osebje.

Kjer je potrebno dostopanje do stopnje tajnosti ATOMAL, morajo države članice tak dostop zavesti na NATO varnostnem certifikatu.

Dostopanje do tajnih podatkov stopnje STROGO TAJNO mora biti posebno kontrolirano. Osebe z odobrenim dostopom do te stopnje tajnih podatkov so zavedene in vodene v ustreznem registru ali kontrolni točki. Vse osebe, ki jim preneha veljati tak dostop morajo biti nemudoma umaknjene s takega seznama. Seznam mora vsebovati datum in biti podpisan s strani pooblaščene osebe. Vsebovati mora čin, ime, stopnjo dovoljenja za dostop do tajnih podatkov in datum prenehanja veljavnosti dovoljenja za dostopanje.

Dostopanje do kripto materijala je omogočeno le posebno pooblaščenim in ustrezno izobraženim osebam. V izrednih razmerah konflikta lahko pooblaščeni poveljnik izda pisno dovoljenje za dostopanje do podatkov stopnje STROGO TAJNO, čeprav oseba ne poseduje ustreznega dovoljenja. Zaželjeno je, da taka oseba že poseduje dovoljenje nižje stopnje tajnosti.

Vsaka oseba za katero se smatra, da lahko predstavlja nevarnost zvezi NATO je lahko odstranjena z mesta, če lahko ogroža varnost. V primeru prekinitve veljavnosti dovoljenja za dostopanje podatkov mora nacionalna oblast narediti vse za obvestitev osebe in izvedbo vseh ustreznih postopkov za onemogočanje nadaljnega dostopa do tajnih podatkov.

4.1.4.2 Varnostno izobraževanje

Glavno ogrožanje varnosti izhaja iz pomankanja zavedanja, da vsaka varnostna grožnja izhaja iz posledičnega zmanjšanja varnostnih standardov in varnostnega zavedanja. Naloga varnostnega izobraževanja je usmerjati in opozarjati osebje na trenutne grožnje, z namenom zagotavljanja praktičnih nasvetov za ohranitev varnostnih standardev in nivojev zagotovitve le teh. NAC izdaja letno poročilo, ki vsebuje vse možne varnostne grožnje zvezi NATO, ki skozi J2 SHAPE in varnostno strukturo predstavlja osnovo za izvajanje nadaljnega varnostnega izobraževanja. SHAPE J2 je odgovoren tudi za dobavo potrebnega varnostnega izobraževalnega materijala.

4.1.5 Peti del: Varnost informacijskih sistemov (INFOSEC)

Ta del Direktive AD 70-1 predstavlja nekakšen smerokaz za večino NATO in ACO direktiv in regulativ, ki opredeljujejo področje CIS (Communications&Information Systems–

Komunikacijskih in Informacijskih sistemov) in INFOSEC (Information Systems Security–Varnost informacijskih sistemov). Pomembno je, da vse osebje vključeno v varnost tega področja poseduje ustrezna dovoljenja za dostopanje do teh varnostnih dokumentov.

Varnost informacijskih sistemov in peto poglavje, ki ga obravnava je varnostno občutljive narave, saj ima ta del Direktive AD 70-1 oznako tajnosti INTERNO (NATO RESTRICTED), v večini delov pa tudi TAJNO (NATO SECRET), zato ni predstavljeno v zaključni nalogi. To poglavje obravnava osnovne principe in minimalne standarde za vključitev INFOSEC (Information Technologies Security–Varnost Informacijske Tehnologije) varnostne politike v ACO. Ti standardi izvirajo iz NATO varnostne politike in podpirajočih Direktiv, NATO C3 Board Technical Implementation Directives (NATO Svet za tehnično vključitev Direktiv), ter AMSG (Allied Military Security Guideline–Združene Vojaške Varnostne Usmeritve) dokumentov.

Za izvajanje varnostne zagotovitve INFOSEC je odgovoren varnostni častnik za področje varnosti informacijske tehnologije. Ta mora biti iz stroke in mora izpolnjevati vse strokovne standarde, da lahko ustrezno izvaja nadzore nad delom sistemskih administratorjev in ostalih odgovornih za izvajanje varnostnih postopkov na področju informacijske tehnologije. To področje v CNKZP še ni ustrezno pokrito.

4.1.6 Šesti del: Varnostni postopki

Ta del Direktive je zadnji del in opredeljuje področja:
- kršenja, neizpolnjevanje varnostnih standardov in predpisov,
- izvajanja inšpekcijskih nadzorov,
- in tehničnega varovanja.

Kršenje varnostnih predpisov je nezmožnost izpolnjevanja osnovnih zahtev Direktive AD 70-1. Posledice kršenja ali neizpolnjevanja varnostnih standardov je lahko proceduralne narave, z majhnim vplivom na splošen nivo varnosti ali incident, ki lahko resno ogrozi splošno varnost. Zadnje se mora obravnavati, kot kršenje varnostnih predpisov, ter mora biti zavedeno, poročano in obravnavano. Ob obstoju dvoma bi moral biti incident v začetku obravnavan, kot kršitev varnostnih predpisov.

NATO tajni podatki so ogroženi, ko se delno ali v celoti razkrijejo nepooblaščenim osebam brez ustrezenega varnostnega dovoljenja za dostopanje do tajnih podatkov ali ko je bil predmet možne varnostne grožnje razkritja nepooblaščenega dostopanja do tajnih podatkov. NATO tajni dokumenti, ki so izgubljeni, četudi začasno, izven varnostnega območja se smatrajo za razkrite. Podobno, se tajni podatki, ki so izgubljeni, četudi začasno, znotraj varnostnega območja in ne morejo biti v določenem obdobju locirani, morajo smatrati za razkrite, dokler ni z preiskavo dokazano drugače. Ob taki ugotovitvi se izvede postopek, ki je sestavljen iz prijave varnostne kršitve, začetnega poročila in končnega poročila, katero mora vključevati tudi oceno povzročene škode ter poročilo poveljnika.

Šesti del Direktive AD 70-1 točno opredeljuje postopke izvajanja inšpekcijskih nadzorov. Namen opravljanja inšpekcijskih nadzorov je zagotovitev in pomoč vsem NATO poveljnikom pri zagotovitvi ustreznega varnostnega nivoja, z namenom doseganja varnostnih predpisov in

določil te direktive. Odgovoren za opravljanje nadzorov je sektor J2 SHAPE, oziroma organi v njegovi sestavi. Opredeljeni so časovni inšpekcijski pregledi, ki potekajo, odvisno od kategorije varnostnega območja, dvakrat letno do enkrat na tri leta. Izvaja se tudi preglede z namenom varnostnega svetovanja za novo ustanovljene enote, razpuščene enote ali enote, katere so dobile drugačno vlogo v zvezi NATO. Na podlagi opravljenih varnostnih, inšpekcijskih pregledov se izda ustrezna končna poročila z namenom izboljšanja stanja, kjer je to potrebno.

Za tehnično varnost in varnost komunikacijskih sredstev veljajo podobna določila in predpisi, kot za varnost informacijskih sistemov (INFOSEC). Enako velja tudi za stopnje tajnosti podatkov in iz istega razloga področje ni podrobneje predstavljeno v sklopu zaključne naloge (po AD 70-1).

4.2 DOKUMENT AC/35-D/2000 DIRECTIVE ON PERSONNEL SECURITY

Je dokument izdan s strani NAC in sicer ga je izdal NATO Varnostni komite (Security CommitteeAC/35–Allied Committe/35), kot dopolnilo k Direktivi C-M(2002)49: Security within NATO–Varnost znotraj zveze NATO. Izdan je bil junija 2002. Direktiva je narejena na podlagi usmeritev Direktive AD 70-1 in podrobneje opredeljuje področje kadrovske varnosti. V grobem lahko dokument razdelimo na tri področja in sicer področje osebnih varnostnih potrdil, postopkov varnostnega preverjanja in področja predpisov za dostopanje do tajnih podatkov.

4.2.1 Osebna varnostna potrdila

Področje izdajanja osebnih dovoljenj za dostopanje do tajnih podatkov (PSC–Personal Security Clearances) določa, da mora vsaka oseba, ki dostopa do tajnih podatkov stopnje NATO ZAUPNO in višje, posedovati ustrezna varnostna osebna potrdila. To pomeni, da so vsi ustrezno varnostno preverjeni. Obseg preverjanja je odvisen od stopnje tajnosti podatkov do katerih bo oseba dostopala. Nacionalna varnostna agencija je odgovorna za izvrševanje varnostnih preverjanj, na podlagi katerih se potrdi zanesljivost, zvestoba in zaupljivost v bodoče pooblaščene osebe za dostopanje do nacionalnih tajnih podatkov. Pridobitev nacionalnega osebnega varnostnega potrdila je pogoj za vložitev vloge za pridobitev NATO osebnega varnostnega potrdila.

Pri določanju potrebnih stopenj tajnosti podatkov, ki so pri delu na posameznih delovnih mestih zahtevana, sodeluje vodilni kader. Ta kader mora biti podrobno strokovno seznanjen z načinom dela v organih in varnostno kredibilen in ustrezno izobražen. Odgovoren je tudi za podaljšanje časovno opredeljenih potrdil, spremembo stopnje dostopanja do tajnih podatkov, če sprememba delovnih nalog to narekuje. Kjer je potrebno se lahko zahteva tudi varnostno preverjanje partnerjev in ožjih družinskih članov.

4.2.2 Varnostno preverjanje

Za izvedbo varnostnega preverjanja je zadolžena Nacionalna varnostna agencija. V primeru oseb zaposlenih v CNKZP mora biti vse osebje varnostno preverjeno do stopnje tajnosti

najmanj NATO TAJNO. To pomeni izvedbo razširjenega varnostnega preverjanja. V sklopu MO izvaja varnostno preverjanje OVS, ki je v sklopu Urada za varovanje tajnih podatkov. Na nivoju 16.BNZP je odgovorna oseba za varnostna preverjanja poveljnik bataljona, oziroma po njegovem pooblastilu sektor bataljonske kadrovske službe S-1. Ta tudi poda predlog za postopek varnostnega preverjanja, ki ga odobri in podpiše načelnik J-1 (kadrovski sektor na nivoju GŠ).

Pri varnostnem preverjanju se preverja in upošteva več kritrijev. Preverja se ali je oseba kadarkoli izvedla, oziroma poskušala izvesti dejanja sabotaže, terorističnega dejanja, če se druži ali se je družila s pripadniki raznih terorističnih, kriminalnih ali obveščevalnih skupin, ki so delovali v poskusih politične destabilizacije doma ali v tujini. Preverja se ali je oseba kdaj ponarejala uradne dokumente, posebno varnostne in vezane na varnostno preverjanje, ki je v teku. Preverja se ali je oseba imela ali ima finančne težave ali težave z uporabo drog, alkohola ter preteklimi kriminalnimi dejanji in seksualnimi prekrški, ki bi bili lahko razlog za izsiljevanja. Preverja se ali je oseba bila udeležena raznih demonstracij, kjer je izkazovala uradno nezaupanje, nezanesljivost, nezvestobo skozi govor ali dejanja. Preverja se, da ni oseba sodelovala v vdiranju v informacijske in komunikacijske sisteme. Preverja se tudi mentalno zdravje in zdravje ožjih sorodnikov, če obstaja možnost izseljevanje s strani raznih terorističnih, obveščevalnih ali drugih organizacij, z namenom dostopanja in razkritja NATO tajnih podatkov.

Zahteve za varnostno preverjanje, za pridobitev potrdila za dostopanje do tajnih podatkov stopenj NATO ZAUPNO in NATO TAJNO, morajo vsebovati podatke za obdobje zadnjih petih let ali obdobje od osemnajstega leta starosti, če je to krajše. Ostale zahteve so sledeče:
- izpolnitev vprašalnika osebnega varnostnega preverjanja,
- preverjanje identitete/državljanstva/nacionalnega statusa,
- preverjanje lokalnih in nacionalnih varnostnih arhivov.

Zahteve za varnostno preverjanje, za pridobitev potrdila za dostopanje do tajnih podatkov stopenj NATO STROGO TAJNO, morajo vsebovati podatke za obdobje zadnjih desetih let, ali obdobje od osemnajstega leta starosti, če je to krajše. Ostale zahteve so sledeče:
- izpolnitev vprašalnika osebnega varnostnega preverjanja,
- podrobno preverjane preteklosti osebe s poudarkom na finančnem stanju, zaposlitvah, izobrazbi, vojaški službi in izvedbi intervjujev, kjer nacionalna zakonodaja to dopušča.

Po izvedenem varnostnem preverjanju je Nacionalna varnostna agencija zadolžena za zavrnitev ali odobritev izdaje osebnega varnostnega potrdila za dostopanje do tajnih podatkov.

UVTP je zadolžen tudi za podaljšanje in ponovno izdajo osebnih varnostnih potrdil. Za stopnjo tajnosti NATO STROGO TAJNO in NATO TAJNO je potrebno zagotoviti podaljšanje v najkasneje petih letih od datuma prve izdaje, za stopnjo tajnosti NATO ZAUPNO pa najkasneje v desetih letih od prve izdaje. Po Direktivi AD 70-1 je minimalni pogoj za podaljšanje dovoljenja za dostopanje do stopnje NATO TAJNO najkasneje v desetih letih, kar pomeni, da je slovenska nacionalna zahteva strožja, saj zahteva podaljšanje najkasneje v petih letih.

Vse osebje, katero dostopa obdeluje in prenaša ter uničuje tajne podatke se mora zavedati svojih odgovornosti in pomembnosti izvajanja ustreznih varnostnih postopkov, za kar mora poskrbeti varnostni častnik v organu, skozi ustrezna predpisana varnostna izobraževanja.

4.2.3 Dostopanje do tajnih podatkov

Po pridobitvi osebnega varnostnega potrdila, izkazanem upravičenem interesu in seznanitvi skozi vsa potrebna varnostna izobraževanja, se lahko dostopa do tajnih podatkov v namene opravljanja dela, kadar je to potrebno. Tudi ti postopki so standardizirani in predpisani ter skrbi za njihovo izvajanje ustrezen organ in varnostno osebje. V CNKZP skrbi za pravilno izvajanje teh postopkov varnostni častnik in zaposleni v CNKZP. Med izjeme pri dostopanju do tajnih podatkov štejemo enkratno dostopanje, predčasno dostopanje do stopnje višje od tiste pridobljene z predhodnim varnostnim preverjanjem in nujen dostop (predvsem v vojnem času). Izjema pri nujnem dostopanju je dostopanje do tajnih podatkov stopnje NATO STROGO TAJNO, kjer lahko izjemoma dostopa do tajnih podatkov samo pooblaščena oseba, ki poseduje osebno varnostno potrdilo za dostopanje do stopnje tajnosti NATO TAJNO.

Direktiva opredeljuje tudi postopke za dostopanje do tajnih podatkov v namene organiziranja in izvedbe raznih konferenc in seminarjev, dostopanje do tajnih podatkov s strani ne-NATO organizacij ali držav, ki niso članice zavezništva ter za dostopanje kurirjev, osebnih varnostnikov in spremljevalcev (po AC/35-D/2000).

4.3 DOKUMENT AC/35-D/2001 DIRECTIVE ON PHYSICAL SECURITY

Je dokument izdan s strani NAC in sicer ga je izdal NATO Varnostni komite (Security Committee AC/35–Allied Committe/35), kot dopolnilo k Direktivi C-M(2002)49: Security within NATO–Varnost znotraj zveze NATO. Izdan je bil junija 2002. Dokument obdeluje več različnih področij in sicer:

- varnostne zahteve,
- fizične varnostne ukrepe,
- minimalne standarde za hranjenje tajnih podatkov NATO,
- zaščita pred tehničnim napadi ter
- fizična varnost komunikacijskih in informacijskih sistemov.

4.3.1 Varnostne zahteve

Po določilih varnostne politike zveze NATO je potrebno vse prostore, objekte, pisarne in ostala varnostna območja, kjer se hranijo, dostopajo, obdelujejo in uničujejo tajni podatki ustrezno fizično zaščititi. Stopnjo zaščite določa več faktorjev in sicer:

- nivo klasifikacije in kategorije tajnih podatkov,
- količina in oblika zapisa tajnih podatkov,
- varnostna potrdila in upravičenost interesa,
- ocena lokalne ogroženosti NATO enot za grožnje sabotaž, terorističnih napadov,...,
- način hranjenja NATO tajnih podatkov.

Fizično varovanje mora biti načrtovano z namenom preprečitve nasilnega vdora nepooblaščenih oseb, preprečitve in detekcije vohunjenja vrinjenih nezvestih in nezanesljivih oseb, omogočanja delitve dostopanja oseb po principu upravičenosti interesa za dostop do tajnih podatkov in omogočanje nemudnega odzivanja na vse potencialne in odkrite kršitve

varnostnih predpisov ter postopkov z namenom nepoooblaščenega dostopanja do tajnih podatkov.

4.3.2 Fizični varnostni ukrepi

Fizični varnostni ukrepi morajo biti del celotnega varnostnega sistema, kateri mora biti podprt z ustrezno kadrovsko varnostjo, varnostjo informacij, varnostjo informacijskih in komunikacijskih sistemov. Vse skupaj mora biti v skladu z NATO varnostno politiko in upoštevano že ob načrtovanju takih objektov, saj se tako močno zmanjšajo stroški predelave varnostnih območij, z namenom doseganja predpisanih standardov. Zunanji fizični ukrepi, predvsem gradbeni, v kombinaciji z ustreznim varovanjem z varnostno intervencijsko skupino omogočajo takoimenovano globinsko varovanje. Pomembno je tudi periodično testiranje opreme in izvajanje treningov ukrepanja ob izrednih razmerah v takih objektih. Posebno je to pomembno ob menjavi varnostne opreme in spremembi namembnosti varnostnega območja ali objekta.

4.3.2.1 Varnostna območja

Območja, kjer se hranijo tajni podatki NATO ZAUPNO in višje stopnje, morajo izpolnjevati neslednje zahteve:

- NATO varnostno območje I. stopnje za hranjenje tajnih podatkov stopnje NATO ZAUPNO in višje. Ta izpolnjuje zahteve, kot so: omogočanje vstopanja in izstopanja na kontrolirani točki. Kontrola vstopa omogoča vstop samo pooblaščenim osebam in ima jasno označeno klasifikacijo in stopnjo tajnosti podatkov, ki se hranijo na varnostnem območju.
- NATO varnostno območje II. stopnje za hranjenje tajnih podatkov stopnje NATO ZAUPNO in višje, z varnostnimi sredstvi in postopki, kateri so izvedeni interno. Ta izpolnjuje zahteve: omogoča vstopanje in izstopanje na kontrolirani točki. Kontrola vstopa, ki omogoča vstop brez spremljave samo osebam, ki so ustrezno pooblaščene za vstop na območje ter varnostno preverjene. Za vse ostale osebe se mora zagotoviti spremljava ali podobni ukrepi, z namenom onemogočanja dostopa nepooblaščenih oseb do tajnih podatkov.
- Administrativna območja so varnostna območja, katera so postavljena pred varnostnimi območji I. in II. stopnje, z namenom postavitve vidnega parametra, znotraj katerega je možno locirati vse osebe in vozila na varnostnem območju. Na administrativnem območju se lahko hrani tajne podatke do stopnje NATO ZAUPNO.

Vsa področja, ki niso operativna 24 ur na dan, morajo biti varnostno pregledana s strani pooblaščene osebe, z namenom zagotovitve ustreznega hranjenja tajnih podatkov in preprečevanja nepooblaščenega dostopanja.

4.3.2.2 Specifični fizični varnostni ukrepi

To poglavje opredeljuje vse dodatne fizične varnostne ukrepe, njihov opis in opis njihovega vpliva na višjo splošno varnost območja. Opisuje vpliv graditve območja z ograjami, znotraj katerih se vključi sisteme za detektiranje vdorov, sistem televizijskega nadzora zaprtega tokokroga, ustrezen sistem osvetlitve. Poudarjeno je, da mora biti sistem vhodov istega varnostnega nivoja, kot ograja in podprt z ustreznim sistemom dostopov. Ustrezen sistem

identifikacije je obvezen za varnostna območja I. in II. stopnje. Upoštevati je potrebno določila za spremstvo obiskovalcev, ki so določena na podlagi nacionalnosti osebe, osebnega dovoljenja za dostopanje do tajnih podatkov, izkazanega upravičenega interesa za dostopanje do tajnih podatkov in ostalih varnostnih zahtev. Za obiskovalce brez predvidenega spremstva je obvezno nošenje ustrezne identifikacijske kartice, iz katere je razvidno da gre za obiskovalca. Vpeljan je lahko tudi sistem osebnih pregledov, z namenom preprečitve odtekanja tajnih podatkov, vendar mora biti pred vstopom razvidno obvestilo o pooblaščenem izvajanju takih pregledov. Vse to mora biti doseženo in izvedeno z ustrezno tehnično opremo, ki mora biti potrjena s strani Nacionalne varnostne agencije. Predvsem velja to za blagajne in trezorje, ključavnice in detektorje v varnostnih območjih I. in II. stopnje.

4.3.3 Minimalni standardi za hranjenje tajnih podatkov NATO

NATO varnostna politika točno predvideva minimalne varnostne standarde za hranjenje NATO tajnih podatkov različnih stopenj. Glavne usmeritve, predpisi, ukrepi in postopki so zavedeni v Direktivi AD 70-1 in AC/35-D/2001.

Za tajne podatke NATO STROGO TAJNO je predvidena vrsta ukrepov, ki med seboj zagotavljajo višji nivo varovanja in sicer morajo biti znotraj varnostnega območja I. ali II. stopnje v ustreznem nacionalno odobrenem varnostnem kontejnerju ali blagajni. Izvajati se mora dodatno kontrolo s stalnim varovanjem ali intervalnimi pregledi območja ustrezno preverjenega in usposobljenega varnostnega osebja, z največ dvournimi presledki, ali z namestitvijo ustreznega sistema detekcije vdorov in intervencijsko varnostno ekipo, ki mora biti usposobljena za reagiranje v časovno določenem varnostnem načrtu.

Za tajne podatke NATO TAJNO je predvidena vrsta ukrepov, ki med seboj zagotavljajo ustrezen nivo varovanja in sicer morajo biti znotraj varnostnega območja I. ali II. stopnje pod enakimi varnostnimi pogoji, kot za NATO STROGO TAJNO, vendar z nekaterimi dopustnimi odstopanji. Nahajati se morajo v ustreznem nacionalno odobrenem varnostnem kontejnerju ali blagajni, vendar brez dodatnih kontrol. Če se nahaja na varnostnem območju odprtega tipa mora zagotavljati izvajanje naslednjih predpisov. Izvajati se mora dodatno kontrolo s stalnim varovanjem ali intervalnimi pregledi območja ustrezno preverjenega in usposobljenega varnostnega osebja, z največ štiriurnimi presledki, ali z namestitvijo ustreznega sistema detekcije vdorov in intervencijsko varnostno ekipo, ki mora biti usposobljena za reagiranje v časovno določene varnostnem načrtu.

Za tajne podatke NATO ZAUPNO je predvidena vrsta ukrepov, ki med seboj zagotavljajo ustrezen nivo varovanja in sicer morajo biti znotraj varnostnega območja I. ali II. stopnje pod enakimi varnostnimi pogoji, kot za NATO STROGO TAJNO in NATO TAJNO, vendar brez dodatnih varnostnih zahtev. Za tajne podatke NATO INTERNO je zahtevano shranjevanje v zaklenjenih ustreznih varnostnih kontejnerjih ali blagajnah. Pomembna je uvedba predpisanega sistema hranjenja in dostopanja sistema številčnih kombinacij in ključev za dostopanje do tajnih podatkov in ustrezen sistem evidentiranja teh dostopov. Prav tako je potrebno poskrbeti za uvedbo sistema uporabe telefaksov in kopirnih strojev, ki se uporabljajo za pošiljanje in razmnoževanje tajnih podatkov.

4.3.4 Zaščita pred tehničnimi napadi

Namen varnostnih ukrepov pred tehničnimi napadi je vzpostavitev ustreznega sistema varovanja, ki vključuje vse ukrepe za preprečevanje napadov in vrinjanje v tehnične sisteme in objekte, kjer se hranijo tajni podatki. Ukrepi se izvajajo z namenom preprečevanja aktivnega in pasivnega prisluškovanja, ustreznega varovanja in preprečevanja napadov na električne in elektronske sisteme, vse skupaj z namenom vzpostavitve tehnično varnih območij z ustreznim sistemom varnostnih pregledov.

Varnostni ukrepi za zaščito pred prisluškovanjem morajo biti redno izvajani v vseh objektih, kjer se obdelujejo tajni podatki stopnje NATO TAJNO in višje. Izvajajo se ukrepi, kot so omejitev dostopa, varnostni pregledi osebja, uporaba objektov z ustreznimi zvočno izoliranimi gradbenimi elementi (stene, tla, vrata, okna, ...) za zaščito pred pasivnim prisluškovanjem, izogibanje pred posredovanjem tajnih podatkov preko nezaščitenih in varnostno nepregledanih komunikacij. Ožičenje, tehnična oprema, električne in elektronske naprave, pisarniška oprema na varnostnih območjih mora biti pregledana s strani ustrezno tehnično izurjenega osebja po pooblastilu in odredbi ustreznega nacionalnega varnostnega organa.

V tehnično varnih območjih je potrebno redno izvajati varnostne preglede vse tehnične opreme, prepovedana je uporaba in vnos katerekoli elektronske opreme (mobilnih telefonov in ostalih elektronskih naprav z vgrajenimi elektro-akustičnimi komponentami), prepovedan je vstop nepooblaščenim osebam, noben kos pisarniške opreme in tehnične opreme ne sme biti vnešen pred izvedenim protiprisluškovalnim in tehničnim pregledom (vsak kos opreme mora imeti svojo inventarno šifro) in noben telefon ne sme biti v takem območju, če je to le možno. Kadar to ni možno mora biti fizično odstranjen ali odklopljen, ko se v prostoru govori o tajnih podatkih stopnje NATO TAJNO ali višje.

4.3.5 Fizična varnost komunikacijskih in informacijski sistemov

Posebna pozornost je namenjena varnosti komunikacijskih in informacijskih sistemov, katera je zagotovljena skozi izvajanje predpisov in ukrepov predpisanih v varnostnih direktivah. Točno so določene zahteve za gradbene konstrukcije, stavbno pohištvo, ventilacijske sisteme in ostale sisteme, kateri so del varnostnih območij, kjer se nahajajo informacijski in komunikacijski sistemi za hranjenje, obdelavo, pošiljanje in uničenje tajnih podatkov (po AC/35-D/2001).

4.4 DOKUMENT AC/35-D/2002 DIRECTIVE ON SECURITY OF INFORMATION

Je dokument izdan s strani NAC in sicer ga je izdal NATO Varnostni komite (Security Committee AC/35–Allied Committe/35), kot dopolnilo k Direktivi C-M(2002)49: Security within NATO–Varnost znotraj zveze NATO. Dokument je bil revidiran in izdan marca 2004. Direktiva je narejena na podlagi usmeritev Direktive AD 70-1 in podrobneje opredeljuje področje varnosti informacij. Področje je nazorno predstavljeno že v poglavju, ki opredeljuje Direktivo AD 70-1, zato to poglavje v nadaljevanju ni podrobneje razdelano.

5. POMEMBNI DOKUMENTI ZA VARNOSTNO ZAGOTOVITEV CNKZP

Nacionalne varnostne zahteve morajo biti v skladu z NATO predpisi, uredbami in določili. Po določilih varnostne zagotovitve mora imeti vsak NATO integriran CNKZP - Control and Reporting Center (v nadaljevanju CRC), ustrezno NATO in nacionalno akreditacijo preden je lahko vključen in operativen v NATINADS. Dokumenti, katere mora imeti vsak tak CRC, so hranjeni v ustreznih varnostnih mapah, ki se nahajajo v ustreznih, predpisanih prostorih, blagajnah ali trezorjih.

5.1 SSRS (SYSTEM SPECIFIC SECURITY REQUIREMENTS STATEMENT)

Izjava o sistemskih specifičnih varnostnih zahtevah, kjer je opredeljeno vse o varnostnih zahtevah za varnostno zagotovitev in delovanje CRC-jev integriranih v NATINADS mrežo. Je dokument stopnje tajnosti NATO INTERNO. Dokument na katerega se navezuje je AC/35-D/1015. SSRS je v skladu z dokumentom EN CSRS (Enlargement Nation Community Security Reqirement Statement). Drugi dokument, ki predstavlja podlago za kreiranje SSRS dokumenta je CSRS, za Crisis Response Operations in NATO Open Systems-Operacije kriznega odzivanja za NATO odprte sisteme.

V tej izjavi je vključenih več poglavij katera natančno opredeljujejo različna varnostna področja in zahteve za posamezna področja. Ta poglavja opredeljujejo več področij:

- Uvod z zgodovino sistema, lokacijo sistema in njegovimi uporabniki.
- Definicijo sistema z vlogo sistema in varnostnimi stopnjami tajnih podatkov. Varnostna dovoljenja uporabnikov, ki so najmanj stopnje NATO TAJNO. Administratorji in kripto skrbniki pa NATO STROGO TAJNO, oziroma do najvišje stopnje tajnosti podatkov, ki jih obdeluje sistem.
- Varnostne zahteve z možnimi grožnjami sistemu, ki jih delimo na tri kategorije: naravne, nenamerne in namerne.
- Definicije varnostnih območij: GSE (Global Security Environment), ki predstavlja varnostno domeno izven kontrole CNKZP. LSE (Local Security Environment), ki se nanaša na varnostno domeno znotraj območja CNKZP. I. Varnostno območje mora biti ustrezno fizično in proceduralno varovano, zaradi posedovanja, procesiranja in upravljanja s podatki ustrezne stopnje tajnosti NATO. LSE področje je področje odgovornosti ISSO– Informations Systems Security Officer-ja.
- Definicije varnostnih ukrepov, kot so dostop in dostopne kontrole, z namenom identifikacije vseh uporabnikov sistema in njihove avtentikacija (po SSRS).

5.2 SECOPS (SECURITY OPERATING PROCEDURES)

Je dokument, kateri opredeljuje vse varnostne postopke v CNKZP. Sestavljen je iz dveh delov. V dokumentu so navedena tudi razmerja in relacije sodelovanja med Nacionalno varnostno agencijo, organom odgovornim za varnost komunikacijsko-informacijskih sistemov ter nalogami varnostnega častnika CNKZP ali 16.BNZP.

Ta dokument postavlja minimalne varnostno operativne zahteve, katere morajo biti izpolnjene za delovanje CNKZP. Vsi posamezniki, ki delujejo v sistemu morajo biti seznanjeni z zahtevami in določili dokumenta SecOPs. Prvi del opisuje varnostne postopke vseh uporabnikov v sistemu ter je namenjen vsem zaposlenim v CNKZP. Drugi del pa se osredotoča na varnostne zahteve za tehnično osebje, s področja komunikacijske in informacijske tehnologije (CIS/Security). Torej vse tiste, kateri imajo dodatne specifične tehnične ali varnostne odgovornosti ter naloge.

Dokument opisuje vse postopke v primeru vstopa obiskovalcev CNKZP in vstopa pogodbenih podizvajalcev, oziroma vzdrževalcev podsistemov. Prav tako so navedeni vsi pogoji katere mora izpolnjevati vsaka oseba, da pridobi dovoljenje za vstop v CNKZP ter za dostopanje do tajnih podatkov.

Navedena tudi funkcija podregistra in njegova vloga pri hranjenju podatkov ustrezne stopnje tajnosti. Zavedeni so tudi vsi postopki za uničenje tajnega materiala in podatkov ustreznih stopenj tajnosti. Opisani in opredeljeni so tudi postopki v primeru zaznave varnostnih kršitev.

5.3 SITE INSTALATION REPORT

Poročilo je dokument, izdan s strani NATO, kateri podaja akreditacijsko ali reakreditacijsko poročilo NATO akreditacijske skupine za vsako preverjeno CRC mesto. Ta dokument opredeljuje natančno razporeditev, opis, lastnosti in specifikacije elementov ter prostorov akreditiranega CRC-ja.

5.4 CERTIFICATE OF COMPLIANCE

Certifikat ustreznosti je certifikat, ki se izdaja s strani proizvajalca programske opreme, kateri s tem dokumentom jamči, da je programska oprema izdelana v skladu z določili zveze NATO za tehnične sisteme nadzora zračnega prostora. Torej je interoperabilna z ostalimi sistemi zveze NATO in NATO CRC-ji.

5.5 NAČRT VAROVANJA TAJNIH PODATKOV V CNKZP

Vsako varnostno območje mora imeti izdelan načrt varovanja tajnih podatkov (v nadaljevanju NV). Načrt je izdelan na podlagi 32. člena Uredbe o varovanju tajnih podatkov (Uradni list RS, št. 74/05). Tudi CNKZP ima izdelan NV, vendar zaradi interne narave dokumenta in njegove stopnje tajnosti ni predstavljen v zaključni nalogi. Predstavljen je splošen vzorec VN, z namenom predstavitve predpisane vsebine NV. V grobem lahko razdelimo načrt varovanja tajnih podatkov na splošen in poseben del.

5.5.1 Splošen del načrta varovanja tajnih podatkov

V začetku splošnega dela NV je podana ocena ogroženosti, ki kasneje vpliva na izhodiščne kriterije za določanje stopnje nivoja varnostne zagotovitve območja. V oceni so vključeni

morebitni nasilni vstopi, tatvine, naravne nesreče in drugi incidenti v preteklosti na lokaciji in v njeni neposredni okolici ter verjetnost takih dogodkov v prihodnosti. V nadaljevanju sledi opis glavnih in pomožnih objektov ter celotnega varnostnega območja.

Pri opisu makrolokacije je obvezen izdelan opis in zemljevid z vsemi objekti, dovoznimi potmi, bližnjimi površinami, stanovanjskimi in industrijskimi naselji ter vse dovozne poti. Navedena je tudi stopnja varnostnega območja. Opisani morajo biti tudi posamezni prostori objektov in konstrukcijske značilnosti stavb. Podani morajo biti podatki o sistemu varovanja kompleksa ali zgradbe z povezavo fizičnega in tehničnega varovanja. Fizično varovanje mora biti opredeljeno z opisom nalog, izvajalci, načinom dela, intervencijskimi nalogami in območji delovanja.

Po tipih se navede uporabljeno varnostno tehnično opremo, ki je uporabljena za varovanje kompleksa, zgradbe in varnostnega območja (v nadaljevanju VO). Sem spadajo:
- sistemi mehanske zaščite (zunanja ograja, zapornice, bariere, protivlomna vhodna vrata, varnostne rešetke, protivlomne folije na oknih…),
- sistemi za nadzor dostopov (čitalci brezkontaktnih kartic, biometrični sistemi prepoznavanja oseb, električne ključavnice, videodomofonski sistemi),
- sistemi protivlomnega (PV) varovanja (IR javljalniki z alarmno centralo in prenosom alarmnega signala v varnostno nadzorni center (VNC)),
- sistem požarnega varovanja v zgradbi (senzorji in ročni javljalniki za zaznavanje požara ter alarmna požarna centrala s povezavo za javljanje v center, sistemi za samodejno gašenje požara, požarne instalacije),
- sistemi varnostne osvetlitve v kompleksu in zgradbi,
- sistemi videonadzora (video nadzor širše okolice, notranjosti objekta, posameznih prostorov, VO, v videonadzor vgrajen sistem za zaznavanje in javljanje gibanja v video nadzorovanem območju; elektronsko arhiviranje dogodkov, lokacija, mediji za hranjenje videomateriala).

Vključen mora biti tudi opis točk blokade. Opiše se postopke in točke blokade, načine aktiviranja in preklica ter pristojnosti. Opiše se posamezne nadzorne točke in naloge na njih. Točke se vnese v ustrezne tlorise.

NV vsebuje tudi seznam usposabljanj s področja varnosti vseh oseb, ki dostopajo do tajnih podatkov. Seznam usposabljanj je priložen, kot priloga NV. Usposabljanja s področja varovanja tajnih podatkov se mora izvajati najmanj enkrat letno in ob vsaki spremembi zakonodaje s področja varovanja tajnih podatkov. Evidenca usposabljanj za delo s tajnimi podatki vsebuje naslednje rubrike: tema usposabljanja, čas in kraj, izvajalci in udeleženci
Po 38. členu ZTP mora biti nosilec načrta varovanja (v nadaljevanju NNV) zadolžen za izvajanje in beleženje vseh takih usposabljanj. Zagotovljen mora biti notranji nadzor, ki ob uvedbi disciplinskega postopka ali sumu kaznivega dejanja osebi po pravnomočnosti postopka, ki dostopa do tajnih podatkov nadaljnje to prepreči.

5.5.2 Poseben del načrta varovanja tajnih podatkov

Poseben del NV še podrobneje opredeli in opiše VO in vse glavne ter pomožne objekte in prostore v njih. Prav tako se podrobneje opredeli vse postopke in sisteme tehničnega

varovanja ter električne energetske, klimatske, prezračevalne in komunikacijske instalacije. Dodatno se opredeli naslednje elemente za VO I. stopnje:

- v prostorih so sestanki, na katerih se zvočno obravnavajo tajni podatki določene stopnje;
- prostori so operativni center, v katerem so tajni podatki (panoji, tabele na stenah, …) stopnje tajnosti do vključno _____ vidni že ob vstopu v prostor;
- akustična izolacija vrat, oken, sten, …
- vizualna izolacija - rolete za zastiranje oken; refleksne folije na oknih;
- TEMPEST zaščita, če je potrebna
- odlaganje mobilnih telefonov in snemalnih naprav pred vstopom v VO v predalnik, …
- izvajanje protiprisluškovalnih pregledov
- nadzor nad vnosi in iznosi opreme- postopki, zadolžitve.

TEMPEST je izraz, ki opredeljuje standard zaščite ožičenja in informacijskih sistemov, predvsem državnih organov in ustanov, pred nezaželjenim in nepooblaščenim dostopanjem do tajnih in ostalih podatkov. To je opredeljeno predvsem skozi nezaželjeno prestrezanje, analiziranje ter razkrivanje podatkov, ki se pošiljajo, obdelujejo, sprejemajo ali kakorkoli obdelujejo z opremo za informacijsko obdelavo podatkov. Nezaželjena oddajanja so sestavljena iz električnih ali akustičnih impulzov, ki so nenamerno oddajani s strani enega od mnogih virov znotraj sistemov in opreme, kateri obdelujejo nacionalne ali mednarodne tajne podatke. NATO standard opredeljuje tri stopnje zaščite in sicer:

- Stopnja A, ki je nastrožja po stopnji zaščite in predvideva delovanje v območju, kjer je možno nezaželjeno dostopanje s strani nepooblaščene osebe iz sosednjega prostora ali enega metra oddaaljenosti. Je standard za najstrožje laboratorijske razmere.
- Stopnja B, je rahlo manj stroga in predvideva, da se nepooblaščena oseba ne more približati bližje od 20m, oziroma na ekvivalent debeline različnega gradbenega materiala. Je standard za zaščiteno opremo znotraj zaščitenih področij.
- Stopnja C, je najmanj zahteven standard za mobilne taktične sisteme in predvideva, da se nepooblaščena oseba ne more približati bližje od 100m, oziroma na ekvivalent debeline različnega gradbenega materiala.

Vsi podatki in predpisi, ki določajo standarde na tem področju so tajni in niso javno dostopni. Vsi sistemi morajo biti ustrezno TEMPEST certificirani, vendar kot celota in ne samo za posamezne komponente, ker se z povezavo samo enega nezaščitenega elementa (npr. kabla) lahko zelo poveča oddaja nezaželjenih signalov. Cenejša zaščita je postavitev sistemov v popolnoma elektronsko zaščitene prostore.

Podrobneje se opredeli ukrepe fizičnega varovanja in sicer se opredeli zunanje in notranje fizične varovanje. Navede se izvajalce fizičnega varovanja, kako in kdaj se izvaja, lokacije varnostnih točk, nadzor čistilnega in vzdrževalnega osebja, morebitne pogodbe z zasebnimi varnostnimi družbami ter opis intervencijske skupine znotraj VO.

Poseben del opredeljuje podrobneje tudi ukrepe tehničnega varovanja. Opiše se postopke, tehnične podatke in ukrepe za sisteme:

- sistemi mehanskega varovanja,
- sistemi za nadzor dostopov,
- sistemi protivlomnega varovanja,
- sistem požarnega varovanja,
- sistemi videonadzora in varnostne osvetlitve.

Pomemben del sistema je izdelava, hranjenje evidenc in opisov vzdrževalnih pregledov ter preverjanja ustreznosti sistemov. Zavede se periodična testiranja in preglede, rezultate preverjanj in nastavitev ter postopke ob napakah. V tem delu VN se napiše tudi postopke ob zamenjavi ali izgubi ključev ali kombinacij za dostopanje do tajnih podatkov.

V tem delu se poimensko opredelita NNV in njegov namestnik z vsemi potrebnimi podatki o razpoložljivosti. Ob koncu vzorca NV so navedene tudi vse evidence, ki morajo ali je zaželjeno, da se nahajajo, kot priloge ali ločeno. Evidence, ki so priloge k NV so:
- Evidenca o dopolnitvah in spremembah vsebine NV.
- Informacija o odzivnem času intervencijske službe, policije in gasilcev.
- Spiski vzdrževalnega in servisnega osebja, ki lahko pod določenimi pogoji vstopa na lokacijo oziroma v VO.

Ločene evidence so sledeče:
- Evidenca tajnih podatkov v VO.
- Evidenca vstopov v VO.
- Načrt in evidenca usposabljanj za delo s tajnimi podatki.
- Evidenca o posegih in preverjanjih v VO in na tehnični varnostni opremi.

Podrobneje so opredeljeni izredni dogodki in postopki za ukrepanje ob nastopu le teh:
- postopek ob sprožitvi protivlomnega alarma,
- postopki ob nasilnem vstopu in nepredvidenem dogodku (velja za požar, potres, povodenj ali druge naravne nesreče),
- postopki in ukrepi ob izgubi, razkritju ali odtujitvi tajnih podatkov,
- ukrepi in postopki pri opravljanju vzdrževalnih in drugih del v varnostnem območju.

5.5.2.1 Postopek ob sprožitvi protivlomnega alarma

Za primer sprožitve protivlomnega alarma v VO se opišejo naslednji postopki:
- naloge osebe, ki sprejme alarmni signal (VNC), nadaljnje obveščanje NNV in drugih,
- v primeru nasilnega vdora obveščanje Obveščevalno Varnostna Služba (OVS) MORS,
- v primeru lažnega alarma pisno obveščanje OVS,
- s službo za varovanje usklajeno zavarovanje območja; kdo vodi zavarovanje,
- evakuacija na rezervno lokacijo v primeru potrebe.

5.5.2.2 Postopki ob nasilnem vstopu in nepredvidenem dogodku

Opredeli se naslednje postopke in ukrepe, ki v splošnem veljajo tudi za požar, potres, povodenj in druge naravne nesreče:
- način in dolžnost obveščanja (kdo, koga),
- postopki do prihoda odgovorne osebe (kdo je to),
- način vstopa v VO,
- postopki zavarovanja lokacije in VO,
- kdo in v katerih primerih odloči o evakuaciji,
- izvedba:
  - varovanja prenosa TP na drugo-rezervno lokacijo,
  - varovanja TP na drugi lokaciji,
  - inventure TP in opreme za obdelavo TP.
- evidenca in poročilo o dogodku.

5.5.2.3 Postopki in ukrepi ob razkritju, izgubi ali odtujitvi tajnih podatkov

Opredeli se navodila za ukrepanje, poročanje, javljanje, naloge zaposlenih, moštva za varovanje, morebitna dodatna navodila za moštvo, ki varuje objekt, predvsem pa način zavarovanja kraja v primeru dogodkov, obveščanja odgovornih in drugih služb (varnostni organi, gasilci, policija, …), intervencija. Kadar se ugotovi sum odtujitve tajnega podatka, oziroma je dejansko prišlo do odtujitve tajnega podatka, je treba zagotoviti vse potrebno za zavarovanje dokazov in preprečiti možnost povzročitve še večje škode. Ugotovi se vsa dejstva in okoliščine pri odtujitvi ali razkritju z namenom, da se prepreči ponovna odtujitev ali razkritje in takoj obvesti organ, ki je originator tajnega podatka.
V navedenih primerih se opišejo naslednji postopki:

- Takojšnje obveščanje o dogodku (NNV, OVS, osebe, ki je določila stopnjo TP, vodja pristojne organizacijske enote).
- Zavarovanje kraja dejanja in sledi - usklajeno s službo za varovanje (če je prišlo do odtujitve, nasilnega vstopa in podobno, oziroma dokazov, da je prišlo do razkritja tajnega podatka nepooblaščeni osebi).
- Pregled evidence tajnih dokumentov in inventura (odredi NNV).
- Obveščanje NVO v primeru, da je prišlo do odtujitve tajnega podatka NATO ali EU, oziroma tuje države.
- Drugi potrebni postopki in ukrepi za ugotovitev okoliščin odtujitve in izsledite storilca, preprečitev ponovitve dejanja, zmanjšanje posledic ter zavarovanje tajnega podatka.

NNV po potrebi odredi preizkus delovanja sistemov (protivlomnega varovanja, video nadzornega sistema, kontrole dostopov).

Postopki varnostne službe (VS): delavci VS v primerih izrednih dogodkov ne smejo vstopati v VO, ampak ga morajo zavarovati in počakati na prihod NNV. V VO lahko vstopajo zaradi preprečevanja ogrožanja življenja ali če je to drugače posebej odrejeno. NNV lahko vstopi v spremstvu policaja, zaradi osebne varnosti.

Postopki in ukrepi zaposlenih: kadar zaposleni ugotovi sum, da je prišlo do odtujitve ali razkritja tajnega podatka, o tem takoj obvesti NNV oziroma svojega vodjo in mu posreduje vse podatke o okoliščinah, ki kažejo na to, da je prišlo do odtujitve ali razkritja tajnega podatka. V okviru pristojnosti izpelje NNV dodatne postopke in ukrepe za varovanje tajnih podatkov. V primeru, da kdorkoli v OE ugotovi morebitno grožnjo, ki bi kazala na poškodovanje, odtujitev ali drugačno ogrožanje tajnih podatkov, ki se nahajajo v VO, o tem obvesti NNV.

5.5.2.4 Postopki pri opravljanju vzdrževalnih in drugih del v varnostnem območju

Določi se postopke in pristojnosti, vezane na omenjene dejavnosti in osebe:

- kdo lahko kaj izvaja, način predhodne najave,
- način preverjanja identitete, dovoljenja za dostop do TP, opreme, ki se vnaša,
- način gibanja, spremstvo,
- režim in ukrepi v zvezi z varovanjem TP v času dejavnosti (shraniti TP v varnostne vsebnike, …).

Kot je razvidno je NV pomemben interni dokument, ki jasno opredeljuje naloge, postopke in ukrepe za vse predvidene in nepredvidene dogodke v tipu objekta, kot je CNKZP.

6. ZAKLJUČEK

S članstvom Republike Slovenije v zvezi NATO in EU se je ta obvezala k izpolnjevanju določil in predpisov obeh mednarodnih organizacij. Eden od predpogojev za pridružitev in zagotovitev delovanja znotraj teh struktur, je postavitev ustreznega varnostnega sistema za dostopanje, obdelovanje, pošiljanje, hranjenje in unčevanje NATO in EU tajnih podatkov. Ta sistem predstavlja osnovo varnostne zagotovitve vseh udeleženih v procesu dela, znotraj obeh organizacij.

Vidne spremembe na tem področju je Slovenija doživela po letu 2001, ob sprejetju Zakona o tajnih podatkih. S tem korakom je opredelila in definirala naloge osnovnih pooblaščenih nacionalnih organov, za izvedbo ustrezne postavitve varnostnega sistema, za vsa varnostna območja in področja, kjer se tajni podatki dostopajo in obdelujejo. Pomembnost varnostnega področja se kaže tudi v množici predpisov in ukrepov za doseganje željenega minimalnega varnostnega nivoja, ki je predpisan glede na različne kriterije in potrebe za posamezna območja. Med varnostno pomembna območja spada tudi CNKZP, ki je del NATINADS. Tako predstavlja le kamenček v mozaiku mreže, ki je spletena čez zračni prostor območja zveze NATO, z namenom izvajanja kolektivne varnosti zračnega prostora na območju držav članic.

Pomembnost ustanovitve in vzdrževanja ustreznega varnostnega sistema, znotraj tega pa sistema varovanja tajnih podatkov, se kaže tudi v mnogih aferah in incidentih (prisluškovanje znotraj organov EU, afera SOVA). Ti so posledica pomanjkljivosti in napak pri varnostni zagotovitvi. Poudariti je potrebno, da je vsak varnostni sistem dober kolikor ima ustrezen nivo varnostne kulture oseb, ki dostopajo in obdelujejo tajne podatke, tako nacionalne, kot mednarodne. Zveza NATO ima dobro dodelan sistem standardov in predpisov, ki opredeljujejo varnostno področje in posledično ga je deloma prevzela tudi EU. Vse te predpise poleg nacionalnih izpolnjuje tudi CNKZP, kar potrjuje tudi dejstvo, da je akreditiran s strani NATO evalvacijske skupine. Potrebna je še akreditacija z nacionalne strani.

Pri vzpostavitvi varnostnega sistema CNKZP aktivno sodelujejo vsi zaposleni. Pomembno vlogo pri dvigu nivoja varnosti in izobraževanja imajo vsi zaposleni v S2, predvsem varnostni častniki. Njihova naloga je tudi izvajanje ustreznih ukrepov in izobraževanja, z namenom sledenja vsem varnostnim spremembam in potrebam. Varnostno morajo biti pokrita vsa varnostna področja in sicer fizično, kadrovsko, varnost informacij, industrijsko in informacijskih-komunikacijskih sistemov. Slednje je v tehnični enoti, kot je CNKZP, še posebno pomembno in bi bilo smotrno v prihodnosti zagotoviti dodatnega varnostnega častnika za področje informacijsko-komunikacijske tehnologije. Ta mora biti nujno iz stroke in z določenimi izkušnjami pri ravnanju s tajnimi podatki. Dejstvo je, da neustrezno ravnanje in varnostna nekultura zaposlenih lahko resno ogrožata operativnost in kompatibilnost CNKZP, kot NATO CRC-ja znotraj NATINADS.

Kot I. varnostno območje, kjer se obdelujejo, hranijo, dostopajo, pošiljajo in uničujejo tajni podatki stopne NATO ZAUPNO in višje, mora biti CNKZP vedno v koraku z vsemi minimalnimi standardi in predpisi tako na nacionalnem nivoju, kot v zvezi NATO. V prihodnosti se bodo zahteve in predpisi še dopolnjevali in postajali strožji, kar pomeni tudi dodatne zahteve in izobraževanje na varnostnem področju. Zato je pomembna zagotovitev

ustreznega števila varnostnega kadra, z namenom doseganja ustreznega in kvalitetnega varnostnega nivoja tako objektov samih, kot tudi nivoja varnostne kulture in zavedanja vseh zaposlenih.

LITERATURA

- mag. ČALETA, Denis. Ustrezen sistem varovanja tajnih podatkov – nujnost v Slovenski vojski. Bilten Slovenske vojske. 2003, let. 5/2, št. 2/2003, str. 99-116.
- mag. ČRNEC, Damir. Ravnanje s tajnimi podatki. Obramba. 2004, let. 36, št. 1/2004, str. 18-21.

VIRI

- NATO, ACO Directive Number 70-1.
- NATO, AC/35-D/2000 Directive on Personnel Security.
- NATO, AC/35-D/2001 Directive on Physical Security.
- NATO, AC/35-D/2002 Directive on Security of Information.
- Zakon o tajnih podatkih, Ur. List RS, št. 87/01, 101/03, 135/03.
- Uredba o varovanju tajnih podatkov, Ur. List RS, št. 74/05.
- Uredba o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov, Ur. List RS, št. 70/02.
- Uredba o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov, Ur. List RS, št. 031-07/2002-1
- Hišni red Centra za nadzor in kontrolo zračnega prometa Brnik.

INTERNETNI VIRI

- http://mors-web/intranet/ovs/varnostne_naloge/fiz_teh_var.htm
- http://en.wikipedia.org/wiki/TEMPEST

IZJAVA O AVTORSTVU

Spodaj podpisani Grega Osojnik, rojen 24.01.1977 v Ljubljani, kandidat 17. generacije Šole za častnike, izjavljam, da sem nalogo izdelal sam, s pomočjo mentorja st Gorana Vareka.

Ljubljana, september, 2007 nvu VII Grega Osojnik