UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Jožef Grabušnik
Mentor: doc. dr. Iztok Prezelj

TEHNIČNO IN FIZIČNO VAROVANJE NA OBRAMBNEM PODROČJU

Specialistično delo

Ljubljana, 2007

ZAHVALA

Dragici, Loresani in Anemariji.

VSEBINA

SEZNAM SLIK IN TABEL

SLIKE

TABELE

PRILOGE

A. Predlog vzpostavitve varnostnih območij
B. Varovalne ograje
C. Obrazec za takojšnje poročanje o okvari tehničnega sistema
D. Obrazec za mesečno poročanje o okvarah tehničnega sistema
E. Označevanje varnostnih območij
F. Začasni standardi na področju tehničnih sistemov za varovanje
G. Tabelarni prikaz opremljenosti varnostnih območij
H. Poročilo o izbiri varovalne ograje v Ministrstvu za obrambo Republike Slovenij

SEZNAM UPORABLJENIH KRATIC IN OKRAJŠAV

ACE	Allied Command Europe – Evropsko združeno poveljstvo
AJP	Allied Joint Publication – Združena zavezniška publikacija
FDV	Fakulteta za družbene vede
GŠSV	Generalštab Slovenske vojske
G-2	Obveščevalno-varnostni sektor Poveljstva sil Slovenske vojske
G-3	Operativni sektor Poveljstva sil Slovenske vojske
G-4	Logistični sektor Poveljstva sil Slovenske vojske
I	Interno
J-2	Obveščevalno-varnostni sektor Generalštaba Slovenske vojske
NRVSNR	Notranja razsvetljava in vzdrževanje sistemov notranje razsvetljave
NSRMP	Nato Security Risk Management Process
OVS	Obveščevalno-varnostna služba Ministrstva za obrambo
PSSV	Poveljstvo sil Slovenske vojske
PVTP	Pravilnik o varovanju tajnih podatkov na Ministrstvu za obrambo
RS	Republika Slovenija
SDPVO	Sklep o določitvi za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja
SDR	Slovensko društvo za razsvetljavo
ST	Strogo tajno
SV	Slovenska vojska
T	Tajno
TP	Tajni podatek
UOOSV	Uredba o obveznem organiziranju službe varovanja
UVTP	Uredba o varovanju tajnih podatkov
VPŠ	Višja policijska šola
Z	Zaupno
ZZasV	Zakon o zasebnem varovanju
ZoO	Zakon o obrambi
ZVOP	Zakon o varstvu osebnih podatkov

1 UVOD

Že na začetku svojega obstoja je človek razvil potrebo po varovanju skrivnosti. Skozi stoletja so se načini varovanja razvijali in spreminjali. Razvoj varovanja skrivnosti je narekoval razvoj tehnologije, s katero so posamezniki ali skupnosti dosegali prednosti pred drugimi in s tem potrebo po tajnosti.

Za dosego cilja, zavarovati skrivnost pred drugimi, pa je človek začel presegati svojo domišljijo. Skrivne kote v jamah so zamenjale sodobne in drage naprave, ki nas varujejo pred zlorabo tajnosti. Varovanje pa ni prepuščeno samo tehniki, tajne podatke varuje tudi človek. Še več, človek je tisti, ki nadzoruje tehniko. Žal pa je človek tudi tisti, ki zlorablja, razkriva skrivnost in čuti potrebo, da nekomu drugemu, za določeno korist, izda nekaj, kar temu daje prednost pred drugimi.

Republika Slovenija (v nadaljnjem besedilu: Slovenija) v tem ni nikakršna izjema, saj je tudi njeno varnostno okolje dinamično in spremenljivo ter neločljivo povezano z negotovostjo in nestabilnostjo v državah znotraj evroatlanskega območja in zunaj njega.

Negotovost in nestabilnost sta povezana z mednarodnim terorizmom in množičnimi migracijami, organiziranim kriminalom, trgovino z drogami, korupcijo, etičnimi in verskimi nasprotji, nestabilnimi režimi, teritorialnimi spori in spori zaradi naravnih virov, rastjo ali upadom prebivalstva, epidemijami ter udari na informacijske infrastrukture in njihovimi zlorabami (povzeto po Furlan, 2006: 12). Vse te pojavne oblike vplivajo na splošno raven varnosti RS, ki jo po Grizoldu (1999: 23) lahko razumemo kot stanje, v katerem je zagotovljen uravnotežen fizični, duhovni in duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave.

Edmonds varnost dodatno opredeljuje kot nejasen in večpomenski koncept, ki ga običajno štejemo med temeljne družbene vrednote, hkrati pa trdimo, da gre pri tem konceptu za okoliščine, v katerih so zagotovljene oziroma zaščitene vse temeljne družbene vrednote. Varnost je torej mogoče opredeliti kot sredstvo pa tudi kot metodo zavarovanja družbenih vrednot (Edmons v Jelušič, 1997: 70).

Z razvojem informacijske infrastrukture je Slovenija postala zelo ranljiva tudi na komunikacijsko-informacijskem področju. Na tem področju obstajajo različna tveganja, ki

ogrožajo varnost kritične infrastrukture, varnost baz podatkov kot temeljev za odločanje in delovanje državnih, finančnih, gospodarskih, socialnih, zdravstvenih in drugih organov.

Prezelj razume grožnje varnosti v kontekstu razmerja do varnosti. Pri tem pa poudarja, da je razmerje deterministično v obe smeri in da razumevanje varnosti referenčnega objekta vpliva na identificiranje groženj varnosti tega objekta in obratno. Pri tem poudarja, da brez ogrožanja varnosti pojem varnosti sploh ne bi bil spoznaven in torej sploh ne bi obstajal. Sam koncept varnosti opredeljuje z njegovim nasprotjem, podobno kot ne bi mogli nečesa označiti za svetlo ali veliko, ne da bi razumeli, kaj pomeni temno ali majhno (Prezelj, 2005: 9).

Različna tveganja, ki so jim izpostavljeni državni organi, so prinesla razvoj tehnologije na področju varovanja. Varnosti ne zagotavlja samo človek, ampak jo vedno bolj dopolnjuje tudi tehnika. Razvoj tehnike za varovanje tajnih podatkov in sredstev je zelo napredoval.

Posebnost varnostnega sistema pa so tajni in zaupni podatki, ki jih je treba varovati pred morebitnim sovražnikom. Za nadzor javnosti so ti podatki nedosegljivi (Jelušič, 1997: 78).

Največ tajnih podatkov, ki jih je treba varovati v Sloveniji, je na obrambnem področju. Varnost obrambnega področja zagotavljajo obveščevalni, protiobveščevalni in varnostni organi (Zakon o obrambi, prečiščeno besedilo 2004: 32. in 33. člen). Njihova naloga je načrtovanje, organiziranje in zagotavljanje varnosti tajnih podatkov in sredstev. Varnost zagotavljajo s fizičnim in tehničnim varovanjem.

S sistemom tehničnega varovanja se na obrambnem področju varujejo osebe, premoženje Ministrstva za obrambo in tajni podatki (Zakon o tajnih podatkih, 2003, dopolnjen 2006: 39. člen). Varovanje se izvaja fizično ter z uporabo tehničnih sredstev in kombinirano.

Fizično varovanje zajema ukrepe za zaščito osebja, objektov vojaške infrastrukture, tajnih dokumentov, orožja in minskoeksplozivnih sredstev ter drugih materialno-tehničnih sredstev. Fizično varovanje zagotavlja varnost pred vohunjenjem, sabotažami, uničenjem in krajo.

Tehnično varovanje objektov vojaške infrastrukture je še vedno dopolnilo fizičnemu varovanju. Skupaj pa zagotavljata povišano pripravljenost za delovanje vseh poveljstev in enot Slovenske vojske. S povišano pripravljenostjo se pred različnimi vrstami ogrožanja zagotavlja varnost objektov, ljudi v objektih, tajnih dokumentov, ki se hranijo v varnostnih območjih, ter oborožitve, streliva, minskoeksplozivnih in materialno-tehničnih sredstev.

S prehodom na profesionalno vojsko in ukinitvijo nabornega sistema se je način varovanja spremenil. Zaradi pomanjkanja vojakov za varovanje je Slovenska vojska začela tajne podatke in objekte varovati s kombiniranim varovanjem (tehnično in fizično).

Objekti in stopnje tehničnega varovanja so opredeljeni v Direktivi za organizacijo in izvajanje varovanja objektov v Slovenski vojski, številka: I 854-03-6/2003-2-64 z dne 14. 2. 2003, minister za obrambo pa je za urejanje področja tehničnega varovanja in odpravo pomanjkljivosti izdal Obvezne usmeritve za kratkoročne in srednjeročne aktivnosti za boljše varovanje vojaških objektov (Kabinet ministra, št. 854-03-1/2000, z dne 22. 2. 2000).

Do leta 2000 je celotno področje tehničnega varovanja objektov za potrebe Slovenske vojske organizirala in vodila Obveščevalno-varnostna služba Ministrstva za obrambo Republike Slovenije, v sestavi katere je bil oddelek za tehnično varovanje. Obveščevalno-varnostna služba je izdelovala varnostne ocene in načrte varovanja, načrtovala pa je tudi gradnjo in izvedbo tehničnega varovanja. Slovenska vojska je načrtovala le fizično varovanje objektov in je leta 2001 od Obveščevalno-varnostne službe prevzela naloge za svoje sisteme tehničnega varovanja.

Zakon o obrambi (Uradni list RS, št. 103/04 – prečiščeno besedilo) v 29. členu določa, da vlada določi objekte in okoliše objektov, ki so posebnega pomena za obrambo, ter predpiše ukrepe za njihovo varovanje. Na tej podlagi je bila sprejeta Uredba o določitvi objektov in okolišev objektov, ki so posebnega pomena za obrambo, in ukrepih za njihovo varovanje (Uradni list RS, št. 7/99 in 67/03). Glede na to, da se v nekaterih objektih obravnavajo tudi tajni podatki različnih stopenj tajnosti, je treba pri vzpostavljanju sistema varovanja upoštevati določbe Zakona o tajnih podatkih (Uradni list RS, št. 135/03 – prečiščeno besedilo in 28/06), Uredbe o varovanju tajnih podatkov (Uradni list RS, št. 74/05), Pravilnika o varovanju tajnih podatkov na Ministrstvu za obrambo (šifra 0070-5/2006-4 z 21. 2. 2006) in Sklepa o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja (Uradni list RS, št. 94/2006). Poleg teh ključnih predpisov je treba pri načrtovanju in izvajanju postopkov in ukrepov varovanja upoštevati tudi druge predpise in interne akte, ki se nanašajo na to področje, kot so: Pravila službe v Slovenski vojski (Uradni list RS, št. 49/96, 111/00 in 52/01), Direktiva za organizacijo in izvajanje varovanja objektov v Slovenski vojski (2002) in Hišni red v poslovnih stavbah na obrambnem področju.

Slovenija je z vstopom v zvezo Nato morala spremeniti tudi zakonodajo na področju varovanja tajnih podatkov. Rešitve varovanja tajnih podatkov in objektov, ki so bile v

uporabi do leta 2004, niso več zagotavljale varnosti po Natovih standardih. Razen sprejete zakonodaje na področju tehničnega varovanja na obrambnem področju ni napotil ali usmeritev, ki bi poenostavili delo podrejenih funkcijskih organov za nameščanje tehničnih sistemov v varnostna in druga območja.

V Natovih civilnih in vojaških telesih in znotraj držav članic Nata je sistematični pristop za določitev potrebnih protiukrepov za samozaščito informacij, podpornih služb in resursov določen v Natovem procesu upravljanja z varnostnim tveganjem (Nato Security Risk Management Process – NSRMP, AC/35(AHWG-SPG)WP(2004)0010-Annex 1).

NSRMP je metoda, ki pomaga vodstvom Natovih civilnih in vojaških teles pri odločanju o ustreznih in cenovno sprejemljivih ukrepih za zaščito tajnih podatkov in materialov. NSRMP upošteva minimalne varnostne standarde in temelji na naslednjih načelih:

- zaščitni ukrepi nikoli ne nudijo popolne zaščite pred vsemi vrstami groženj in ranljivosti, ampak omejijo tveganje na sprejemljivo raven, upoštevajoč ceno teh ukrepov;
- najcenejši ukrepi so tisti, ki skupaj uporabljeni predstavljajo integralni in uravnoteženi režim varovanja;
- težnja po zmanjšanju tveganja na sprejemljivo raven tehta potencialno škodo in ceno varovanja.

Ta načela so vgrajena v različne uporabne in dokumentirane procese, ki se lahko obnavljajo, če se spremenita ogroženost ali ranljivost tajnih podatkov.

NSRMP omogoča določeno fleksibilnost pri določanju posameznih stopenj zaščite tajnih podatkov ali drugače občutljivih ali vrednih materialov glede na oceno tveganja. Zaradi doslednosti in skladnosti so upoštevani tudi minimalni varnostni standardi za varovanje Natovih tajnih podatkov in občutljivih materialov, kot jih določajo Natova varnostna politika (NATO Security Policy) in njegove podporne direktive.

Slovenija je z ratifikacijo Natovih direktiv in standardov določila, da mora tehnično in fizično varovanje ustrezati standardom zveze Nato. S tehnični sistemi se morajo dosegati minimalne zahteve po varnostni direktivi AD 70-1 (ACE Security Directive). Na podlagi teh direktiv je Slovenija spremenila in prilagodila slovenske predpise, ki urejajo tehnično in fizično varovanje (Čaleta, 2004: 61).

Upoštevati je treba, da se bo normativno področje za varovanje tajnih podatkov in materialov stalno spreminjalo in dopolnjevalo. Zato bo treba vselej preverjati veljavnost

posameznega predpisa ali internega akta ter postopke in ukrepe varovanja prilagajati veljavnim predpisom in internim aktom.

Specialistično delo je odraz potrebe po učinkovitem in najprimernejšem varovanju tajnih podatkov in objektov na obrambnem področju Republike Slovenije. Na tem področju v Sloveniji ni znanstvenih in strokovnih analiz. Urejena je le zakonodaja.

2 METODOLOŠKO HIPOTETIČNI OKVIR

2.1 PREDMET PREUČEVANJA

Predmet preučevanja v specialističnem delu je tehnično in fizično varovanje na obrambnem področju v Republiki Sloveniji. Pri preučevanju in analiziranju tehničnih in fizičnih sistemov bom poskušal prispevati k poenotenju sistemov tehničnega in fizičnega varovanja na obrambnem področju Republike Slovenije. Poenotenje sistemov bo prispevalo k večji varnosti tajnih podatkov in objektov na obrambnem področju Republike Slovenije. Z delom želim prispevati k večji kompatibilnosti sistemov ter k sodobnosti sistema tehničnega varovanja, ki bo uspešno dopolnjeval fizično varovanje.

Specialistično delo bo vsebovalo analizo tehničnih sistemov in naprav, ki so že vgrajeni v varnostna območja in objekte Ministrstva za obrambo (v nadaljnjem besedilu: ministrstva), in sistemov, ki se še bodo vgrajevali v varnostna območja in objekte ministrstva skladno z zakonodajo, sprejeto po letu 2004. Pri tem bom upošteval ključni problem ministrstva, to je vsestransko in racionalno uporabo tehničnih sredstev in pripadnikov Slovenske vojske za varovanje tajnih podatkov in objektov.

S hitrim spreminjanjem varnostnih razmer v svetu in regiji je varnost začela dobivati novo vlogo, iz katere izhajajo nove naloge in načini varovanja tajnih podatkov in objektov na obrambnem področju (Prezelj, 2006: 2). Zato bom v delu poskušal predstaviti nove trende, ki omogočajo učinkovito varovanje tajnih podatkov in materialov. Pri tem bom izhajal iz splošne relevantnosti specialističnega dela, ki je v preučevanju sprejetih standardov tehničnih sistemov in fizičnega varovanja na obrambnem področju Republike Slovenije, ter iz empirične relevantnosti, ki je v uporabnih izhodiščih, za izvajanje ustreznih tehničnih ukrepov v Sloveniji, pri zagotavljanju varnosti tajnih podatkov in varovanju objektov na obrambnem področju.

Na obrambnem področju Republike Slovenije postajajo tehnični sistemi vse bolj prisotni pri varovanju tajnih podatkov in objektov, zato je njihovo poznavanje nujno. Poznavanje teh sistemov in njihovo nemoteno delovanje, brez okvar, pa bo lahko zagotovil samo usposobljen kader. Zato se bo vsebina mojega dela lahko uporabljala tudi kot del napotil ali usmeritev za namestitev tehničnih sistemov in zagotavljanje fizičnega varovanja na obrambnem področju Republike Slovenije.

S specialističnim delom želim svoje dveletne izkušnje in znanje na področju tehničnega varovanja prenesti na vse varnostne organe v Slovenski vojski, ki se ukvarjajo z varovanjem tajnih podatkov in objektov na obrambnem področju Republike Slovenije. Z delom si lahko pomagajo tudi vsi pripadniki, ki izvajajo usposabljanje in izobraževanje varnostnega osebja v Slovenski vojski. Predvsem pa je delo namenjeno vsem, ki se želijo podrobneje seznaniti s tehničnimi sistemi, ki vse bolj nadomeščajo človeški vir pri zagotavljanju varnosti tajnih podatkov in objektov.

2.2 CILJI PREUČEVANJA

Pri preučevanju tehničnega in fizičnega varovanja na obrambnem področju Republike Slovenije ter v poveljstvih in enotah Nata sem si zastavil naslednje cilje:

1. prikazati in preučiti standarde in postopke za varovanje tajnih podatkov in objektov v Natu in na obrambnem področju Republike Slovenije;
2. preučiti tehnične sisteme za varovanje tajnih podatkov in objektov na obrambnem področju Republike Slovenije;
3. preučiti fizično varovanje tajnih podatkov in objektov na obrambnem področju Republike Slovenije;
4. in kot končni cilj naloge: prispevati k izgradnji enotnega sodobnega tehničnega in fizičnega varovanja, ki bo zagotavljal učinkovito varnost na obrambnem področju Republike Slovenije.

2.3 HIPOTEZE

Glede na cilje specialističnega dela sem izhajal iz naslednjih hipotez:

1. standardi in postopki za varovanje tajnih podatkov in objektov na obrambnem področju Republike Slovenije so delno usklajeni s standardi Nata;
2. standardi tehničnega varovanja tajnih podatkov in objektov na obrambnem področju Republike Slovenije so usklajeni s standardi Nata;
3. namestitev tehničnih sistemov na objekte in vanje zmanjšuje obseg fizičnega varovanja;

4. samo enotno, učinkovito in sodobno tehnično in fizično varovanje bo zagotavljalo varnost tajnih podatkov in objektov na obrambnem področju Republike Slovenije.

2.4 METODE

Pristop k specialističnem delu je sistemsko-tehnični. Analizi sistemske urejenosti področja bo sledila analiza tehničnih rešitev, pri tem pa se ne bom spuščal v popolne podrobnosti tehničnih sistemov.

Pri preučevanju tehničnega in fizičnega varovanja na obrambnem področju bom uporabil še naslednje metode:

- uporabo in analizo pisnih in elektronskih virov;
- primerjalno metodo;
- metodo izkustva;
- kvalitativno analizo s pomočjo programskega paketa DEXi (za pomoč pri odločanju).

2.4.1 Uporaba in analiza pisnih in elektronskih virov

Metoda analize vsebine besedil in dokumentov Slovenije in Nata bo uporabljena za ugotavljanje lastnosti tehničnih in fizičnih sistemov, ki zagotavljajo varnost tajnih podatkov in objektov na obrambnem področju Republike Slovenije. Vanjo bom vključil različna znanstvenoteoretična in strokovna dela, pa tudi poljubna dela s področja preučevanja tematike specialističnega dela. Mediji bodo knjige, zakonodaja, strokovni in poljudnoznanstveni članki, različni statistični podatki, internetne strani znanstvenih, strokovnih in drugih civilnih in vojaških institucij.

2.4.2 Primerjalna metoda

Primerjalna metoda bo uporabljena za primerjavo varovalnih ograj, s katerimi ograjujejo objekte na obrambnem področju Republike Slovenije. Na podlagi primerjalne metode in kvalitativne analize bom poskusil izbrati najprimernejšo varovalno ograjo, s katero bodo ograjeni objekti na obrambnem področju Republike Slovenije.

2.4.3 Metoda izkustva

Pri izdelavi dela bom upošteval svoje dveletne izkušnje na področju tehničnega in fizičnega varovanja. Opisal bom poglede in rešitve pri nameščanju in vgradnji tehničnih sistemov v varnostna območja, v objekte ministrstva in na te objekte. Upošteval bom razprave in dogovore, ki so potekali v različnih skupinah, v katerih sem sodeloval.

2.4.4 Kvalitativna analiza

Z metodo kvalitativne analize bom poskušal izbrati najprimernejšo varovalno ograjo za varovanje objektov na obrambnem področju Republike Slovenije. V analizi bom uporabil varovalne ograje slovenskih proizvajalcev. Analizo bom izvedel s pomočjo programske opreme DEXi.

Vsi našteti postopki bodo omogočili potrditev in poglobitev hipotez. Pridobljene podatke bom v zaključku soočil z izhodiščno teorijo in s tem prispeval k njeni obogatitvi.

2.5 TEMELJNI POJMI

Varnost je stanje, ki ga dosežemo, ko so določene informacije, materialna sredstva, osebe, dejavnosti, naprave in oprema zaščiteni pred vohunjenjem, sabotažo, uničenjem in pred terorizmom, kot tudi pred izgubo ali nepooblaščenim razkritjem (AAP-6, 2003: 2-S-3).

Tveganje je verjetnost, da bo varnostno šibka točka uspešno izkoriščena oziroma ogrožena do te mere, da bo prišlo do zlorabe zaupnosti, celovitosti in/ali razpoložljivosti ter bo s tem povzročena škoda (C-M, 2002: 63).

Obvladovanje tveganj je sistematični pristop k določanju varnostnih protiukrepov, potrebnih za zaščito podatkov in podpornih storitev in sredstev, ki temelji na oceni ogroženosti in ranljivosti. Vključuje načrtovanje, organiziranje, vodenje in nadziranje sredstev za zagotavljanje, da tveganje ostane znotraj spremenljivih meja (C-M, 2002: 64).

Tajni podatek je dejstvo ali sredstvo z delovnega področja organa, nanašajočega se na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost, ki ga je treba zaradi razlogov, določenih v Zakonu o tajnih podatkih (v nadaljnjem besedilu: ZTP),

zavarovati pred nepoklicanimi osebami in ki je v skladu z ZTP določeno ali označeno za tajno (ZTP, 2006: 2. člen).

Ocena ogroženosti objekta je niz notranjih in zunanjih faktorjev, ki vplivajo na vrsto, obliko in velikost sistema zaščite varovanih kompleksov, oseb in transportov (Golob, 1997: 125).

Načrt ukrepov fizičnega varovanja je sistem fizičnih ukrepov, ki opredeljuje in določa ukrepe ravnanja osebja v različnih varnostnih situacijah, z namenom preprečitve nepooblaščenega vstopa v varovane prostore in preprečitve kaznivih dejanj (UVTP, 2005: deveto poglavje).

Varnostno območje je fizično ločeno in označeno območje ali prostor, ki se ustanovi z namenom zaščite določenega materiala, dokumentov, informacij in sredstev pred zunanjimi vplivi. Namen ustanovitve varnostnega območja je, da se vzpostavi sistem nadzora, ki preprečuje nepooblaščen dostop do tajnih podatkov. Prostor mora biti zaščiten pred fizičnim vdorom, odtujitvijo, požarom, vdorom vode in drugimi nevarnostmi (Faganel, Anžič, 2006: 2).

Varovano območje je območje, na katerem oseba, ki varuje (stražar, varnostnik), izvaja ukrepe varovanja v skladu z načrtom fizičnega varovanja. Varovano območje lahko obsega kontrolirano območje, kontroliran objekt, kontroliran prostor, nadzorovano območje, nadzorovan objekt, vitalno območje ter vitalni objekt.

Kontrolirano območje je območje na zunanjem robu varovanega območja. Kontroliran je lahko tudi prostor ali objekt, ki je pod občasnim fizičnim in stalnim tehničnim nadzorom.

Nadzorovano območje je območje ali objekt pod stalnim fizičnim in tehničnim nadzorom, ki je obdano z mehansko oviro z omejenim številom vhodov pod ustreznim nadzorom.

Varovani prostor je soba, hodnik, dvorišče, skladišče ali shramba, kjer so shranjeni pomembni podatki ali sredstva, ki jih varujejo pred nepooblaščenimi osebami. Po ravni varovanja ločijo tri skupine varovanih prostorov:

- nadzorovani prostor, v katerem gibanje oseb ni ovirano,
- prostor omejenega gibanja, v katerem je gibanje oseb časovno ali osebno omejeno, in
- izključujoči prostor, v katerem je gibanje dovoljeno le pooblaščenim osebam, prisotnost v prostoru pa je časovno omejena (čim krajša).

Varovana točka je območje v prostoru, kjer so nameščeni senzorski elementi z možnostjo neposrednega odkrivanja dogodkov.

Sistem varovanja je sestavljen iz sistemov za preprečevanje in nadzorovanje, iz alarmnih sistemov, sistemov za prenos alarmnih sporočil, postopkov v varnostno nadzornih centrih ali varnostno nadzornih točkah ter dejavnosti notranjih varnostnih in interventnih sil (Golob, 1997: 27).

Tehnično varovanje je varovanje s tehničnimi sistemi, ki nadzorujejo vstop v prostor in izstop iz njega ter dogajanje v prostoru ali njegovi okolici (Ukaz za organiziranje in izvajanje varovanja objektov GŠSV, 2001).

Tehnični sistemi so tehnična sredstva, ki omogočajo nadzorovanje, odkrivanje in javljanje dogodkov (ZZasV, 2004: 2. člen).

Fizično varovanje je zagotavljanje varnosti oseb, predmetov, dokumentov in objektov s fizično silo – človeški vir (Ukaz za organiziranje in izvajanje varovanja objektov GŠSV, 2001).

Straža so stražarske sile, ki nadzirajo vstope v objekte in izstope iz njih, opravljajo dela na stalnih stražarskih mestih, obhode, izvajajo varnostne preglede in dela v varnostno nadzorni točki (Pravila službe v Slovenski vojski, 2003: točka 3.1).

Interventne sile so sile, ki jih mora imeti vsaka varnostno nadzorna formacija in ki so sposobne poslati najmanj dva človeka na katero koli točko varnostnega ogrožanja, ne da bi se s tem oslabilo varovanje področja kjer koli drugje (AD 70-1, 1997:19).

Nadzor je odzivna in preprečevalna dejavnost (Golob, 1997: 85).

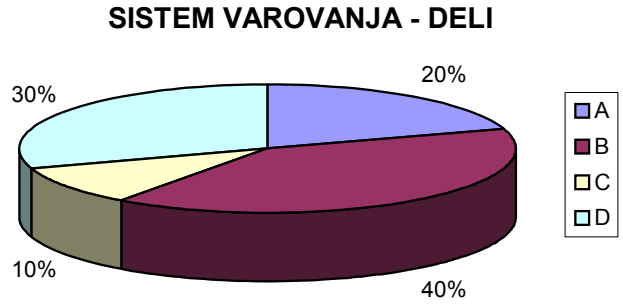
3 VAROVANJE TAJNIH PODATKOV V REPUBLIKI SLOVENIJI IN V NATU

3.1 SISTEMSKA UREDITEV TEHNIČNEGA VAROVANJA

Sistem varovanja je skupek ukrepov in dejavnosti, ki jih izvajajo pooblaščene osebe z namenom preprečevanja kaznivih dejanj. Varovanje lahko izvajajo le usposobljeni posamezniki ali skupine. Pri izvajanju varovanja uporabljamo tehnična sredstva, ki samostojno ne morejo opravljati nečesa, kar lahko počne le človek, torej ne varujejo, ampak jih je človek izdelal z namenom, da mu olajšajo preprečevanje, nadzorovanje, odkrivanje in javljanje ter omogočajo lažje in učinkovitejše obvladovanje storilcev kaznivih dejanj.

Optimalno varnost lahko zagotovi samo kombinacija mehanskega varovanja, elektronskega nadzora in javljanja, varnostno taktičnih ukrepov (prepovedi prehodov, dostopa, prostega gibanja) in človeškega vira – osebnega varovanja.

Slika 3.1: Deleži celovitega sistema varovanja



Vir: International Security Review, št. 110 1999.

Legenda:

- A: elektronski nadzor in javljanje (videonadzor, alarmne naprave, senzorji, javljalniki),

- B: mehanska zaščita (ograje, rešetke, rolete, protivlomne folije, ključavnice, protivlomna vrata itd.),
- C: človeški vir – osebno varovanje (straža, varnostniki, hitrost interventnih sil) in
- D: varnostni postopki (nadzor vstopa, omejitve gibanja).

Varnostni dejavniki so v grafu prikazani glede na njihovo pomembnost. Posplošen model ne predstavlja deležev glede na vrsto varovanega objekta, njegovo velikost, pomembnost ipd., ampak deleže iz splošnih ugotovitev za lažje predstavljanje celotnega sistema varovanja. Iz grafa je vseeno razvidno, da so najpomembnejši varnostni postopki.

Stoodstotno in popolno varovanje je nedosegljivo, zato tudi ni mogoče zagotoviti popolne varnosti ustanov, vojašnic, podjetij itd. S kombinacijo mehanske zaščite, elektronskega nadzora in javljanja, človeškega vira in taktičnih varnostnih postopkov pa se lahko zagotovi optimalna raven zaščite.

3.1.1 Sistemska ureditev tehničnega varovanja v Natu

Mandat Severnoatlantskega sveta AD 70-1 opredeljuje osnovne principe in minimalne standarde varnosti, ki jih uveljavlja Natovo združeno poveljstvo v Evropi (ACE). O principih in minimalnih standardih varnosti so se dogovorile države članice. To so varnostni standardi, ki omogočajo ustrezno zavarovano izmenjavo tajnih podatkov (Čaleta, 2004: 63). Pri tem pa so vzpostavljeni ustrezni fizični ukrepi, s katerimi se prepreči nepooblaščen dostop do stopnjevanih informacij zveze Nato. Ti ukrepi temeljijo na principu varnostnih območij. Princip varnostnih območij zahteva nadzorovan sistem, ki je vzpostavljen tako, da upošteva posebnosti stalno zaposlenega osebja, pogodbenih izvajalcev in obiskovalcev (AD 70-1, 1997: 4).

Učinkovit nadzor vstopov v varnostno območje zahteva uvedbo uporabe varnostnih kartic, od straže oziroma varnostnega osebja pa, da zagotovi celovitost varnostnih območij. Zato je varnostno osebje/straža ustrezno usposobljeno, varnostno preverjeno in učinkovito nadzorovano (AD 70-1, 1997: 4).

Vse stopnjevane informacije zveze Nato so shranjene v ustreznih odobrenih varnostnih vsebnikih. Ključi in kombinacije morajo biti varovani z ukrepi, ki so predpisani za določeno raven tajnosti.

Vsaka formacija ACE mora zagotoviti ukrepe za zaščito stopnjevanih dokumentov pred nepooblaščenim vpogledom. Dokumenti pa se morajo varovati tudi v času dela z njimi.

3.1.1.1 Varnostna območja

Temeljni kamen pri izvajanju fizične varnosti predstavlja dejstvo, da je treba stopnjevane informacije stopnje Confidential/zaupno in višje ustrezno obdelovati in hraniti v varnostnih območjih, za katere ima zveza Nato izdelane posebne kriterije (Faganel, Anžič, 2006: 3).

Administrativno območje (Administrative Zone) je območje, v katerem se obdelujejo in hranijo podatki nižjih stopenj kot v varnostnem območju I. in II. stopnje. Maksimalna stopnja tajnosti podatkov, ki jih obdelujejo in hranijo v tem območju, je Restricted/interno. Administrativno območje mora biti vidno označeno in določeno. Če je le mogoče, se mora izvajati nadzor nad vstopom in izstopom oseb in vozil. Vzpostavitev teh območij ni obvezna, lahko pa bistveno pripomore k izboljšanju ravni varovanja v formacijah ACE (Čaleta, 2004: 70).

Varnostno območje II. stopnje (Nato Class II. Security Area) je območje, v katerem se Natove informacije s stopnjo Confidential/zaupno ter višje shranjujejo in obdelujejo tako, da jih je mogoče z internim nadzorom zavarovati pred dostopom nepooblaščenih oseb. Sam vstop v varnostno območje ne pomeni neposrednega dostopa do tajnih podatkov. Samo območje pa zahteva dodatne ukrepe za preprečevanje vstopa v varnostno območje, in sicer:

- ustrezno varovan vhod, skozi katerega vsi vstopajo in izstopajo pod nadzorom;
- sistem vstopne kontrole, ki dopušča vstop samo tistim osebam, ki so varnostno preverjene in imajo ustrezna pooblastila za vstop. Vsem drugim posameznikom pa je treba na podlagi ustreznih varnostnih postopkov dodeliti določeno spremstvo ali pa so potrebni drugi ukrepi, ki bodo preprečili nenadzorovan vstop v prostore in nepooblaščen dostop do tajnih podatkov (AD 70-1, 1997: 16).

Varnostno območje I. stopnje (Nato Class I. Security Area) je območje, v katerem se Natove informacije stopnje Confidential/zaupno in višje shranjujejo in obdelujejo tako, da že vstop v varnostno območje I. stopnje pomeni možnost dostopa do tajnih podatkov. Varnostno območje se lahko vzpostavi pod naslednjimi pogoji:

- ustrezno varovan vhod, skozi katerega vsi vstopajo in izstopajo pod nadzorom;
- sistem vstopne kontrole, ki dopušča vstop samo osebam, ki so varnostno preverjene in posebno pooblaščene za vstop v to območje;

– natančno določene stopnje in kategorije tajnosti informacij, ki se obdelujejo in hranijo v tem prostoru (AD 70-1, 1997: 15, 16).

Za vstop v varnostno območje I. stopnje se osebi izda posebno dovoljenje. Izda ga predstojnik organa ali organizacije, v kateri je varnostno območje, oziroma oseba, ki jo predstojnik organa ali organizacije za to pisno pooblasti.

3.1.1.2 Kontrola vstopov v varnostna območja in izstopov iz njih

Vstopi v varnostno območje I. in II. stopnje morajo biti nadzorovani:

– s sistemom identifikacijskih kartic in
– s sistemom osebne prepoznave/identifikacije.

Kontrola vstopov in izstopov vsebuje vse elemente prožnosti in prilagodljivosti za izvajanje vsakodnevnih operativnih zahtev.

Kriteriji vstopa v varnostna območja in izstopa iz njih so naslednji:

– vse stalno osebje mora biti ustrezno varnostno preverjeno za ustrezno stopnjo tajnosti, vsaj do stopnje tajno;
– obiskovalci z ustreznim varnostnim potrdilom lahko pridobijo začasno dovoljenje za gibanje brez spremstva;
– obiskovalci brez ustreznega varnostnega potrdila ne smejo vstopati v varnostno območje, razen v izrednih primerih. Pred vstopom pa se morajo izvesti vsi ukrepi, ki bodo preprečili nepooblaščen dostop do tajnih podatkov;
– pogodbeno osebje (vključno z vzdrževalci in čistilci) je treba varnostno preveriti na ustrezno raven varnostnega preverjanja ali pa jih je treba spremljati ves čas zadrževanja v varnostnem območju.

Sistem identifikacijskih kartic, ki omogoča vstop v varnostna območja I. in II. stopnje, je treba podpreti z avtomatsko registracijo. Avtomatska registracija je samo dopolnilo in nikakor ni popolna zamenjava za varnostno/stražarsko službo.

Dostop v varnostna območja je lahko usmerjan in nadzorovan s stražarskega mesta, ki z delovanjem usposobljenega in ustreznega varnostnika/stražarja zagotavlja naslednje:

– vrata ali ograja z vgrajenim sistemom za avtomatski vstop morajo zagotavljati preprečitev fizičnega dostopa v območje. Polovična zapora ni sprejemljiva;
– varnostno osebje/straža izvaja nadzor z videonadzornim sistemom in ima ustrezno komunikacijsko povezavo s točko vstopa;
– varnostno osebje/straža mora imeti možnost, da zavrne avtomatski dostop osebe v prostor, čeprav ima ta ustrezno programirano identifikacijsko kartico;

– sistem registracije je lahko nadgrajen z ustrezno osebno identifikacijsko številko (Faganel, Anžič, 2006: 5).

Izvajanje pozitivnega nadzora in sistem kontrole vstopov morata zagotavljati preprečevanje nepooblaščenih dostopov in olajšati dostopanje pooblaščenih oseb skozi kontrolne točke v varnostna območja. To se lahko izvede z uporabo sistema osebne prepoznave, vendar pa je učinkovitejša uporaba sistema identifikacijskih kartic. Zapisi na identifikacijskih karticah morajo biti ustrezno nadzorovani. Identifikacijske kartice morajo imeti naslednje lastnosti:

- oštevilčene so s serijsko številko,
- imeti morajo identifikacijske značilnosti imetnika (podpis in slika),
- biti morajo ustrezne oblike in se morajo uporabljati samo v določeni organizaciji, z njih pa se ne sme razbrati identifikacija organizacije,
- z njih mora biti mogoče razbrati, v katera območja in do katere stopnje imajo osebe dostop,
- pri gibanju zunaj varnostnih območij, jih je treba hraniti zunaj vidnega dosega nepooblaščenih oseb.

Skupni sistem identifikacijskih kartic je dopusten samo za združena poveljstva oziroma skupne organe.

3.1.1.3 Tehnično varovanje tajnih podatkov

S sistemom tehničnega varovanja v poveljstvih in enotah Nata se varujejo osebe, premoženje in tajni podatki. Varovanje se izvaja s fizičnim varovanjem, z uporabo tehničnih sredstev ali kombinirano.

Varovanje je sestavljeno iz vseh dejavnosti, ukrepov in postopkov, ki jih opravljajo vojaške osebe. Njihova naloga je, da sebe, drugo osebo ali premoženje ščitijo pred uničenjem, poškodovanjem, odtujitvijo oziroma pred izvedbo drugega kaznivega dejanja.

Pri izvajanju varovanja uporabljajo vojaške osebe pridobljena znanja, psihofizične sposobnosti, dokumentacijo (zakonska pooblastila, pravilnike, hišne rede, načrte …), živali (največkrat pse) in tehnična sredstva (sredstva protivlomnih sistemov, sistemov videonadzora, kontrole vstopa in identifikacije, sredstva za samodejno odkrivanje in javljanje nepooblaščene prisotnosti ali požara, protipožarna sredstva, komunikacijska sredstva, prevozna sredstva in specialno opremo za pripadnike interventnih sil).

Sistemi tehničnega varovanja v poveljstvih in enotah Nata morajo dosegati minimalne zahteve po varnostni direktivi AD 70-1. Obstoječe sisteme, ki ne dosegajo teh standardov,

je treba spremeniti oziroma dograditi. Uvajanje novih sistemov mora biti v skladu z omenjeno direktivo in akti, ki urejajo to področje (AD 70-1, 1997: 117-120).

Kvaliteten sistem tehničnega varovanja je mogoče zagotoviti le z ustrezno integracijo vseh funkcionalnih področij in njihovih tehničnih sredstev, kar pa zahteva načrtovanje celotne sheme tehničnega varovanja pred njegovo izvedbo na varovanem objektu.

Tehnična sredstva se uporabljajo kot pripomoček varnostnemu osebju za zmanjšanje odvisnosti varovanja s človeškim virom. Uporaba tehničnih sredstev pa omogoča:

- da je pri varovanju večjih kompleksov lahko število varnostnega osebja manjše,
- da ima varnostno osebje dodaten pregled nad stanjem varovanega objekta iz varnostno nadzornega centra,
- da se zmanjša število obhodov po objektu in
- da je reakcija varnostnega osebja ob alarmnih stanjih bistveno hitrejša.

Pomembna razloga za uporabo tehničnih sredstev v sistemih tehničnega varovanja sta tudi odvračanje in preprečevanje oziroma onemogočanje dostopa morebitnim storilcem do varovanih območij.

Od tehničnih sredstev se za učinkovito varovanje tajnih podatkov in materialov uporabljajo mehanska zaščita, sistemi za nadzor gibanja, alarmni sistemi in sistemi videonadzora.

Sredstva mehanske zaščite oziroma protivlomni sistemi se uporabljajo pri varovanju prostorov vojaške infrastrukture in predstavljajo prve ovire za vstop v nadzorovana območja. Namenjena so za opozarjanje na varovana območja ali prostore in preprečujejo vstop nepooblaščenim osebam.

Najznačilnejši sistem varovanja objektov je varovalna ograja; ta mora ustrezati določenim standardom.

Ograja okoli območja je iz kovinske mreže. Dimenzije mreže so 50 x 50 mm, mreža pa je povezana z žico premera 3 mm. Mrežni del ograje je visok vsaj 2,15 metra in dopolnjen z nadgradnjo. Nadgradnja je lahko iz kolutov bodeče žice ali iz trikrakih štrlečih kovinskih palic, ki so med sabo povezane z bodečo žico, ali iz najmanj treh vrst bodeče žice ali jeklenih palic. Jeklene palice se na zunaj in navznoter raztezajo pod kotom 45 stopinj. Povezovalna žica mora biti galvanizirana ali oblečena v plastično prevleko. Tudi bodeča žica mora biti galvanizirana oziroma kemično obdelana. Kemična obdelava žice preprečuje korozijo. Napenjalna žica je nameščena na vrhu, v sredini in na spodnjem delu ograje. Odprtina pod ograjo ne sme biti višja kot 50 mm. Ograja je na spodnjem delu sidrana z meter dolgimi jeklenimi palicami (razdalja med njimi je najmanj en meter), ki

preprečujejo, da se ograja lahko privzdigne. Če je zemljišče pod ograjo mehko, je nanj treba položiti pas betona ali asfalta. Stebri ograje so iz betona ali materiala, ki je odporen proti koroziji. Vrata ograje so izdelana na podlagi istih standardov kot ograja, podlaga pod vrati pa je asfaltirana. Ograja je postavljena na očiščenem zemljišču (brez grmovja in dreves). Očiščeno zemljišče mora zagotoviti ustrezen vizualni nadzor nad ograjo. Če je le mogoče, je treba zagotoviti 25-metrski očiščen pas na obeh straneh ograje (AD 70-1, 1997: 28).

Kovinske rešetke na oknih in vratih varnostnih območij morajo zagotavljati ustrezno varovanje. Kvaliteta se doseže z izbiro pravega jekla, ki ga z običajnimi rezili ni mogoče rezati, hkrati pa je še vedno dovolj žilavo, da ne poči pri močnem udarjanju ali zvijanju. Kjer že zid zgradbe predstavlja ustrezno oviro, morajo biti vsa okna in druge odprtine, strehe, police, odtočne cevi, ki so 5,5 metra nad nenadzorovanim zemljiščem, ustrezno varovane s kovinskimi rešetkami, vgrajenimi v jekleni okvir. Okenski okvir se varuje na notranji strani ali na strani odpiranja. Rešetke so debele 25 mm (minimalno 20 mm) in postavljene na razdaljo 150 mm od centra. Dopolnjene so lahko s horizontalnimi prečkami dimenzije 45 x 6 mm na razdalji 200 mm (maksimalno 500 mm) (AD 70-1, 1997: 28).

Protivlomna varovalna vrata so sestavljena iz okrepljenih oziroma varjenih tečajev, elementov proti dvigovanju (stranski zatiči), jeklenih okvirjev, širokokotnega kukala, protivlomne ključavnice ter jeklenih in izolacijskih plošč v jedru vrat. Preprečevati morajo nepooblaščen vstop v objekt oziroma prostor. Vrata morajo biti odporna proti udarcem, raztezanju, lomljenju in dvigovanju, prav tako pa morajo zagotavljati preprečevanje širjenja požara. Odpirati se morajo v prostor (AD 70-1, 1997: 28).

Zapahi, zasuni in verižice so nameščeni na notranji strani vrat ali oken in onemogočajo dvigovanje in nasilno lomljenje vrat.

Protivlomne folije preprečujejo lomljenje steklenih površin, ki se sicer ob udarcih razbijejo, vendar pa zaradi lepljenja na folijo ne razpadejo. Protivlomne folije se uporabljajo predvsem na oknih in vratih, kjer se hranijo tajni dokumenti in pomembna tehnična sredstva.

Ključavnice so množičen element protivlomnega sistema (AD 70-1, 1997: 20 in 21).

Protivlomne omare, trezorji in blagajne – njihovo skupno ime je vsebniki – sodijo med protivlomna sredstva, ki se uporabljajo predvsem za shranjevanje tajnih dokumentov in osebnega orožja.

Če se v varnostni omari hranijo podatki različnih stopenj tajnosti, mora varnostna omara ustrezati najvišji stopnji tajnosti podatkov, ki se hranijo v njej. Z najvišjo stopnjo tajnosti omaro vidno označimo (nalepka) na zunanji prednji strani omare.

Trdne sobe so protivlomno odporne sobe z zidovi iz kvadrov, betona, opeke ali druge močne konstrukcije z odpornostjo, ki je enakovredna 150 mm betona ali betonskih blokov oziroma drugih materialov enakovredne odpornosti (AD 70-1, 1997: 20).

Sistemi za nadzor gibanja opozarjajo, odkrivajo in javljajo nepooblaščeno prisotnost in spadajo med preventivne varnostne sisteme, ki omogočajo nadzor nad zaposlenimi, zunanjimi in drugimi osebami, ki stopajo v varovana območja. Sestavljeni so iz sistema za identifikacijo oziroma prepoznavanje in sistema pristopne kontrole (Faganel, Anžič, 2006: 9).

Med alarmne sisteme se uvrščajo naprave, ki omogočajo nadzorovanje dogajanja v varovanem prostoru oziroma odkrivajo spremembe in posredujejo sprožene signale na vnaprej določene lokacije (varnostno nadzorni center).

Alarmni sistemi so sestavljeni iz javljalnikov in sredstev za prenos alarmnih in drugih signalov. Delovanje alarmnih sistemov temelji izključno na odkrivanju sprememb energij na varovanih točkah ali v varovanih prostorih (AD 70-1, 1997: 19).

Nato uporablja za varovanje svojih objektov dve skupini alarmnih sistemov:

- sisteme za odkrivanje in javljanje nepooblaščene prisotnosti in
- sisteme za odkrivanje in javljanje požara.

Sistemi za odkrivanje in javljanje nepooblaščene prisotnosti so sistemi, ki se največkrat namestijo v prostore ali na objekte. V kombinaciji s protivlomnimi sistemi (nameščanje senzorjev v elemente protivlomnih sistemov ali na te elemente) predstavljajo učinkovito zaščito prostora in objektov.

Zaradi velike požarne ogroženosti nekaterih objektov so sistemi za odkrivanje in javljanje požara množično sredstvo v uporabi poveljstev in enot Nata. Sisteme samodejnega odkrivanja in javljanja požarov sestavljajo avtomatski in ročni javljalniki ter sredstva za komunikacijo ali prenos sproženih alarmnih signalov do ustreznega varnostno nadzornega centra.

Sistem videonadzora predstavlja funkcijsko povezana specialna tehnična sredstva, ki s sprejemanjem, prenašanjem, obdelavami, arhiviranjem in prikazi sprejetih slik omogočajo vizualno opazovanje in nadzor ter poznejše analiziranje dogajanj v varovanih prostorih.

V poveljstvih in enotah Nata uporabljajo sisteme videonadzora za nadzorovanje prostorov v objektih in njihovi neposredni okolici. Prav tako se uporabljajo sistemi videonadzora v kombinaciji s protivlomnimi sistemi.

Kombinirana uporaba omogoča preverjanje sprejetih alarmnih signalov in določanje mikrolokacije mesta, kjer se je sprožil signal. Na ta način se izjemno poveča možnost interventnega posredovanja.

Videosredstva se uporabljajo tudi kot dodatni varnostni elementi (videodomofon) za varovanje vstopanja v posamezna varnostna območja in nadzor nad njim.

Sistemi videonadzora so sestavljeni iz:

- naprav za izvajanje neposrednega nadzora (kamere, specialni objektivi, sistemi za premikanje kamer, ohišja, navadni in infrardeči reflektorji, grelci),
- sredstev za prenos signalov iz kamer do varnostno nadzornega centra,
- sredstev za prikazovanje sprejetih ali arhiviranih videosignalov z delilniki slik ter
- naprav za arhiviranje oziroma shranjevanje videosignalov.

3.1.1.4 Fizično varovanje tajnih podatkov

V državah, kjer nacionalna zakonodaja omogoča fizično varovanje tajnih podatkov, je treba izvajati redne nadzore varnostnega območja, in sicer tako znotraj kot tudi zunaj tega območja. Nadzori se izvajajo zaradi nepooblaščenega odnašanja/vnašanja tajnih podatkov in drugih nedovoljenih sredstev.

Varnostno osebje/straža mora zagotoviti verodostojnost in varnost varnostnih območij in tajnih podatkov zveze Nato.

Za varnostno osebje/stražo se zahteva, da je ustrezno varnostno preverjeno, usposobljeno in nadzorovano:

- v sklopu varnostnih nalog straža izvaja dolžnosti, kot so kontrola vstopa, straženje na stacionarnih stražarskih mestih, izvajanje obhodov, odzivanje na alarmna stanja in incidente. Z varnostnim osebjem/stražo se izvaja osnovno in nadaljevalno usposabljanje, ki zagotavlja, da so vsi pripadniki seznanjeni z vsemi vidiki svojih dolžnosti. Varnostno osebje/straža je varnostno preverjeno najmanj do stopnje tajnosti Confidential/zaupno;
- kjer je treba izvesti oboroženo varovanje, je zelo pomembno, da je varnostno osebje/straža ustrezno usposobljeno in opremljeno z natančnimi navodili o uporabi orožja;

– v varnostnih območjih I. in II. stopnje je treba zunaj delovnega časa izvajati ustrezne obhode, ki bodo zagotovili ustrezno varovanje vseh varnostnih območjih pred kompromitiranjem, poškodovanjem in izgubo tajnih podatkov. Pogostost obhodov je odvisna od lokalnih razmer, vendar pa je treba upoštevati navodilo, da se obhodi izvajajo pogosteje kot na vsaki dve uri (Faganel, Anžič, 2006: 6).

3.1.1.5 Odločitev o vzpostavitvi varnostnega območja

Odločitev o stopnji varnostnega območja v poveljstvih in enotah Nata se sprejme na podlagi stopenj tajnosti tajnih podatkov, s katerimi poveljstvo ali enota upravlja ali bo upravljala, ter na podlagi načina delovanja varnostnega območja.

Če bo varnostno območje delovalo na način, da tajni podatki niso vidni že ob vstopu vanj, bo poveljstvo ali enota vzpostavilo varnostno območje II. stopnje. Če bo vpogled v tajne podatke mogoč že z vstopom v varnostno območje, bo poveljstvo ali enota vzpostavilo varnostno območje I. stopnje.

Oseba, ki bo vstopila v varnostno območje, mora biti o tem nedvoumno in jasno obveščena, še preden vstopi v to območje. Obvestilo mora vsebovati dobro vidne napise: »naziv poveljstva ali enote – VARNOSTNO OBMOČJE I. oziroma II. STOPNJE«. Napisu so lahko dodana še druga obvestila, povezana z varnostnimi postopki in ukrepi, ki se izvajajo v varnostnem območju.

Za označitev administrativnega območja ni potrebno posebno obvestilo, ampak zadošča, da je območje oziroma stavba ali okoliš, v katerem je območje, označeno s tablami o imenu poveljstva ali enote ter obvestilom o nadzoru.

Pri odločitvi o velikosti varnostnega območja je treba vedeti, ali bodo v varnostnem območju tudi prostori za delo zaposlenih (večji prostor z ustreznimi dodatnimi prostori, kjer se bodo tajni podatki tudi obdelovali), ali bo območje namenjeno le za hranjenje in evidentiranje tajnih podatkov. Pomembno pri odločitvi o velikosti območja je tudi, ali bodo območje uporabljali zunanji uporabniki. V tem primeru je treba za varnostno območje določiti še dodatni prostor in spremembo režima dela v samem varnostnem območju.

Pri načrtovanju velikosti varnostnega območja je treba upoštevati tudi podatek o vrstah tajnih podatkov. Vedeti je treba, ali se bodo v varnostnem območju obravnavali samo podatki na papirju ali bodo v območju tudi podatki na elektronskih medijih.

Osebe, ki delajo v varnostnem območju, morajo zagotavljati, da bo vsaka oseba, ki vstopa v varnostno območje, imela ustrezno stopnjo dostopa do tajnih podatkov. Osebe, ki

delajo v varnostnem območju, morajo osebi omogočiti vpogled samo v tiste tajne podatke, do katerih ima odobren dostop.

Po zbranih osnovnih podatkih za vzpostavitev varnostnega območja se izdela osnutek načrta varnostnega območja.

3.1.2 Sistemska ureditev tehničnega varovanja v Republiki Sloveniji

V Sloveniji je sistemsko tehnično varovanje tajnih podatkov določeno z Zakonom o tajnih podatkih (Uradni list RS, št. 87/2001, 135/2003 in 28/2006) (v nadaljnjem besedilu: ZTP). V zakonu so določene skupne osnove enotnega sistema določanja, varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov Slovenije, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države.

Po tem zakonu se morajo ravnati državni organi, organi lokalnih skupnosti, nosilci javnih pooblastil ter drugi organi, ki razpolagajo s tajnimi podatki. Skladno z njim morajo ravnati tudi dobavitelji, izvajalci gradenj ali izvajalci storitev (čistilni servisi in podobni).

Vsakdo, komur je bil zaupan tajni podatek, ali vsakdo, kdor se je seznanil z vsebino tajnega podatka, je odgovoren za njegovo varovanje in ohranitev njegove tajnosti (ZTP, 2001, 2003 in 2006: 1. člen).

V zakonu so razloženi določeni termini:

- *tajni podatek* je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno-varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v zakonu, zavarovati pred nepoklicanimi osebami in ki je z zakonom določen kot tajen;
- *dostop* je seznanitev osebe s tajnim podatkom ali zmožnost osebe pridobiti tajni podatek na podlagi dovoljenja za dostop do tajnih podatkov;
- *varnostno preverjanje osebe* je poizvedba, ki jo je pred izdajo dovoljenja za dostop do tajnih podatkov opravil pristojni organ in katere namen je zbrati podatke o morebitnih varnostnih zadržkih;
- *varnostni zadržki* so ugotovitve varnostnega preverjanja, iz katerih izhaja, da obstajajo dvomi o zanesljivosti in lojalnosti osebe, ki naj bi dobila dovoljenje za dostop do tajnih podatkov;

– *ogrožanje vitalnih interesov države* je ogrožanje njene ustavne ureditve, neodvisnosti, ozemeljske celovitosti in obrambne sposobnosti (ZTP, 2001: 2. člen).

Zakon določa, da lahko brez dovoljenja za dostop do tajnih podatkov dostopajo predsednik republike, predsednik vlade, poslanec, državni svetnik, župan in občinski svetnik, minister in predstojnik vladne službe, ki je neposredno odgovoren predsedniku vlade, varuh človekovih pravic in njegov namestnik, guverner, namestnik in viceguverner centralne banke, član računskega sodišča, sodnik, generalni državni tožilec in generalni državni pravobranilec (ZTP, 2001: 3. člen). Zakon v 4. členu dovoljuje dostop do tajnih podatkov brez dovoljenja tudi Komisiji Državnega zbora Republike Slovenije za nadzor nad delom varnostnih in obveščevalnih služb.

Z zakonom je urejena izdaja dovoljenja za dostop do tajnih podatkov. Izdaja dovoljenja je bila dopolnjena in spremenjena v ZTP leta 2003. V letu 2003 je zakon pri preverjanju oseb za dostop do tajnih podatkov ločil preverjanje glede na stopnjo tajnosti dokumenta. Tako je določil: osnovno varnostno preverjanje, razširjeno varnostno preverjanje in razširjeno varnostno preverjanje s poizvedovanjem.

Z ZTP 2001 so bile spremenjene tudi stopnje tajnosti, in sicer:

– podatki z oznako državna tajnost ali državna skrivnost v strogo tajno,
– podatki z oznako uradna tajnost ali uradna skrivnost ali vojaška skrivnost – strogo zaupno v tajno,
– podatki z oznako uradna tajnost ali uradna skrivnost ali vojaška skrivnost – zaupno v zaupno,
– podatki z oznako uradna tajnost ali uradna skrivnost ali vojaška skrivnost – interno v interno.

3.1.2.1 Varnostna območja

Zakon o tajnih podatkih iz leta 2001 ter njegova sprememba in dopolnitev iz leta 2003 nista konkretno določila varnostnega območja. Varnostno območje se je prvič uredilo in določilo v letu 2002, in sicer z Uredbo o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov (Uradni list RS, št. 70/2002).

V uredbi so standardi za vzpostavitev varnostnega območja zelo skopi. V 8. členu uredba določa tri stopnje varnostnega območja, in sicer:

- varnostno območje III. stopnje, kjer se obdelujejo in hranijo tajni podatki stopnje interno,
- varnostno območje II. stopnje, kjer se obdelujejo in hranijo tajni podatki stopnje zaupno, in
- varnostno območje I. stopnje, kjer se obdelujejo in hranijo tajni podatki stopnje tajno in strogo tajno (praviloma v ločenih prostorih).

Konkretni standardi so bili sprejeti šele z Uredbo o varovanju tajnih podatkov leta 2005 (Uradni. list RS, št. 74/2005). Standardi za vzpostavitev varnostnega območja so postali strožji in konkretni. Z uredbo v letu 2005 pa je prišlo tudi do spremembe poimenovanja stopenj varnostnih območij. Tako se je varnostno območje III. stopnje preimenovalo v upravno varnostno območje. Uredba (2005) je določila, da se lahko v varnostnem območju II. stopnje zaradi poostrenih standardov pod določenimi pogoji hranijo tudi dokumenti s stopnjo tajnosti tajno.

3.1.2.2 Kontrola vstopov v varnostna območja in izstopov iz njih

Vsi vstopi v varnostna območja in izstopi iz njih potekajo pod nadzorom. Obiskovalci in druge osebe lahko vstopajo v varnostna območja in izstopajo iz njih samo pod nadzorom zaposlenih oseb v varnostnem območju.

Vsak vstop v varnostna območja II. in I. stopnje in izstop iz njih se evidentira v posebno knjigo vstopov in izstopov, ki jo vodi odgovorna oseba varnostnega območja.

ZTP iz leta 2003 je določal, da se v varnostno območje I. stopnje vstopa skozi varnostno točko, kjer se preveri, ali ima oseba dovoljenje in upravičen razlog za vstop v območje. V varnostni točki se zagotovi, da oseba v območje ne vnese nobenih mehanskih ali elektronskih naprav, s katerimi bi lahko odtujila tajni podatek. Vstop v varnostno območje in izstop iz njega se evidentirata. Leta 2006 je sprememba ZTP odpravila varnostno točko.

3.1.2.3 Tehnično varovanje tajnih podatkov

Tehnično varovanje varnostnih območij je bilo do leta 2005 urejeno zelo skopo. Predvidevalo je le videonadzor vhoda in protiprisluškovalni pregled varnostnega območja I. stopnje. Za hranjenje tajnih podatkov so bile določene omare in blagajne. Blagajne za varovanje tajnih podatkov s stopnjo tajnosti tajno in strogo tajno so morale imeti elektronsko ključavnico in protivlomni sistem javljanja. Blagajna za shranjevanje dokumentov s stopnjo tajnosti strogo tajno pa je imela dodatno nameščen protitrgalni senzor.

3.1.2.4 Fizično varovanje tajnih podatkov

Fizično varovanje tajnih podatkov je bilo do leta 2006 zagotovljeno s stalno dežurno ali stražarsko službo. Način varovanja je predpisan v Pravilih službe v Slovenski vojski ter v izvedbenih dokumentih poveljstev in enot Slovenske vojske.

3.1.2.5 Odločitev o vzpostavitvi varnostnega območja

Odločitev o vzpostavitvi varnostnega območja sprejme odgovorni predstojnik organa. Za vzpostavitev varnostnega območja morajo biti izpolnjeni določeni pogoji. ZTP iz leta 2001 je določal postopke in ukrepe, ki so potrebni, da se lahko vzpostavi določeno varnostno območje; ti so morali obsegati:

- splošne varnostne ukrepe,
- varovanje oseb, ki imajo dostop do tajnih podatkov,
- varovanje prostorov,
- varovanje dokumentov in medijev, ki vsebujejo tajne podatke,
- varovanje komunikacij, po katerih se prenašajo tajni podatki,
- način označevanja stopenj tajnosti,
- varovanje opreme, s katero se obravnavajo tajni podatki,
- način seznanitve uporabnikov z ukrepi in postopki varovanja tajnih podatkov,
- kontrolo in evidentiranje dostopov do tajnih podatkov ter
- kontrolo in evidentiranje pošiljatelja in distributerja tajnih podatkov (ZTP, 2001: 38. člen).

Po zbranih osnovnih podatkih za postavitev varnostnega območja vsak organ izdela načrt varovanja. V načrtu varovanja se upoštevajo najnujnejši standardi, ki so določeni z Uredbo o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov (Uradni list RS, št. 70/2002). V načrtu se podrobneje predpišejo fizični, organizacijski in tehnični ukrepi ter postopki za varovanje tajnih podatkov, glede na stopnjo tajnosti in oceno ogroženosti.

Standardi so bili dopolnjeni s sprejetjem uredbe v letu 2005 in spremembo ZTP v letu 2006.

3.2 ORGANI IN SLUŽBE ZA ZAGOTAVLJANJE VARNOSTI TAJNIH PODATKOV NA OBRAMBNEM PODROČJU V REPUBLIKI SLOVENIJI

Odgovornost za varovanje objektov ministrstva je relativno razpršena in se lahko deli na odgovornost uporabnikov oziroma organizacijskih enot, ki uporabljajo posamezne objekte in območja, ter na strokovno odgovornost posameznih organizacijskih enot. Odgovornost izhaja iz nalog, ki jih določen organ opravlja, bodisi na podlagi predpisov oziroma internih aktov ministrstva bodisi na podlagi odgovornosti drugih organov in organizacij zunaj ministrstva. Kot strokovni nosilci nalog s področja varovanja so na podlagi 32. člena Zakona o obrambi (v nadaljevanju ZoO) določeni Obveščevalno-varnostna služba[1] in štabnovarnostni organi Slovenske vojske (Balant in Čaleta, 2006: 2). Naloga Obveščevalno-varnostne službe je, da predlaga dokument, s katerim bo enotno urejeno področje fizičnega in tehničnega varovanja objektov, ki so posebnega pomena za obrambo.

Comment [AK1]: ???

3.2.1 Razmejitev pristojnosti na področju varovanja

V Generalštabu Slovenske vojske (v nadaljnjem besedilu: GŠSV) je nosilec načrtovanja in organiziranja tehničnega in fizičnega varovanja objektov vojaške infrastrukture Sektor za obveščevalno-varnostne zadeve (v nadaljnjem besedilu: J-2).

J-2 izdaja smernice in izhodišča za načrtovanje in razvoj tehničnega in fizičnega varovanja objektov vojaške infrastrukture za Slovensko vojsko ter nadzira delo podrejenih poveljstev in enot na področju tehničnega in fizičnega varovanja.

J-2 opredeli skupine objektov Slovenske vojske, ki se fizično in tehnično varujejo, in varnostna območja, ki so potrebna na posameznem objektu. J-2 vodi komisijo za tehnično in fizično varovanje v Slovenski vojski ter v sodelovanju z drugimi službami načrtuje in nadzira izgradnjo novih sistemov tehničnega varovanja (izgradnja se načrtuje v srednjeročnem programu opremljanja).

Poleg tega ima J-2 še naslednje naloge:

- sodeluje pri prevzemu sistemov tehničnega varovanja v operativno delovanje,
- sodeluje s Policijo pri varovanju (posredno varovanje) objektov vojaške infrastrukture,

[1] Obveščevalno-varnostne službe so stare kot civilizacija, prvi je o njih pisal Su Cun Vu v petem stoletju pred našim štetjem (The new encyclopaedia Britannica, 1992).

- zbira podatke o realizaciji opravljenih del, zagotavljanja servisnih storitev oziroma pogodbenih obveznosti ter o nepravilnostih obvešča pristojne službe,
- enkrat letno izvede ogled objektov vojaške infrastrukture in preveri stanje na področju tehničnega in fizičnega varovanja ter
- izvaja nadzor.

Zaradi zagotavljanja celovitega varovanja morajo organi J-2 sodelovati s strokovnimi organi v ministrstvu, in sicer:

- na področju uporabe računalniške oziroma informacijske opreme,
- na področju uporabe telekomunikacijskih sredstev (radijskih zvez, telefonije, mobilne telefonije),
- pri nastajanju ocene sistema varovanja,
- z varnostnim častnikom, ki je neposredno zadolžen za varovanje GŠSV in
- s podregistrom Nata za hranjenje tajnih podatkov na GŠSV.

Varnostni oddelek Poveljstva sil Slovenske vojske (v nadaljnjem besedilu: G-2) v sodelovanju z Logističnim sektorjem Poveljstva sil (v nadaljnjem besedilu: G-4) načrtuje, določa in oblikuje zahteve po uporabi in vzdrževanju sistemov tehničnega varovanja ter določa prioritete, vodi evidence sistemov tehničnega varovanja ter načrtuje in nadzira vzdrževanje sistemov tehničnega varovanja. G-2 je v sodelovanju z G-4 odgovoren za investicijsko in tekoče vzdrževanje tehničnih sistemov.

Poleg tega ima G-2 še naslednje naloge:

- sodeluje pri prevzemu sistemov tehničnega varovanja v operativno delovanje,
- sodeluje pri izdelavi ocene ogroženosti ter sistemov tehničnega in fizičnega varovanja,
- vzpostavi stik s Policijo zaradi možnosti zunanjega (posrednega) varovanja objektov vojaške infrastrukture,
- z vojaško zdravstveno enoto preučuje možnosti za uvedbo vojaških službenih psov v sistem varovanja ter
- organizira usposabljanja za uporabo tehničnih sredstev v sistemih varovanja.

Zaradi zagotavljanja celovitega varovanja organi G-2 sodelujejo s strokovnimi organi:

- na področju uporabe računalniške oziroma informacijske opreme,
- na področju uporabe telekomunikacijskih sredstev (radijskih zvez, telefonije, mobilne telefonije),
- z Operativnim sektorjem Poveljstva sil pri izbiri vrste tehničnega in fizičnega varovanja,

- s pogodbenimi strankami pri postavitvi, delovanju in servisiranju tehničnega varovanja in
- s podregistrom Nata za hranjenje tajnih podatkov na Poveljstvu sil.

Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje (v nadaljnjem besedilu: PDRIU) izdeluje študije za elemente varovanja po naročilu J-2.

Varnostni organi v poveljstvih in enotah Slovenske vojske na podlagi zahtev in odobrenih načrtov nadzorujejo nemoteno delovanje sistemov varovanja. V sodelovanju z logističnimi organi zagotavljajo vzdrževanje tehničnih sistemov.

Na vseh stopnjah poveljevanja od ravni bataljona naprej je organ logistike v poveljstvu ali štabu strokovno odgovoren za načrtovanje vzdrževanja sistemov tehničnega varovanja.

Upravljanje s sistemi tehničnega varovanja znotraj posameznega vojaškega objekta (v miru) je v pristojnosti poveljnika oziroma upravnika objekta.

V izrednem ali vojnem stanju, ko določena poveljstva in enote zapustijo vojaške objekte, prevzamejo upravljanje s sistemi tehničnega in fizičnega varovanja poveljniki vojaško teritorialnih poveljstev.

Pri upravljanju s sistemom tehničnega in fizičnega varovanja se smiselno uporabljajo določila 14., 20., 29., 30., 55. in 57. člena ZoO ter od 253. do 346. točke Pravil službe v Slovenski vojski.

3.2.2 Svetovanje in podpora

3.2.2.1 Svetovanje

Za vsak objekt ali območje posebnega pomena za obrambo je treba v načrtu varovanja določiti osebo, ki bo odgovorna za izdelavo načrta. Na višji ravni je treba določiti organizacijsko enoto, ki nudi potrebno pomoč pri načrtovanju in izvajanju postopkov ter ukrepov varovanja. Za vse organizacijske enote ministrstva, razen Slovenske vojske, izvaja te naloge Obveščevalno-varnostna služba, za enote in zavode Slovenske vojske pa jih izvaja J-2 v sodelovanju z Obveščevalno-varnostno službo.

Inšpekcijski nadzor na obrambnem področju izvaja Inšpektorat Republike Slovenije za obrambo (IRSO). Notranji nadzor varovanja vojaških objektov in okolišev pa izvaja Slovenska vojska v skladu z akti o vodenju in poveljevanju.

3.2.2.2 Podpora

Pristojni organi v ministrstvu oziroma v Slovenski vojski nudijo podporo za vzpostavljanje varnostnih območij. Podporo izvajajo z rednim spremljanjem, poročanjem o stanju tehničnega varovanja in predlogi za izboljšanje stanja varovanja.

V ministrstvu oziroma Slovenski vojski se za poročanje uporabljata obrazca TV-1 in TV-2.

Obrazec TV-1 (priloga C) je poročilo o okvari sistemov tehničnega varovanja. Izpolnijo ga upravniki tehničnih sistemov in ga dostavijo nadrejenemu takoj po nastanku okvare. Nastalo okvaro javijo servisni službi, ki ima podpisano pogodbo z ministrstvom za vzdrževanje tehničnih sistemov.

Obrazec TV-2 (priloga D) je mesečno poročilo o delovanju sistemov tehničnega varovanja za pretekli mesec v tekočem letu. Poveljstva in enote ga dostavljajo svojemu prvonadrejenemu kot prilogo dopisa ali funkcijskega mesečnega poročila.

3.3 PRIMERJALNE UGOTOVITVE

Po vstopu Republike Slovenije v zvezo Nato je bilo treba spremeniti in dopolniti veljavno zakonodajo na področju varovanja tajnih podatkov. Komuniciranje z organi Nata ter prenos in shranjevanje tajnih podatkov Nata so zahtevali dopolnitev Zakona o varovanju tajnih podatkov in spremembo Uredbe o varovanju tajnih podatkov ter spremembo drugih predpisov, ki urejajo varovanje tajnih podatkov.

Po uveljavitvi omenjenih dopolnitev in sprememb zakonodaje je bilo treba spremeniti urejenost varnostnih območij. Varnostna območja je bilo treba posodobiti in opremiti skladno z ratificiranimi direktivami Nata. Posodobitev in izgradnja sta terjali določena finančna sredstva, ki pa pri takih posegih niso majhna, saj je varnostna oprema precej draga. Na objektih, kjer ni bilo mogoče zagotoviti predpisane gradbene ureditve, je bilo treba kupiti boljšo – dražjo opremo.

Na tem področju je veliko dela opravila Obveščevalno-varnostna služba Ministrstva za obrambo ter drugi organi in ustanove, ki se ukvarjajo z nacionalno varnostjo. Predvsem je bilo treba preučiti Natove direktive, jih prevesti in skladno z njimi predlagati spremembe zakonskih predpisov na področju varovanja tajnih podatkov v Republiki Sloveniji. Zato je bilo nujno treba spremeniti način razmišljanja in način varovanja tajnih podatkov, predvsem pa enakomerno porazdeliti naloge med odgovorne službe in organe. Z

varovanjem tajnih podatkov se je do leta 2004 predvsem ukvarjala Obveščevalno-varnostna služba. Naenkrat pa je bilo teh nalog za eno službo preveč, zato so se morale naloge skladno z nacionalno zakonodajo porazdeliti tudi na druge službe in organe, ki se ukvarjajo z varnostnoprotiobveščevalno dejavnostjo na obrambnem področju Republike Slovenije. S tem sta bila zagotovljena večja preglednost nalog in učinkovitejši nadzor nad varovanjem tajnih podatkov.

4 TEHNIČNO VAROVANJE

4.1 TEHNIČNA VARNOST TAJNIH PODATKOV IN OBJEKTOV

Vsi objekti, zgradbe, pisarne, sobe in druga območja, kjer se hranijo in/ali obdelujejo nacionalni tajni podatki ter Natovi tajni podatki in materiali, morajo biti zaščiteni z ustreznimi ukrepi za tehnično in fizično varovanje.

Organ ali organizacija si mora pred izdajo sklepa o določitvi varnostnega območja pridobiti mnenje državnega varnostnega organa o ustreznosti varnostno tehnične opreme, vgrajene v varnostno območje, ter postopkov in ukrepov varovanja varnostnega območja (UVTP, 2005: 12. in 17. člen).

Pri vzpostavitvi varnostnega območja se morajo upoštevati naslednji dejavniki:

- stopnja tajnosti in kategorija podatkov,
- količina in oblika hranjenja podatkov (podatki, shranjeni na papirju ali na informacijskih medijih),
- dovoljenje za dostop do podatkov in potreba po seznanitvi z vsebino podatkov zaposlenih,
- ocene ogroženosti s strani varnostnoobveščevalnih služb in
- način hranjenja podatkov (ZTP, 2006: 38. člen).

Na obrambnem področju Republike Slovenije imajo tehnična sredstva v sistemu varovanja tajnih podatkov naslednjo vlogo:

- preprečiti morajo nedovoljen ali nasilen vstop nepooblaščenih oseb,
- odvračati, ovirati in zaznati morajo kakršna koli dejanja nelojalnega osebja,
- ločevati morajo osebje pri dostopu do tajnih podatkov v skladu z načelom potrebe po seznanitvi z vsebino tajnih podatkov ter
- čim hitreje zaznati vsako varnostno kršitev in nato čim hitreje ukrepati.

Mesta, kjer se obdelujejo in hranijo tajni podatki, morajo biti ustrezno fizično in tehnično varovana. Fizično varovanje izvajajo enote oziroma moštva za varovanje objektov/straža. Vsi objekti, kjer se obdelujejo in hranijo tajni podatki, morajo imeti vse leto zagotovljeno neprekinjeno 24-urno tehnično varovanje .

Varnostna območja I. in II. stopnje, kjer se obdelujejo in hranijo tajni podatki, morajo biti tehnično varovana (UVTP, 2005: 10. člen).

Varnostno tehnična oprema varnostnih območij mora ustrezati pogojem, ki jih na predlog nacionalnega varnostnega organa določi Vlada Republike Slovenije (UVTP, 2005: 18. člen).

Območja oziroma prostori morajo onemogočiti nenadzorovan vstop skozi vrata, okna, klet ali streho. Območja oziroma prostore mora nadzorovati moštvo za varovanje/straža. Za tehnično varovanje se uporabljajo naslednji sistemi oziroma njihove kombinacije:

- sistem za samodejno odkrivanje in javljanje gibanja – kombinirani mikrovalovni in infrardeči pasivni javljalniki gibanja,
- sistem za samodejno odkrivanje in javljanje požara – nastavljivi avtomatski javljalniki požara,
- sistem za avtomatsko gašenje požara,
- informacijski sistem za kontrolo vstopa,
- sistem televizije zaprtega kroga,
- protivlomni sistemi in
- videodomofon (UVTP, 2005: 10. člen).

4.1.1 Varnostna območja

Tajni podatki stopnje tajnosti zaupno ali višje stopnje se lahko obravnavajo in hranijo samo v določenem, vidno označenem prostoru (v nadaljnjem besedilu: varnostno območje), ki je glede na način obravnavanja tajnih podatkov uvrščen v varnostno območje I. ali II. stopnje.

Tajni podatki stopnje interno se lahko obravnavajo tudi v upravnem območju.

Varnostna območja morajo biti organizirana in opremljena tako, da ustrezajo standardom, ki so določeni v zakonu, uredbi o tajnih podatkih in sklepu o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja.

Varnostno območje I. stopnje je označen prostor, v katerem se lahko obdelujejo tajni podatki stopnje zaupno ali višje stopnje tajnosti tako, da že sam vstop v varnostno območje pomeni dostop do tajnih podatkov. V varnostnem območju I. stopnje se izvajajo najmanj naslednji varnostni postopki in ukrepi:

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

- vodenje razvida tajnih podatkov, s katerimi se oseba seznani že ob samem vstopu v varnostno območje;
- prepoved vnosa kakršnih koli mehanskih, elektronskih in optičnih sestavnih delov, s katerimi bi bilo mogoče nepooblaščeno posneti, odnesti ali prenesti tajne podatke;
- neposredno in neprekinjeno fizično varovanje varnostnega območja, ki se lahko na podlagi ocene ogroženosti dopolni ali nadomesti z elektronskim sistemom za protivlomno varovanje varnostnega območja, katerega alarmni signal je vezan na enoto, odgovorno za ukrepanje ob alarmu. Reakcijski čas interventnih sil mora biti krajši od sedmih minut;
- ob nadomestitvi fizičnega varovanja s sistemom tehničnega varovanja mora ta sistem zagotavljati celovit nadzor varnostnega območja, ki mora biti nadzorovano iz varnostno nadzornega centra, sistem pa mora imeti zagotovljeno rezervno napajanje;
- po končanem delovnem času se pregledajo prostori (UVTP, 2005: 10. člen, drugi odstavek).

Varnostno območje II. stopnje je označen prostor, v katerem se tajni podatki stopnje zaupno ali višje stopnje obravnavajo tako, da sam vstop v to območje in gibanje v njem še ne omogočata dostopa do teh podatkov. V varnostnem območju II. stopnje se izvajajo najmanj naslednji varnostni postopki in ukrepi:

- sistem vhodnega nadzora dovoljuje vstop v to območje samo osebam, ki imajo dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti in morajo v območje vstopiti zaradi opravljanja delovnih nalog;
- vzpostavljena mora biti taka organizacija dela, ki bo zagotavljala, da bodo imele osebe, ki delajo v varnostnem območju, dostop le do tistih tajnih podatkov, ki jih potrebujejo za opravljanje delovnih nalog, in sicer do tiste stopnje tajnosti, za katero imajo dovoljenje;
- sistem za nadzor gibanja zagotavlja, da druge osebe vstopajo v varnostno območje samo v spremstvu osebe, ki je zaposlena v varnostnem območju, ali ob izvajanju druge enakovredne oblike nadzora, ki zagotavlja, da bo oseba vstopila samo v dele območja, povezane z namenom obiska, in se bo, če je to potrebno, seznanila le s tistimi tajnimi podatki, ki so povezani z namenom obiska, in sicer do tiste stopnje tajnosti, za katero ima dovoljenje;

- vnos kakršnih koli mehanskih, elektronskih in optičnih sestavnih delov, s katerimi bi bilo mogoče tajne podatke nepooblaščeno posneti, odnesti ali prenesti, je dovoljen, vendar mora biti vsa oprema izključena. Vsakokratno uporabo te opreme odobri oseba, odgovorna za varnost varnostnega območja;
- po končanem delovnem času se varnostno območje varuje s sistemom fizičnega ali protivlomnega varovanja oziroma z občasnimi fizičnimi pregledi prostorov, določenimi v načrtu varovanja (UVTP, 2005: 10. člen, tretji odstavek).

Okoli varnostnega območja I. ali II. stopnje ali na poti, ki vodi v tako varnostno območje, se lahko vzpostavi upravno območje. Za upravno območje je potreben vidno določen obseg prostora, v katerem lahko organ nadzira vstopanje v ta prostor in izstopanje iz njega oziroma gibanje oseb in vozil v njem. V upravnih območjih se lahko shranjujejo in obdelujejo samo tajni podatki stopnje interno. Z varnostnimi postopki in ukrepi pa se mora zagotavljati, da imajo dostop do teh podatkov samo osebe, ki so s pisno izjavo potrdile, da so seznanjene s predpisi, ki urejajo obravnavanje tajnih podatkov, in se morajo s temi podatki seznaniti zaradi opravljanja delovnih nalog (UVTP, 2005: 10. člen, četrti odstavek).

Osebe javnega ali zasebnega sektorja lahko za namene varovanja premoženja, življenja ali telesa posameznikov ter reda v njenih prostorih od posameznika, ki namerava vstopiti v ta prostor ali izstopiti iz njega, zahtevajo, da navede vse ali nekatere osebne podatke ter razlog vstopa ali izstopa. Po potrebi lahko osebne podatke preverijo tudi z vpogledom v osebni dokument posameznika.

V evidenci vstopov in izstopov se lahko o posamezniku vodijo samo naslednji osebni podatki:

- osebno ime,
- številka in vrsta osebnega dokumenta,
- naslov stalnega ali začasnega prebivališča,
- zaposlitev,
- datum in ura vstopa ali izstopa ter
- razlog vstopa v prostor ali izstopa iz njega.

Evidenca iz prejšnjega odstavka velja za uradno evidenco in se lahko hrani največ tri leta od vpisa. Nato se podatki o osebi zbrišejo ali uničijo (ZVOP, 2004: 82. člen).

V predlogu za vzpostavitev varnostnega območja mora vodja organizacijske enote ministrstva pridobiti mnenje Obveščevalno-varnostne službe o primernosti lokacije in pogojih za vzpostavitev ustreznega varovanja.

Obveščevalno-varnostna služba v sodelovanju s strokovnimi službami ministrstva, ki so pristojne za posamezna področja varovanja tajnih podatkov (varovanje tajnih podatkov v informacijskih in komunikacijskih sistemih in drugo), opravi ogled lokacije in izda mnenje, v katerem opiše vse organizacijske, tehnične in druge posege, ki jih je treba opraviti za vzpostavitev varnostnega območja.

Mnenje iz prejšnjega odstavka vsebuje podatke o nujnih posegih in oceno predvidenih finančnih posledic. Oceno predvidenih finančnih posledic pripravi organizacijska enota ministrstva, pristojna za gospodarjenje z nepremičninami (SGN).

Po končanih delih v varnostnem območju in po uspešno opravljenem tehničnem prevzemu (gradbena dela, električne in varnostne instalacije) mora vodja organizacijske enote ministrstva, pristojne za gospodarjenje z nepremičninami, obvestiti Obveščevalno-varnostno službo, da opravi ponovni ogled varnostnega območja in zaprosi nacionalni varnostni organ za mnenje (PVTP, 2006: 21. člen).

Obveščevalno-varnostna služba na podlagi svojih ugotovitev in mnenja nacionalnega varnostnega organa predlaga ministru za obrambo, da izda sklep o določitvi varnostnega območja (PVTP, 2006: 21. člen).

4.2 SISTEMI TEHNIČNEGA VAROVANJA

Na obrambnem področju Republike Slovenije se s sistemi tehničnega varovanja (slika 4.1) varujejo osebe, premoženje Slovenske vojske in tajni podatki (ZTP, 2006: 39. člen). Varovanje se izvaja s fizičnim varovanjem, z uporabo tehničnih sredstev ali kombinirano (tehnični sistemi in fizično varovanje).

Varovanje je sestavljeno iz vseh dejavnosti, ukrepov in postopkov, ki jih opravljajo vojaške osebe, da sebe, drugo osebo ali premoženje ščitijo pred uničenjem, poškodovanjem, odtujitvijo oziroma pred izvedbo drugega kaznivega dejanja.

Pri izvajanju varovanja uporabljajo vojaške osebe pridobljena znanja, psihofizične sposobnosti, dokumentacijo, ki je na razpolago (zakonska pooblastila, pravilnike, hišne rede, načrte), živali (največkrat pse) in tehnična sredstva (sredstva protivlomnih sistemov, sistemov videonadzora, kontrole vstopa in identifikacije, sredstva za samodejno odkrivanje in javljanje nepooblaščene prisotnosti ali požara, protipožarna sredstva, komunikacijska sredstva, prevozna sredstva in specialno opremo za pripadnike interventnih sil).

Slika 4.1: Sistemi tehničnega varovanja

Vir: PSSV 2005. Vrhnika.

Sistemi tehničnega varovanja na obrambnem področju Republike Slovenije morajo ustrezati standardom zveze Nato in dosegati minimalne zahteve po varnostni direktivi AD 70-1 (ACE Security Directive). Obstoječe sisteme, ki ne dosegajo teh standardov, je treba spremeniti oziroma dograditi. Uvajanje novih sistemov mora biti v skladu s sklepom o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja (v nadaljnjem besedilu: SDPVO), in z omenjeno direktivo ter drugimi akti, ki urejajo to področje.

Kvaliteten sistem tehničnega varovanja je mogoče zagotoviti le z ustrezno integracijo vseh funkcionalnih področij in njihovih tehničnih sredstev, kar pa zahteva načrtovanje celotne sheme tehničnega varovanja pred njegovo izvedbo na varovanem objektu.

Sistemi tehničnega varovanja so na obrambnem področju Republike Slovenije že upravičili svojo uporabo. Tehnična sredstva se uporabljajo kot pripomoček varnostnemu osebju, da se zmanjša odvisnost varovanja tajnih podatkov in objektov samo s človeškim virom.

Pri varovanju večjih kompleksov s pomočjo tehničnih sistemov je lahko število varnostnega osebja manjše. S pomočjo tehničnih sistemov ima varnostno osebje iz varnostno nadzornega centra ali varnostno nadzorne točke stalen pregled nad stanjem varovanega objekta. S tem se zmanjša ali popolnoma odpravi število obhodov po objektu, reakcije varnostnega osebja ob alarmnih stanjih pa so zato hitrejše. Pomembna razloga za uporabo tehničnih sredstev v sistemih tehničnega varovanja sta tudi odvračanje in

preprečevanje oziroma onemogočanje dostopa morebitnim storilcem do varovanih območij.

Glede na posebnosti varovanja tajnih podatkov in objektov na obrambnem področju Republike Slovenije ni mogoče zagotoviti učinkovitega varovanja samo s tehničnimi sistemi ali samo s fizičnim varovanjem. Učinkovito varovanje se lahko doseže z uporabo obeh sistemov – torej kombinirano.

Za učinkovito varovanje tajnih podatkov in objektov je treba na obrambnem področju Republike Slovenije zagotavljati nenehno izobraževanje in usposabljanje vseh zaposlenih v ministrstvu, in ne samo osebja za varovanje tajnih podatkov in objektov.

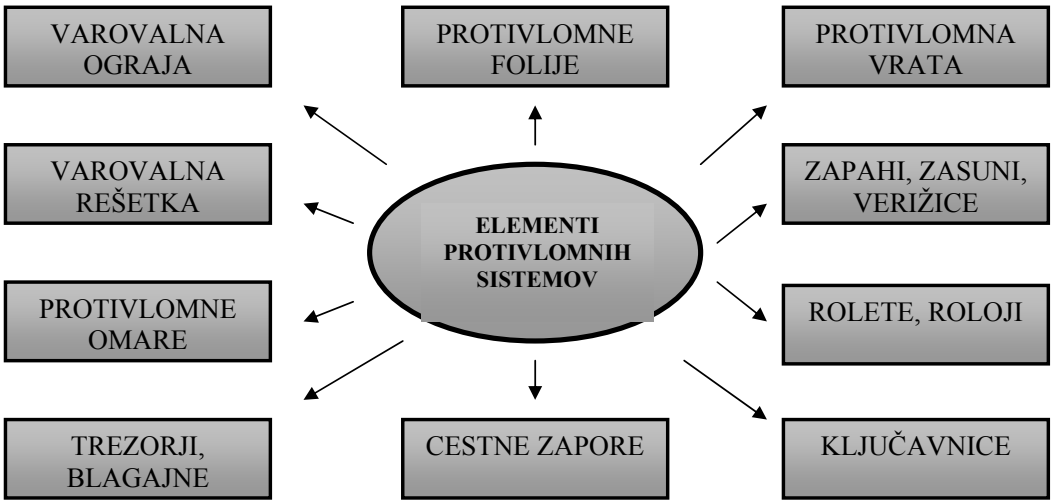
4.2.1 Protivlomni sistemi

Sredstva mehanske zaščite oziroma protivlomni sistemi (slika 4.2) se uporabljajo pri varovanju prostorov vojaške infrastrukture in predstavljajo prve ovire za vstop v nadzorovana območja. Protivlomni sistemi so namenjeni opozarjanju, da je za njimi varovani prostor, ter preprečevanju vstopa nepooblaščenim osebam.

Namen protivlomnega varovanja je:

- zvišanje stopnje varovanja,
- zagotovitev zgodnje detekcije,
- omogočanje hitrega odziva (potreben čas za intervencijo interventnih sil),
- dvig ravni varovanja življenj, opreme in nepremičnin ter
- zmanjšanje vpliva človeškega faktorja (AD 70-1, 1997: 27).

Slika 4.2: Protivlomni sistemi



Vir: GŠSV 2005. Ljubljana.

4.2.1.1 Varovalna ograja

Eden od najznačilnejših delov varovanja objektov na obrambnem področju Republike Slovenije je varovalna ograja (slika 4.3 in priloga B). Varovanje z varovalno ograjo so vsi načini varovanja zunanjega dela varovanega območja. Varovalna ograja mora zagotavljati optimalno varnost pred:

- plezanjem, raztegovanjem, upogibanjem, podiranjem, rušenjem, spodkopavanjem in preskokom ograje,
- rezanjem, sekanjem ali ščipanjem ograje in
- razstavljanjem ograje.

Varovalna ograja je koristna fizična ovira, ki določa mejo območja, za katero se zahteva varnostna zaščita. Opredeljena stopnja zaščite je zagotovljena z višino varovalne ograje, njeno konstrukcijo, uporabljenim materialom in dodatnimi varnostnimi lastnosti, kot so dodani vrhnji deli, sistemi za zaznavo vdora v območje varovanja, osvetlitev ali televizija zaprtega kroga. Ograja, ki obdaja objekte vojaške infrastrukture, mora zagotavljati učinkovito zaščito pred vstopom nepooblaščene osebe na varovano območje. Za zagotavljanje najvišje stopnje varovanja so ograje, ki varujejo objekte vojaške infrastrukture, opremljene s sistemi za zgodnje elektronsko zaznavanje vsiljivcev.

Slika 4.3: Varovalna ograja MS90103 – Acroni

Vir: PSSV 2006. Vrhnika.

Tako opremljene ograje morajo zagotoviti:

- 24-urno zaznavanje in odkrivanje vsiljivcev vse leto,
- zaznavanje posameznih vsiljivcev ali skupine, še preden vdrejo v varovano območje, ki je obdano z varovalno ograjo,
- najvišjo stopnjo zaznavanja vsiljivcev pri rezanju ali dvigovanju ograje ali plezanju čez njo,
- najnižjo stopnjo sprožanja lažnih alarmov,
- ustvarjanje fizičnega in psihološkega odvračanja morebitnih vlomilcev,
- kontrolo pretoka vozil, oseb in tovora,
- zagotovitev časa za intervencijo moštev za varovanje,
- dolgo življenjsko dobo,
- nizke stroške vzdrževanja in
- druge dodatne zahteve, ki so potrebne za učinkovito varovanje objektov.

Poleg navedenih zahtev, ki določajo kvaliteto ograje, morajo ograje, ki varujejo objekte na obrambnem področju Republike Slovenije, minimalno izpolnjevati naslednje tehnične zahteve:

- skupna višina ograje naj ne bo nižja od 3 metrov,
- ograja brez dodatnih elementov mora biti visoka najmanj 2,15 metra in
- na obeh straneh ograje mora biti zagotovljen najmanj 5-metrski očiščeni pas/varnostni pas (če je le mogoče, 25-metrski).

Poleg tega so priporočene še naslednje zahteve:

- dimenzija temeljev za ograjo mora biti 150 x 150 x 800 mm, za nosilne stebre pa 400 x 400 x 800 mm,

- trdnost materiala mora vzdržati silo 1200 N/mm^2,
- vsi kovinski elementi ograje morajo biti zaščiteni proti rjavenju,
- dodatni elementi (nadgradnja varovalne ograje) – ostrivci morajo biti premera 450 do 1000 mm.

Varovalna ograja se lahko dopolni z:

- dodatno (dvojno) ograjo,
- nadzorom s pomočjo televizije zaprtega kroga,
- varnostno razsvetljavo in
- uporabo službenih psov.

Učinkovitost vsakega varnostnega območja je v veliki meri odvisna od stopnje varovanja na njegovih vstopnih točkah. Zato morajo biti vsa vrata v ograji zgrajena v skladu z istim varnostnim standardom kot ograja. Vstopi in izstopi skozi vrata v ograji pa morajo biti nadzorovani; v nasprotnem primeru je delovanje ograje v smislu varovanja ničnо.

Glede na izbiro ustreznega tipa varovalne ograje (slika 4.4) in vgrajenih senzorjev v njene elemente mora ograja ustrezati naslednjim zahtevam:

- ne glede na izbiro ponudnika mora sistem omogočati povezljivost in združljivost z že obstoječimi sistemi,
- izbrani sistem mora omogočiti povezanost v varnostno nadzorni center ali varnostno nadzorno točko,
- izbrani sistem mora biti v skladu s smernicami za izvajanje varovanja območij, objektov ministrstva ter standardi zveze Nato, ki so določeni v direktivi AD 70-1,
- sistem mora omogočati izklop posameznih območij (vhodna vrata).

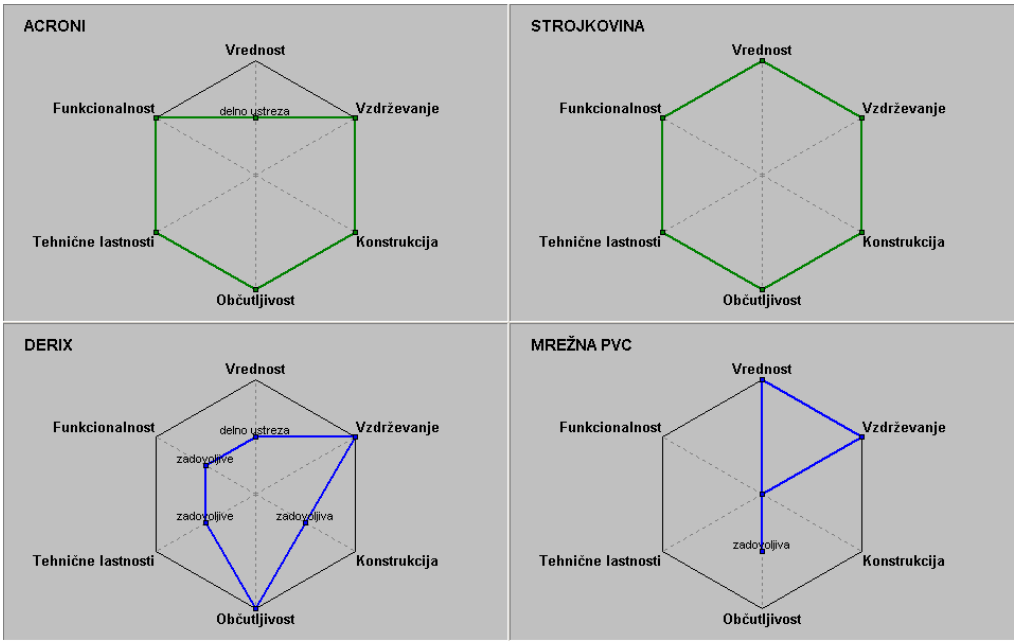
Za varovanje objektov ministrstva, ki se ne nahajajo na urbanih območjih in kjer ima teren večje naklone, se mora postaviti varovalna ograja, ki konstrukcijsko omogoča postavitev na zahtevnih terenih (priloga B). Za varovanje objektov ministrstva v urbanih naseljih pa so primerne varnostne ograje, ki poleg funkcionalnosti ne motijo videza okolice.

Objekti I. in II. skupine se morajo varovati z varovalno ograjo, ki ima v svoji konstrukciji vgrajene senzorje in omogočajo elektronski nadzor varovalne ograje. Vgrajeni senzorji so odvisni od vrste varovalne ograje in morajo izpolnjevati vse zahteve, ki jih postavijo uporabniki. Senzorji morajo biti preizkušeni in atestirani v Sloveniji.

Nasilni vdori v varovana območja se lahko preprečijo tudi s posebno ureditvijo prostora, in sicer:

- z nasipi in trdnimi ograjami okoli varovanega območja,
- z zavoji vozišča, ki omejujejo hitrost dostopa vozil do varovanega območja,
- s trdnimi zapornicami,
- z ovirami na vozišču, ki omejujejo hitrost dostopa vozil do varovanega območja (asfaltne ali betonske grbine),
- z ovirami okoli varovanega območja, ki preprečujejo parkiranje vozil, in
- z bojnim delovanjem oklepnih vozil (tank, bojno vozilo pehote, bojno oklepno vozilo) – v vojni – na vstopnih točkah v varovano območje.

Slika 4.4: Grafični prikaz lastnosti različnih varovalnih ograj



Vir: Poveljniško štabna šola 2007. Poljče.

Grafični prikaz lastnosti različnih varovalnih ograj je nastal na podlagi primerjalne in kvalitativne analize s pomočjo programske opreme DEX-i.

Kriteriji, ki sem jih uporabljal pri izbiri varovalne ograje, so bili: tehnične lastnosti, funkcionalnost, vzdrževanje in vrednost varovalne ograje. Pri izračunu je bila najpomembnejša funkcionalnost varovalne ograje z 32 odstotki, sledile so ji tehnične

lastnosti s 25 odstotki, vzdrževanje z 32 odstotki in vrednost varovalne ograje s 7 odstotki. Pri analizi sem upošteval tudi vrednost izdelka in servisne ure popravila varovalne ograje. Cena varovalne ograje Acroni in vrednost servisne ure (popravilo varovalne ograje po deformaciji) je neprimerno višja kot cena in servisne ure varovalne ograje, ki jo izdeluje in trži Stojkovina. Acronijeva varovalna ograja je kljub ceni primerna za varovanje skladišč streliva in minskoeksplozivnih sredstev zunaj urbanih okolij. Za vse druge objekte in skladišča, ki so v urbanih okoljih, pa je primerna varovalna ograja Strojkovina. Najmanj primerna varovalna ograja za varovanje objektov je varovalna ograja iz plastificirane aluminijaste mreže, ki se uporablja za ograjevanje vrtov in avtocest. Ta varovalna ograja je le neznatna ovira, ki jo je mogoče premagati v zelo kratkem času. Varovalni ograji Strojkovine in Derixa pa sta si podobni. Razlike so v tehnični izvedbi in funkcionalnosti varovalne ograje. Varovalne ogreje so bile leta 2004 praktično testirane na Poveljstvu sil Slovenske vojske.

Podrobnejši opis zahtev pri izbiri najprimernejše varovalne ograje v Ministrstvu za obrambo je zapisan v Poročilu o izbiri varovalne ograje v Ministrstvu za obrambo Republike Slovenije (priloga H).

4.2.1.2 Varovalna rešetka

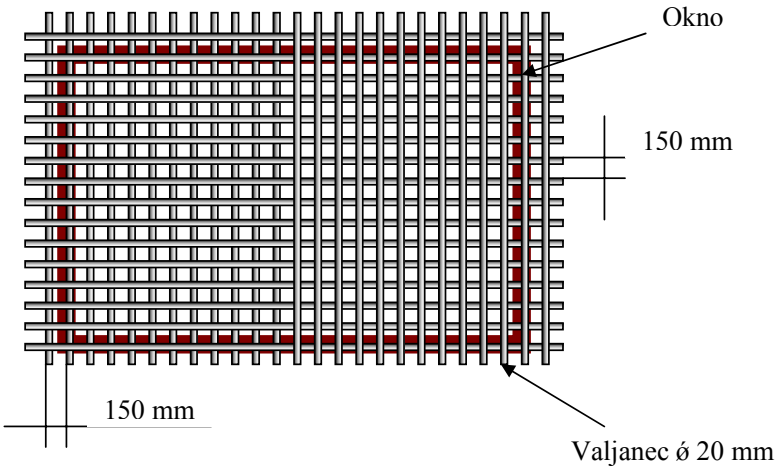
Varovalne (kovinske) rešetke (slika 4.5) na oknih in vratih zagotavljajo ustrezno varovanje. Varovalne rešetke morajo biti ustrezne kvalitete; to dosežemo z izbiro pravega jekla, ki ga z običajnimi rezili ni mogoče rezati, hkrati pa je še vedno dovolj žilavo, da ne poči pri močnem udarjanju ali zvijanju.

Zaradi pravočasne zaznave poskusov rezanja s posebnimi žagami se lahko rešetke dodatno elektronsko varujejo (SDPVO, 2006: 7. člen).

Rešetke se morajo obvezno namestiti na vsa okna varnostnega območja I. stopnje, kjer je višina oken nižja od 5,5 metra nad nenadzorovanimi tlemi.

Rešetke in zaščitne mreže predstavljajo tehnična sredstva protivlomnega sistema, s katerimi se preprečuje vstop v objekte skozi okno.

Slika 4.5: Varovalna rešetka



Vir: Poveljniško štabna šola 2006. Poljče.

4.2.1.3 Protivlomna vrata

Protivlomna varnostna vrata[2] so sestavljena iz okrepljenih oziroma varjenih tečajev,[3] elementov proti dvigovanju (stranski zatiči), jeklenih okvirjev, širokokotnega kukala, protivlomne ključavnice ter jeklenih in izolacijskih plošč v jedru vrat. Zagotavljati morajo varnost proti nepooblaščenem vstopu v objekt oziroma prostor. Protivlomna vrata morajo biti odporna proti udarcem, raztezanju, lomljenju in dvigovanju, prav tako pa morajo zagotavljati preprečevanje širjenja požara. Vrata se morajo odpirati v prostor.

Protivlomna vrata na objektih vojaške infrastrukture morajo preprečevati nasilen vstop z razbijanjem ali odklepanjem. Postavljena morajo biti tako, da je mogoča vizualna komunikacija med osebjem za varovanje in objektom oziroma vhodom, ki ga varujejo.

V ministrstvu se uporabljajo protivlomna (protipožarna) varnostna vrata predvsem na vhodih v posamezna varnostna območja.

Vhodna vrata v varnostna območja I. in II. stopnje morajo biti izdelana iz trdega lesa ali kovine in ne smejo biti poškodovana, tako se lahko takoj opazi poskus nasilnega vstopa v prostor. Lesena vrata morajo biti debela najmanj 40 mm oziroma 2 mm, če so iz pločevine. Tečaji so nameščeni v notranjosti varovanega prostora ter so narezani ali valoviti, tako da preprečijo nepooblaščeno snemanje vrat. Okvir vrat in njegov zapah morata biti čvrsta tako kot sama vrata. Zid, v katerega so vgrajena vrata, vključno s pregrado nad vrati, ne sme biti

[2] Protivlomna vrata morajo preprečiti fizični vstop v prostor tudi skozi krilo.
[3] Protivlomna vrata morajo imeti vsaj tritočkovno zapiranje in morajo ustrezati standardu SIST EN 1627 stopnje 4 (SDPVO: 3. člen) ali stopnje 2 (SDPVO: 21. člen).

bistveno šibkejši, kot so sama vrata. Nobeno steklo, razen ojačanega stekla, ki je tovarniško vgrajeno, se ne sme uporabljati pri varnostnih vratih. Vhodna vrata v varnostno območje II. stopnje morajo biti opremljena z ustrezno varnostno ključavnico. Vrata, ki vodijo v varnostno območje I. stopnje, pa morajo biti opremljena z varnostno kombinacijsko ključavnico, ki jo določajo sprejeti standardi (priloga F). Varnostna kombinacijska ključavnica mora omogočati menjavo kombinacij. Med vrati in ključavnico na okvirju vrat mora biti vgrajena ustrezna odporna kovinska plošča.

4.2.1.4 Zapah, zasun in varnostna verižica

Zapahi, zasuni in verižice so nameščeni na notranji strani vrat ali oken in onemogočajo dvigovanje in nasilno lomljenje. V ministrstvu uporabljajo omenjene elemente predvsem v varovanih prostorih.

4.2.1.5 Protivlomna folija

Protivlomne folije preprečujejo lomljenje steklenih površin, ki se ob udarcih sicer razbijejo, vendar pa zaradi lepljenja na folijo ne razpadejo. Protivlomne folije se v ministrstvu uporabljajo predvsem na oknih in vratih, kjer se hranijo tajni dokumenti stopnje tajno in više ter pomembna tehnična sredstva.

4.2.1.6 Varnostna ključavnica

Ključavnice[4] so množičen element protivlomnega sistema, ki se uporablja v ministrstvu. Ustrezati morajo standardom, ki jih določajo veljavni zakonski predpisi v Sloveniji (priloga F).

Zaradi uporabe različnih vrst ključavnic je treba urediti njihovo uporabo v ministrstvu, in sicer:

- uporaba posameznih ključev (posebej tistih, ki odklepajo ključavnice na vratih pomembnih prostorov, pisarn in skladišč) mora biti natančno določena s posebnim aktom ali v okviru skupnega dokumenta varovanja,
- v primeru izgube posameznega ključa mora biti izdelano navodilo,
- v prostorih s stalno prisotnostjo se uredi sistem skupnega shranjevanja osnovnih in rezervnih ključev ter dostop do njih in
- ključavnice morajo imeti na zunanji strani protivlomni ščit.

[4] Varnostna ključavnica mora ustrezati standardu SIST EN 1301 stopnje 2 (SDPVO: 4. in 22. člen).

Posamezno nastavitev kombinacije elektronske ali mehanske ključavnice na varnostnih omarah lahko poznajo samo osebe, ki jih določi predstojnik organa. Predstojnik organa mora delovne naloge v organu razporediti tako, da je število oseb, ki so seznanjene s posameznimi kombinacijami, čim manjše.

Nastavitev kombinacije elektronske in mehanske ključavnice je treba zamenjati v naslednjih primerih:

- po namestitvi ključavnice,
- periodično vsakih šest mesecev,
- potem ko je oseba, ki pozna kombinacijo ključavnice, prenehala opravljati naloge v organu, zaradi katerih je bila seznanjena s kombinacijo ključavnice, in
- kadar tako odloči predstojnik organa.

Ključi varnostnega območja oziroma ključi prostorov iz varnostnega območja se hranijo v posebnem prostoru zunaj tega območja, tako da je nepooblaščenim osebam onemogočen dostop.

4.2.1.7 Varnostne omare, trezorji in blagajne

Protivlomne omare, trezorji in blagajne oziroma s skupnim imenom vsebniki sodijo med protivlomna sredstva, ki jih v ministrstvu uporabljajo predvsem za shranjevanje tajnih dokumentov in osebne oborožitve (SDPVO, 2006: 10. člen).

Tajni podatki stopnje tajnosti interno se hranijo v pisarniških ali kovinskih omarah.

Tajni podatki stopnje tajnosti zaupno in tajno se hranijo v varnostnih omarah, ki morajo ustrezati najmanj protivlomni stopnji II. Tajni podatki stopnje tajnosti strogo tajno se hranijo v varnostnih omarah, ki morajo ustrezati najmanj protivlomni stopnji III.

Na zunanji strani varnostne omare se glede na stopnjo tajnosti podatkov, ki se hranijo v omari, prilepi v zgornji levi kot vrat nalepka primerne velikosti z veliko tiskano črko oziroma črkama:

- »Z« za stopnjo tajnosti zaupno,
- »T« za stopnjo tajnosti tajno in
- »ST« za stopnjo tajnosti strogo tajno.

Če se v varnostni omari hranijo podatki različnih stopenj tajnosti, mora varnostna omara ustrezati najvišji stopnji tajnosti podatkov, ki se hranijo v njej. Omara se označi z najvišjo stopnjo tajnosti, ki se hrani v njej (UVTP, 2005: 19. člen).

Vsebniki morajo izpolnjevati naslednje zahteve:

- čim dalj časa morajo zadrževati storilca pri premagovanju ovire (vstop v varnostni vsebnik),
- imeti morajo certifikat, ki potrjuje njihovo prilagojenost mednarodnim standardom in usklajenost z njimi,
- imeti morajo kvaliteten zaporni in zaklopni mehanizem in
- pri izbiri se morajo upoštevati določila ZTP.

Vsi vsebniki morajo zagotavljati zaščito pred nasilnim vstopom in nepooblaščenim vstopom s poskusom notranje zlorabe. Glede na navedeno je vedno pomembno upoštevati prostor, kjer stoji varnostni vsebnik. Zunanja varnostna zaščita mora preprečiti nepooblaščen dostop in je zelo pomemben dejavnik, ki vpliva na čas, potreben za nepooblaščen dostop v vsebnik.

Varnostni vsebniki morajo izpolnjevati še naslednje kriterije:

- struktura materiala in sestavljanje vseh delov varnostnega vsebnika ter končna obdelava in toleranca proizvajalca morajo zagotavljati ustrezno zahtevano trdnost strukture in izpolnjevati določene zahteve za vsak razred varnostnega vsebnika;
- dokončno obdelan varnostni vsebnik ne sme imeti nikakršnih proizvodnih pomanjkljivosti, ki bi lahko vplivale na uporabnost in zunanjost. Kovinski deli ne smejo biti rjasti ter imeti ostružkov ali drugih nepopolnosti. Kaljeno jeklo vsebnika je odporno proti vrtanju in dovolj trdno, da predstavlja dolgotrajni odpor pri poskusu nasilnega vstopa v varnostni vsebnik. Vse zunanje in notranje površine morajo biti ustrezno obdelane in zaščitene proti rji;
- varnostni vsebniki so opremljeni z vgrajeno tristopenjsko kombinacijsko ključavnico. Sistem zapiranja mora preprečiti, da bi zaradi določene ovire vrata varnostnega vsebnika ostala odprta in nezaklenjena. Varnostni vsebnik mora omogočati mrtvi tek mehanizma za zapah, ki je povezan z varovano povezavo do ključavnice, ki se lahko zaklene samo v primeru, ko je mehanizem v ustreznem položaju, ta pa zagotavlja zaprtost vsebnika;
- proizvajalec mora izdelati vzorčne primere varnostnih vsebnikov in ključavnic, da jih kupec lahko testira. Kupec preveri tudi možnost opremljanja varnostnega vsebnika z odstranljivimi deli (police) in njihovo namestitvijo, vključno z mehanizmom za zaklepanje;
- spodnja ploskev varnostnega vsebnika mora biti enake velikosti kot vrhnja ploskev. Teža najtežjega varnostnega vsebnika ne sme preseči 11 kilogramov

na kvadratni centimeter njegove spodnje ploskve. Osnovna kapaciteta shranjevanja v varnostnem vsebniku mora omogočati shranjevanje dokumentov ali registrov osnovnih oblik v tipskih predalnikih. Alternativno shranjevanje lahko vključuje namestitev polic namesto predalnikov (AD 70-1, 1997: 20).

Trezorji morajo zadostiti enakim kriterijem kot trdne sobe. Razlika je v tem, da razen vrat ne smejo imeti nobene druge odprtine, ki presega 500 cm^2. Vsaka taka odprtina mora biti ustrezno zaščitena, da se prepreči vnos kakršnega koli trdnega materiala. Trezorska vrata morajo biti izdelana iz močnega jekla ter opremljena s kombinacijsko ključavnico, ki omogoča spreminjanje kombinacij. Poleg tega pa morajo biti v skladu s standardi, ki so jih sprejele države članice Nata za shranjevanje stopnjevanih dokumentov ali materiala izključno stopnje tajnosti strogo tajno (AD 70-1, 1997: 33).

4.2.1.8 Trdne sobe

Trdne sobe so protivlomno odporne sobe z zidovi iz kvadrov, betona, opeke ali druge močne konstrukcije z odpornostjo, ki je enakovredna 150 mm betona ali betonskih blokov oziroma kovine enakovredne odpornosti (SDPVO, 2006: 2. člen). Ti zidovi se, če je le mogoče, ne uporabljajo kot zunanji zidovi objekta. Idealno je, če se zidovi, tla in stropi ter odprtine ustrezno pregledajo. Okna so zaščitena z jeklenimi palicami debeline najmanj 20 mm, ki so vgrajene v beton na razdalji 150 mm. Če je varnostno območje oddaljeno od tal 5,5 metra, območje objekta pa ustrezno zaščiteno, da onemogoča plezanje po objektu, je treba na okna vgraditi mreže. Okna so prevlečena in zaščitena z neprosojnim materialom. Okvir vrat in vrata v trdno sobo so kovinska ali prekrita s kovino in dodatno opremljena z ustrezno kombinacijsko ključavnico, ki omogoča menjavanje kombinacij. Tečaji vrat se morajo nahajati na notranji strani vrat in so ustrezno valoviti in nazobčani, da preprečijo nepooblaščen vstop. Zadnja kovinska plošča, ki obkroža ključavnico, je ustrezno pritrjena na vrata, tako da onemogoča lahko odstranitev. Odstranljiva opozorilna tabla z napisom je pritrjena na zadnjo ploščo. Ventilacijski sistemi pa so zavarovani pred nepooblaščenim dostopom ali vnosom kakršnega koli trdnega materiala. Tla in strop so izdelani iz primerljivih materialov, tako kot stene, da preprečijo in onemogočijo vsak poskus nasilnega nepooblaščenega vstopa v prostor. Obstoječa varnost je lahko nadgrajena z uporabo alarmnega sistema, ki se sproži ob poskusu nepooblaščenega vstopa skozi zid, tla, strop in druge odprtine oziroma ob poskusu nepooblaščenega gibanja v prostoru (AD 70-1, 1997: 32).

4.2.2 Sistemi za nadzor gibanja

Sistemi za nadzor gibanja opozarjajo, odkrivajo in javljajo nepooblaščeno prisotnost in spadajo med preventivne varnostne sisteme, ki omogočajo nadzor nad zaposlenimi ter zunanjimi in drugimi osebami, ki vstopajo v varovana območja ministrstva. Sestavljeni so iz sistema za identifikacijo oziroma prepoznavanje in sistema pristopne kontrole.[5]

4.2.2.1 Identifikacija

Z identifikacijo (slika 4.6) se preverjajo geslo, oznaka in sredstvo, ki jih oseba nosi s seboj. Največkrat je to identifikacijska kartica ali biometrični zapis.

Biometrična identifikacija temelji na tehničnem prepoznavanju določenih lastnosti osebe, ki se identificira. Z obdelavo biometrične značilnosti se ugotavljajo ali primerjajo lastnosti posameznika, tako da se lahko izvede njegova identifikacija oziroma preveri njegova identiteta (ZVOP, 2004: 78. člen).

Biometrični ukrepi se lahko v javnem sektorju določijo le z zakonom, in še to le takrat, če je to nujno potrebno za varnost ljudi, premoženja, za varovanje tajnih podatkov ali poslovne skrivnosti in tega namena ni mogoče doseči z milejšimi sredstvi (ZVOP, 2004: 79. člen). Identificirajo se lahko:

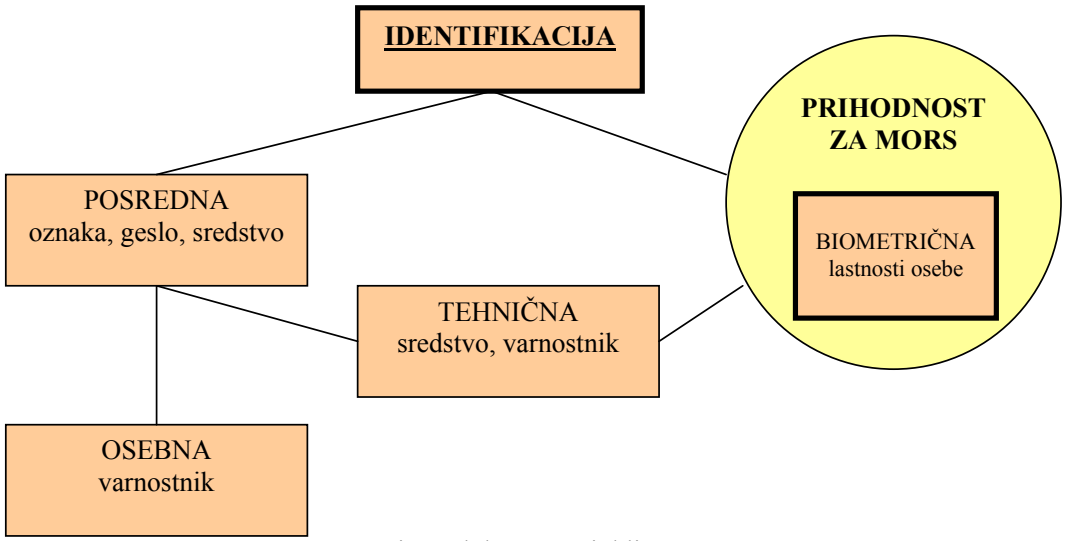
- prstni odtis,
- geometrija dlani,
- glas,
- očesna mrežnica,
- očesna zenica in
- dinamični podpisi.

Sodobni sistemi za nadzor gibanja uporabljajo računalniške baze podatkov in specialne naprave, kot so registratorji, vrtljiva vrata in križi.

V prihodnosti bo treba na obrambnem področju Republike Slovenije poleg že obstoječih sistemov za nadzor gibanja načrtovati tudi uvedbo dražjih in sodobnih biometričnih sistemov za nadzor gibanja.

[5] Pristopna kontrola mora ustrezati standardu SIST EN 50133 razreda 3 (SDPVO: 18. člen).

Slika 4.6: Vrste identifikacij



Vir: Golob 1997. Ljubljana.

4.2.2.1 Vstopna kontrola

Vstopna kontrola v varnostna območja je sestavljena iz elektronske kombinacijske ključavnice in sistema, ki deluje na principu magnetne kartice. Sistema sta v ministrstvu edina predpisana kot sistema za elektronsko kontrolo vstopa. Lahko sta vgrajena z namenom dopolnitve stražarskega varovanja pri nadzorih vstopa v prostor ali objekt. Vstope v varnostno območje in izstope iz njega nadzira operater v varnostno nadzornem centru ali varnostno nadzorni točki.

V sistemu varovanja tajnih podatkov se sistem nikakor ne sme uporabljati samostojno, ampak vedno v kombinaciji z drugimi sistemi. Vgrajen je tako, da prepreči zlorabe vstopov v varnostno območje. Obvezno se vgrajuje pred vstopom v varnostno območje I. in II. stopnje.

Registratorji, ki omogočajo vstop v varnostno območje in izstop iz njega, se namestijo na obeh straneh vhodnih vrat v varnostno območje (slika 4.7). V varnostno območje se vstopi tako, da se položi magnetna kartica na registrator, ta zazna vpisano kodo in sprosti magnet na elektronski ključavnici. Nad vrati je nameščeno samozapiralo, ki po vstopu v prostor samodejno zapre vrata, elektronsko magnetna ključavnica pa jih zaklene.

Evidenca imetnikov magnetnih kartic in dovoljenje za vstop v določene prostore se vodita v varnostno nadzornem centru ali varnostno nadzorni točki. V varnostno nadzornem centru ali varnostno nadzorni točki lahko pooblaščena oseba posamezniku začasno prepreči vstop v točno določen prostor.

Slika 4.7: Sistem kontrole vstopa Keri

Vir: http://www.vtz. 2007. V Sloveniji trži VTZ, d. o. o., Ljubljana.

4.2.3 Alarmni sistemi

Med alarmne sisteme uvrščamo naprave, ki omogočajo nadzorovanje dogajanja v varovanem prostoru oziroma odkrivajo spremembe ter posredujejo tako sprožene signale na vnaprej določene lokacije (varnostno nadzorni center, varnostno nadzorna točka).

Alarmni sistemi so sestavljeni iz javljalnikov in sredstev za prenos alarmnih in drugih signalov. Delovanje alarmnih sistemov temelji izključno na odkrivanju sprememb energij na varovanih točkah ali v varovanih prostorih (AD 70-1, 1997:19).

Ministrstvo uporablja za varovanje svojih objektov dve skupini alarmnih sistemov, in sicer:

- sistem za odkrivanje in javljanje nepooblaščene prisotnosti in
- sistem za odkrivanje in javljanje požara.

Sistemi za odkrivanje in javljanje nepooblaščene prisotnosti[6] se največkrat namestijo v prostore ali na objekte. V kombinaciji s protivlomnimi sistemi (namestitev senzorjev v elemente protivlomnih sistemov) predstavljajo učinkovito zaščito prostora in objektov.

Zaradi velike požarne ogroženosti nekaterih objektov v ministrstvu sisteme za odkrivanje in javljanje požara ministrstvo množično uporablja. Sisteme samodejnega odkrivanja in javljanja požarov sestavljajo avtomatski in ročni javljalniki ter sredstva za komunikacijo ali prenos sproženih alarmnih signalov do varnostno nadzornega centra ali varnostno nadzorne točke.

[6] Sistem za samodejno zaznavanje gibanja oseb mora ustrezati standardu SIST EN 50131 razreda 2 (SDPVO: 23. člen).

4.2.3.1 Sistem za odkrivanje in javljanje nepooblaščene prisotnosti

Sistem za odkrivanje in javljanje nepooblaščene prisotnosti ali sistem za detekcijo gibanja (slika 4.8) se namesti v prostor kot dopolnitev osnovnih varnostnih sistemov. Sistem sam po sebi ne zagotavlja varnosti, njegova učinkovitost se pokaže šele, če je vgrajen v kombinaciji z drugimi sistemi.

Sistem z različnimi senzorji zazna prisotnost nepooblaščene osebe v prostoru in jo javi v varnostno nadzorni center ali varnostno nadzorno točko; tam se natančno določi točka v prostoru oziroma pot nepooblaščenega vstopa v prostor.

Pri vstopu v varnostno območje se lahko sistem izključi, in sicer tako, da se na tipkovnico, ki se nahaja pred vhodom v prostor, odtipka kombinacija večmestnega števila. Vstop v prostor zazna računalnik, ki vodi tehnične sisteme, in opozori operaterja v varnostno nadzornem centru ali varnostno nadzorni točki, da je v prostor vstopila oseba. Operater lahko s pomočjo nadzornega sistema točno določi identiteto osebe, ki je vstopila v prostor. Sistem se običajno kombinira s sistemom vstopne kontrole.

Slika 4.8: Sistem za odkrivanje in javljanje nepooblaščene prisotnosti

Vir: http://www.vtz. 2007. V Sloveniji trži VTZ, d. o. o., Ljubljana.

4.2.3.2 Sistem za odkrivanje in javljanje požara

Sistem se uporablja v kombinaciji z drugimi sistemi, zazna pa povišano temperaturo ali povečano koncentracijo dima v prostoru. Ob zaznavi spremembe se v objektu sproži alarmni signal (sirena), ki opozarja na prisotnost dima oziroma povečano temperaturo v prostoru. Vklop alarma opazi operater v varnostno nadzornem centru ali varnostno nadzorni točki. Operater točno določi mesto nastanka požara in ukrepa skladno s predpisanimi navodili.

Učinkovitost sistema se doseže z namestitvijo senzorjev (slika 4.9) v vseh prostorih objekta; s tem se zagotovi pravočasno odkrivanje požara, ki bi lahko ogrozil varnostno območje ali arhiv, telefonsko centralo ali druge predmete, občutljive za ogenj.

Sistem se lahko dopolni s sistemom za avtomatsko gašenje požara.

Slika 4.9: Avtomatski optični dimni javljalnik požara

Vir: http://www.varnost.si 2007. V Sloveniji trži Varnost, Maribor, d. o. o.

4.2.4 Sistem videonadzora

Sistem videonadzora (SDPVO, 2006: 16. in 17. člen, PVTP, 2006: 25. člen) predstavlja funkcijsko povezana specialna tehnična sredstva, ki s sprejemanjem, prenašanjem, obdelavami, arhiviranjem in prikazi sprejetih slik omogočajo vizualno opazovanje in nadzor ter poznejše analiziranje dogajanj v varovanih prostorih.

V ministrstvu uporabljajo sistem videonadzora za nadzorovanje prostorov v objektih in njihovi neposredni okolici. Sistem videonadzora se uporablja v kombinaciji s protivlomnimi sistemi.

Kombinirana uporaba omogoča preverjanje sprejetih alarmnih signalov in določanje mikrolokacije mesta alarmiranja. Na ta način se izjemno skrajša reakcijski čas sil za interveniranje.

Videosredstva se v ministrstvu uporabljajo tudi kot dodatni varnostni elementi (videodomofon) za varovanje in nadzor vstopa v posamezna varnostna območja in izstopa iz njih.

Sistem videonadzora je sestavljen iz:

- naprav za izvajanje neposrednega nadzora (kamere, specialni objektivi, sistemi za premikanje kamer, navadni in infrardeči reflektorji),
- sredstev za prenos signalov iz kamer do varnostno nadzornega centra ali varnostno nadzorne točke (optični vodnik),

- sredstev za prikazovanje sprejetih ali arhiviranih videosignalov z delilniki slik in
- naprave za arhiviranje oziroma shranjevanje videosignalov (slika 4.10).

Pri namestitvi sistema videonadzora se morajo upoštevati določila Zakona o varstvu osebnih podatkov (Uradni list RS, št. 86/2004 in sprememba št. 113/2005).

Slika 4.10: Videokamera

Vir: http://www.varnost.si 2007. V Sloveniji trži Varnost Maribor, d. o. o.

Zakon o varstvu osebnih podatkov v 74. členu določa, da mora oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, o izvajanju nadzora objaviti obvestilo. Obvestilo je vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznani z izvajanjem videonadzora najpozneje, ko se nad njim začne izvajati nadzor. Obvestilo mora vsebovati naslednje informacije:

- da se izvaja videonadzor,
- naziv osebe javnega ali zasebnega sektorja, ki izvaja nadzor, in
- telefonsko številko za pridobitev informacij, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema.

Pri nadzoru se lahko zbirajo naslednji osebni podatki (ZVOP, 2005: 75. člen):

- posnetek posameznika (slika ali glas),
- datum in čas vstopa v prostor in izstopa iz njega,
- osebno ime posnetega posameznika,
- naslov njegovega stalnega ali začasnega bivališča,
- zaposlitev,
- številka in podatki o vrsti njegovega osebnega dokumenta in
- razlog vstopa.

Osebni podatki iz prejšnjega odstavka se lahko hranijo največ eno leto po nastanku, nato se zbrišejo, če zakon ne določa drugače.

Zakon prepoveduje nadziranje posameznika z videonadzorom v garderobah, dvigalih in sanitarnih prostorih (ZVOP, 2005: 77. člen).

Upravljavec mora poskrbeti, da je sistem videonadzora zavarovan pred dostopom nepooblaščenih oseb.

Pred vhodom v varnostno območje se videokamera namesti tako, da se ne vidijo številke na tipkovnici sistema za odkrivanje nepooblaščene prisotnosti.

4.3 PRENOS VARNOSTNIH SIGNALOV

Sredstva (SDPVO, 2006: 20. in 24. člen), ki se uporabljajo v sistemih varovanja, v trenutku spremembe stanja v varovanem prostoru sprožijo alarmni signal. Alarmni signali oziroma alarmna sporočila se prenašajo do zunanjih svetlobnih in zvočnih sredstev za alarmiranje in do varnostno nadzornega centra ali varnostno nadzorne točke.

Alarmne signale oziroma sporočila se v ministrstvu prenašajo na več načinov:

- po radijskih zvezah,
- po obstoječem javnem telekomunikacijskem telefonskem ali mobilnem omrežju,
- po funkcionalnih sistemih zvez in
- po notranjih kabelskih sistemih.

Varnostno nadzorni center je poseben operativni prostor, v katerem varnostniki operaterji upravljajo in nadzirajo tehnične sisteme za varovanje. V varnostno nadzornih centrih trajno in kontinuirano spremljajo dinamiko dogajanj na varovanih območjih. Na monitorjih nadzornih naprav (slika 4.11) zaznavajo nepooblaščene prisotnosti v varnostnih območjih, drugih prostorih in okolici, ki so pod tehničnim nadzorom. V nadzorno varnostnih centrih se razrešujejo izredni dogodki in odzivanja na alarmne situacije.

Za vzpostavitev varnostno nadzornega centra mora vsak zavezanec, ki je dolžan organizirati službo varovanja, pridobiti licenco v skladu z zakonom, ki ureja varovanje.

V ministrstvu imajo poleg varnostno nadzornih centrov še varnostno nadzorne točke. Varnostno nadzorno točko ima skupina objektov, ki je tehnično varovana. V varnostno nadzorni točki se spremlja dinamika dogajanja v varnostnih območjih in okolici 24 ur na dan vse leto.

Slika 4.11: Nadzorna naprava

Vir: http://www.vtz. 2007. V Sloveniji trži VTZ, d. o. o., Ljubljana.

4.4 RAZSVETLJAVA OBJEKTOV IN PROSTOROV

Da se lahko gibljemo ter opravljamo predvidene dejavnosti z lahkoto, varno in učinkovito, je nujno, da pridobivamo informacije iz okolice.

Največ informacij pridobimo z vidom, zato je zelo pomembno, da imamo v delovnem okolju dovolj in predvsem dobro vidljivost. Za dobro vidljivost pa je potrebna dobra razsvetljava.

V poglavju bom opisal priporočila, ki bi v okolici objekta, na objektu in v objektu lahko ustvarila razmere za dobro videnje in prijazno vidno okolje s pomočjo primerne razsvetljave.

Najprej pa je treba pojasniti izraz vidljivost (predmeta). Vidljivost je merilo težavnosti in točnosti, s katero predmet vidno odkrijemo in prepoznamo (NRVSNR, 2004: 1).

Predvsem v notranjih delovnih prostorih je zelo pomemben vpliv razsvetljave na opravljanje dela.

Da bi lahko točno razpoznali poteze človeškega obraza, je potrebna svetlost prostora okrog 1 cd/m^2. To pa se doseže v normalnih razsvetljevalnih razmerah z vodoravno osvetljenostjo približno 20 lx. Strokovnjaki priporočajo 20 lx kot najmanjšo osvetljenost v notranjosti, kjer ne poteka delo.

Mnogi notranji delovni prostori so videti nesprejemljivo temni, še pri osvetljenosti 200 lx. Zato je za prostore z normalnim nepretrganim delom priporočena minimalna osvetljenost 200 lx (tabela 4.2).

Referenčna površina v notranjosti je površina, na kateri je treba zagotoviti primerno priporočeno osvetljenost (tabela 4.1). V notranjih prostorih je referenčna površina običajno delovna površina.

Tabela 4.1: Razponi priporočenih osvetljenosti za različne površine in dejavnosti

Razponi priporočenih vzdrževalnih osvetljenosti (lx)	Vrsta površine ali dejavnosti
20–30–50	gibanje na prostem, delovišča, okolica objekta
50–100–150	pogosto prečkani prostori;* enostavna orientacija ali kratki občasni obiski
100–150–200	prostori, občasno uporabljeni za delovna opravila
200–300–500	naloge z enostavnimi vidnimi zahtevami
300–500–750	naloge s srednjimi vidnimi zahtevami
500–750–1000	naloge z velikimi vidnimi zahtevami
750–1000–1500	naloge z zelo velikimi vidnimi zahtevami
1000–1500–2000	naloge s specialnimi vidnimi zahtevami
nad 2000	izvajanje zelo natančnih vidnih nalog
* Pri pogosto prečkanih prostorih naj se vrednost uskladi z osvetljenostjo sosednjih delovnih površin ali sosednjih prostorov.	

Vir: NRVSNR 2004. Ljubljana.

Osvetljenosti za različne dejavnosti, ki so podane v tabeli 4.1, so lahko za priporočene vrednosti le ob pogoju, da so upoštevani tudi drugi vidiki, ki vplivajo na vidljivost. Eden od teh drugih vidikov je usmerjenost razsvetljave na delovno površino. Usmerjenost razsvetljave na delovno površino je splošen izraz za opis prostorske porazdelitve svetlobe, ki pada na delovno površino (NRVSNR, 2004: 8).

V številnih uradih se velik delež dejavnosti nanaša na vodoravno osvetljenost delovne površine. Predvsem je pomembna vpadna svetloba. Kot vpadne svetlobe ne sme delati lastne sence na delovno površino delavca. Pri tem sta pomembna vrsta svetilke in njena namestitev.

Pri projektu razsvetljave za vhodne prostore je treba upoštevati vpliv dnevne svetlobe, ki vdira v prostor. Pri tem je treba upoštevati tudi dejstvo, da se lahko obiskovalec, ki vstopi iz svetlega zunanjega sveta, hitro prilagodi nižji osvetljenosti, kot je zunaj. Tudi pri visokem deležu vdiranja dnevne svetlobe se lahko uporabi električna razsvetljava za ustvarjanje značilnosti prostora in dodatek bleska, posebno če je učinek koncentriran na

površino, ki je bolj oddaljena od okna. S tem se doseže zadostna razpoznavnost oseb in predmetov v hodniku ter omogočajo dobro razpoznavni videoposnetki.

Če vstopa v prostor zelo malo dnevne svetlobe, mora električna razsvetljava zapolniti vrzel med možno bleščečo sončno svetlobo zunaj in razmeroma nizko osvetljenostjo v hodnikih. Da bi to dosegli, mora biti osvetljenost 1000 lx, barva notranjih opleskov pa mora imeti višjo odsevnost.

Osvetljenost prostorov in delovnih površin pa je odvisna tudi od prahu, ki se nabira na svetilih in tako onemogoča optimalno osvetljenost. Zato je pomembno servisiranje in vzdrževanje svetilk. Te naloge morajo opravljati čistilne in servisne službe. Njihova naloga je občasno pregledovanje svetilnosti svetil in njihovo periodično čiščenje.

Tabela 4.2: Pregled nekaterih vidnih nalog ali dejavnosti v notranjih prostorih z danimi osvetljenostmi, omejitvijo bleščanja in barvno kakovostjo

Prostor, vidna naloga ali dejavnost	E_{vz}	UGR_m	R_a	Opombe
1. Splošne površine v zgradbah				
veže in predprostori	100	22	60	
prometne površine (prehodi) in hodniki	100	28	40	
stopnice, tekoče stopnice, pomični trakovi	150	25	40	
nakladališča, nakladne rampe	150	25	40	
prostori za odmor	100	22	80	
prostori za telovadbo	300	22	80	
garderobe, umivalnice, kopalnice, toaletni prostori	200	25	80	
prostori za zdravniško oskrbo	500	16	90	
nadzorni prostori, centri vodenja	500	19	80	
skladišča, shrambe, hladilnice	100	25	60	200 lx pri stalni prisotnosti
prostori za pakiranje in odpošiljanje pošte	300	25	60	
nadzorne postaje	150	22	60	200 lx pri stalni prisotnosti
22. Uradi				
urejanje dokumentov, kopiranje, prometne cone itd.	300	19	80	
pisanje, tipkanje, branje, obdelava podatkov	500	19	80	
tehnično risanje	750	16	80	

Prostor, vidna naloga ali dejavnost	E_{vz}	UGR_m	R_a	Opombe
delovna mesta za računalniško podprto načrtovanje	500	19	80	
prostori za konference in seje	500	19	80	
sprejemni pult	300	22	80	
arhiv	200	25	80	
27. Parkirne garaže (znotraj)				
vhodno-izhodne poti (podnevi)	300	25	40	Varnostne barve naj bodo razpoznavne.
vhodno-izhodne poti (ponoči)	75	25	40	
vozne poti	75	25	40	
parkirne površine	75	28	40	Visoka navpična osvetljenost povečuje prepoznavanje potez ljudi, s tem pa tudi občutek varnosti.
30. Letališča (in železniške postaje)				
prometna (povezovalna) območja, tekoče stopnice, pomični trakovi	150	22	80	
območja čakalnic	200	22	80	
območja preverjanja varnosti	300	19	80	
kontrolni stolp zračnega prometa	500	16	80	Razsvetljavo naj bo mogoče regulirati. Preprečiti je treba bleščanje zaradi dnevne svetlobe.
prostori za varnost poletov	500	16	80	
hangarji za testiranje in popravljanje	500	22	80	

Vir: NRVSNR 2004. Ljubljana.

Pojasnila k tabeli 4.2:

Stolpec 1: Naštevanje prostorov, področij, nalog ali dejavnosti

Tu je navedenih le del prostorov (območij), nalog ali dejavnosti, za katere so postavljene specifične zahteve. Če takih navedb ni, naj bodo uporabljene podobne vrednosti za situacije, ki jih je mogoče med seboj primerjati.

Stolpec 2: Povprečne vzdrževalne osvetljenosti E_{vz}

Osvetljenosti morajo biti merjene na določenih točkah delovnega območja. Izračunati je treba srednjo vrednost in enakomernost; osvetljenosti ne smejo biti pod vrednostmi, podanimi v tabeli 4.2.

Stolpec 3: Merjene vrednosti poenotenega števila bleščanja (UGR)

Merjene vrednosti so uporabljene le za navedene položaje, kjer sta uporabljena neugodno bleščanje in metoda ocenjevanja bleščanja. Proizvajalec svetil je dolžan za projektiranje dostaviti točne UGR-vrednosti.

Stolpec 4: Indeks barvnega videza (R_a)

Navedeni indeksi so minimalne vrednosti, potrebne za dela, ki so navedena v stolpcu 1. Za uporabljena svetila mora proizvajalec svetil podati zanesljive podatke za indeks barvnega videza.

Stolpec 5: Opombe

Navedeni so priporočila in opazke za izjeme in posebnosti za delo iz stolpca 1.

Slovenska zakonodaja zelo skopo določa razsvetljavo za varnostna območja. SDPVO omenja razsvetljavo le v 15. členu, kjer določa, da je zunanja razsvetljava najmanj 40 luksov in da se lahko objekt za nočno osvetljevanje namesto običajne razsvetljave opremi z IR-reflektorji; to pa je premalo.

Upoštevati je treba, da se lahko razsvetljava uporablja tudi kot dopolnilo k varovanju objektov in okolice. S svojim nenadnim vklopom in močno usmerjeno svetlobo opozori nepooblaščeno osebo, da je pod nadzorom oziroma da je opažena.

4.5 UGOTOVITVE

S spremembo zakonodaje v letih 2005 in 2006 je Republika Slovenija sprejela zakonska določila, ki omogočajo učinkovito varovanje nacionalnih tajnih podatkov ter tajnih podatkov EU in Nata. Sporazumevanje po elektronskih medijih med EU in Natom je postalo varno in zanesljivo. Na obrambnem področju Republike Slovenije so se uredila in skladno z Natovimi usmeritvami opremila varnostna območja, ki zagotavljajo varen sprejem, prenos, obdelavo in shranjevanje nacionalnih tajnih podatkov ter tajnih podatkov EU in Nata. Republika Slovenija je v celoti ratificirala Natovo direktivo AD 70-1. Natova Varnostna direktiva zavezniškega poveljstva za Evropo AD 70-1 podrobno določa postopke in ukrepe ter minimalne standarde varnosti, ki jih morajo upoštevati vse države članice. Sistemi tehničnega varovanja za varovanje tajnih podatkov v Republiki Sloveniji so v nekaterih segmentih celo strožji od Natovih. Slovenska zakonodaja strožje zapoveduje vstopanje v upravna območja in izstopanje iz njih, prav tako pa so vsa varnostna območja

tudi fizično varovana. Pomanjkljivo določena je le razsvetljava, vendar si na tem področju lahko pomagajo s priporočili Slovenskega društva za razsvetljavo, ki v svoji drugi knjigi natančno priporoča načine in vrste razsvetljave za različne prostore in objekte. Osnova za učinkovito razsvetljavo na obrambnem področju Republike Slovenije pa je zapisana tudi v podpoglavju 4.4 tega specialističnega dela. Na področju varovanja tajnih podatkov manjkajo le usmeritve, napotila in navodila odgovornih organov za varovanje tajnih podatkov.

Na obrambnem področju Republike Slovenije je treba dvigniti tudi raven varnostne kulture vseh zaposlenih. Zato se je treba čim prej lotiti načrtovanja izobraževanja in usposabljanja vseh zaposlenih na obrambnem področju Republike Slovenije. V vojaških šolah je treba spremeniti predmetnik šolskega izobraževanja in usposabljanja ter v učne načrte uvrstiti predmet varnostna kultura.

5 FIZIČNO VAROVANJE OBJEKTOV

Fizično varovanje zajema ukrepe za zaščito osebja, objektov vojaške infrastrukture, tajnih dokumentov, orožja in minskoeksplozivnih sredstev ter drugih materialno-tehničnih sredstev. Fizično varovanje zagotavlja varnost pred vohunjenjem, sabotažami, uničenjem in krajo.

V ministrstvu izvajajo fizično varovanje moštva za varovanje iz enot Slovenske vojske. Prav tako pa morajo vsi zaposleni v ministrstvu izvajati vse zahtevane ukrepe za varovanje območij in objektov vojaške infrastrukture ter varovanje dokumentov in drugih zapisov glede na stopnjo tajnosti.

Operativni sektor Slovenske vojske načrtuje, organizira in zagotavlja izvajanje fizičnega varovanja na vseh objektih Slovenske vojske skladno z Direktivo za organizacijo in izvajanje varovanja objektov v Slovenski vojski.

Fizično varovanje se v Slovenski vojski izvaja:

- s stražarsko službo,
- s prijavno službo,
- z receptorsko službo,
- s požarno službo,
- z varnostno nadzorno službo,
- z varovanjem s službenimi vojaškimi psi,
- z obhodi, kombiniranimi oblikami fizičnega varovanja, interventnimi silami in
- z varovanjem prenosa tajnih dokumentov.

Glede na zmanjševanje moštev za varovanje objektov se fizično varovanje deloma nadomešča s tehničnim ali kombiniranim načinom varovanja.

Fizično varovanje lahko v skladu z veljavno zakonodajo in predpisi izvajajo tudi pooblaščene zasebne družbe/civilne osebe. Izvajalec mora poskrbeti le, da je osebje, ki izvaja varovanje, varnostno preverjeno skladno z veljavno zakonodajo Slovenije.

5.1 ČLOVEK KOT OSNOVNI VIR VAROVANJA

Moštvo, ki zagotavlja 24-urno varovanje vse leto, mora imeti najmanj tri pripadnike v eni izmeni, praviloma iz enote za varovanje vojašnic (objektov). Prvi pripadnik varovanja je operater na tehničnih sistemih, druga dva pa sta varnostnika, ki izmenično opravljata obhode po kompleksu objekta.

V primeru sprožitve alarma praviloma najprej posredujejo pripadniki enote za varovanje vojašnic (objektov). Pripadniki enote za varovanje vojašnic (objektov) imajo svoje interventne sile (skupino za posredovanje), ki posredujejo na objektu v primeru sprožitve alarma ali drugega nepredvidljivega dogodka.

V primeru storitve kaznivega dejanja/prekrška vodja varovanja ali operater na tehničnih sistemih obvešča poveljniški operativni center Slovenske vojske, ta pa vojaško policijo in Obveščevalno-varnostno službo. V primeru napada na objekt se uporabijo sile za intervencijo.

Objekti, ki ne potrebujejo 24-urnega fizičnega varovanja, imajo pa tehnično varovanje, so nadzorovani iz varnostno nadzornega centra. V primeru sprožitve alarma se odzovejo pripadniki interventnih sil enote za varovanje vojašnic (objektov). Pripadniki interventnih sil enote za varovanje vojašnic (objektov) izvajajo tudi obhode objektov.

Sektor J-2 opredeli skupine objektov Slovenske vojske, ki se fizično in tehnično varujejo, ter varnostna območja, ki so potrebna na posameznem objektu. Če je v objektu samo del območja določen kot varnostno območje višje stopnje, se varuje in varnostno opremi samo ta del območja.

5.2 UPORABA SLUŽBENIH PSOV PRI VAROVANJU OBJEKTOV

Slovenska vojska uporablja za izvajanje določenih specialističnih nalog tudi službene pse. Zaradi njihovega izostrenega vonja in nagona se lahko službeni psi uporabljajo za pomoč pri varovanju objektov vojaške infrastrukture.

Psi se načeloma uporabljajo za varovanje predvsem zunaj delovnega časa in ponoči.

Zaradi zmanjševanja števila vojakov pri varovanju objektov vojaške infrastrukture je treba vse zahtevane naloge pri varovanju nadomestiti z drugimi oblikami varovanja. To se lahko doseže z uvajanjem tehničnih sredstev in službenih psov v sisteme varovanja.

Varovanje objektov vojaške infrastrukture s psi opredeljuje Pravilo službe v Slovenski vojski.

Vojaškega psa je smotrno vključiti v varovanje predvsem zelo ogroženih objektov. Vojaški pes lahko samostojno varuje varovani objekt na privezu ali v spremstvu vodnika vojaškega psa v patrulji. Psa lahko uporabijo tudi tako, da varuje objekt znotraj dveh ograj ali pa lahko varuje varovani objekt znotraj celotne ograje.

Objekti, ki se varujejo z vojaškimi psi, morajo biti vidno označeni s tablo z napisom: »OBJEKT VAROVAN Z VOJAŠKIM PSOM«.

Za varovanje objektov lahko uporabimo psa skupaj z vodnikom – patrulje. Taka oblika varovanja je izredno zanesljiva predvsem ponoči, v gozdu ali v drugih primerih slabe vidljivosti in drugih pogojih.

Preventivno se lahko vojaški pes skupaj z vodnikom pojavlja na različnih krajih ob različnih časih.

Za uvajanje psov v sistem tehničnega in fizičnega varovanja v ministrstvu se lahko v prihodnjem obdobju preučijo vse možnosti uporabe, predvsem pri varovanju skladišč orožja in minskoeksplozivnih sredstev.

5.3 UREJENOST OBJEKTOV IN OKOLICE

Vzdrževani objekti in urejena okolica prispevajo k učinkovitosti varovanja lastnine ministrstva. Žal se s to problematiko ukvarja zelo malo ljudi ali pa je omenjena ureditev zelo skopo določena. Nekaj določil lahko izluščimo iz Uredbe o določitvi objektov in okolišev, ki so posebnega pomena za obrambo, in ukrepih za njihovo varovanje (Uradni list RS, št. 7/1999) ter iz spremembe te uredbe (Uradni list RS, št. 17/2003).

Uredba v 1. členu določa objekte, ki so posebnega pomena za obrambo države. Med te uvršča sedeže poveljstev in Generalštaba, stacionarne objekte zvez in nadzora zračnega prostora, letalske baze, stalne priveze ladij in čolnov, objekte, namenjene za skladiščenje oborožitve, streliva, minskoeksplozivnih sredstev ter vojaške opreme, objekte, ki so posebej namenjeni za delovanje poveljstev in državnih organov v vojni, objekte za vzdrževanje oborožitve in vojaške opreme, vojašnice s pripadajočimi objekti, vojaška vadišča, strelišča, poligone.

Minister za obrambo v skladu z oceno ogroženosti in možnostmi varovanja objekta za vsak objekt posebnega pomena za obrambo države določi varnostni pas ali območje, ki je

potrebno za varno uporabo objekta (Uredba o določitvi objektov in okolišev, ki so posebnega pomena za obrambo, in ukrepih za njihovo varovanje: 1. člen).

Uredba v 2. členu določa, kateri objekti se varujejo fizično, tehnično ali kombinirano.

Objekti, ki so posebnega pomena za obrambo države, morajo biti označeni z opozorilnimi znaki (Uredba o določitvi objektov in okolišev, ki so posebnega pomena za obrambo, in ukrepih za njihovo varovanje: 7. člen).

V ministrstvu imajo z urejeno okolico okrog varovalne ograje na zunanji strani objekta precejšnje težave, saj je zemljišče na drugi strani varovalne ograje praviloma civilno. Določil, kako naj bi bila urejena okolica ograje oziroma okoliš objekta, ki je posebnega pomena za obrambo države, pa ni.

Nujno je treba najprej določiti varnosti pas okrog objekta, ki je posebnega pomena za obrambo države. Predlog varnostnega pasu mora izdelati Obveščevalno-varnostna služba in ga predložiti ministru za obrambo v podpis.

Po določitvi varnostnega pasu bo treba zakonsko urediti urejenost okoliša objekta. Posebno pozornost bo treba posvetiti oddaljenosti dreves od varnostne ograje, saj se v zimskem času in v neurjih veliko dreves podre na varnostno ograjo. S tem pa nastajajo nepotrebni stroški popravila varovalnih ograj.

Okrog varovalne ograje so večinoma posajene smreke. Smreka ima površinski sistem rasti korenin, ta pa ji ne omogoča dobre stabilnosti. Ob obilnih snežnih padavinah in večjih neurjih korenine popustijo pod težo snega ali pod pritiskom močnega vetra, in ker so drevesa posajena od varovalne ograje največ dva metra, drevo pade na varovalno ograjo in jo poruši.

Pri zasaditvi dreves in ureditvi okolice varovalne ograje bi bilo treba upoštevati naslednja priporočila:

- okrog varovalne ograje je 25 m širok pas brez dreves,
- v okolici varovalne ograje in objektov se sadijo drevesa, ki imajo globok koreninski sistem (bor, listavci …), in
- trava v varnostnem pasu je lahko visoka največ 20 cm.

Posebno pozornost pa je treba posvetiti vzdrževanju in urejenosti zgradb in rednemu vzdrževanju strelovodov. Strelovode je treba namestiti na vse zgradbe, v katerih se skladiščijo strelivo in minskoeksplozivna sredstva. Strelovod se namesti tudi na vse zgradbe, ki so izpostavljene grmenju več kot 10-krat na leto. Vsaka strelovodna napeljava ima svojo nadzorno knjigo. V knjigo se vpisujejo vsi varnostni pregledi in vzdrževanje

strelovodne napeljave. Nadzor strelovodne napeljave se izvaja najmanj enkrat letno, vsakih pet let pa se pregledajo podzemni vodi. Okolica zgradbe mora biti urejena. Okrog zgradbe je petmetrski travni pas, ki omogoča gasilskim enotam nemoten dostop do zgradbe. Poti do zgradb morajo zagotavljati dostop interventnim silam 24 ur na dan vse leto (požarne poti).

Objekt je urejen s sistemom za odvajanja meteornih vod in ima urejene potočne struge. Pri tem moramo paziti, da je pretočnost zadostna tudi ob največjih nalivih. Pri vzdrževanju potočne struge je treba upoštevati rušilno moč hudournih voda.

Tehnični sistemi na objektih in v njih morajo biti nameščeni tako, da zagotavljajo učinkovito varovanje zgradb. Kamere videonadzornega sistema so nameščene na kovinske drogove, ki so visoki in od zgradbe oddaljeni najmanj 3 m. Vsi vhodi in izhodi skozi varovalno ograjo so pod videonadzorom.

5.4 SODELOVANJE S POLICIJO

Boj proti organiziranemu kriminalu, terorizmu, trgovini z orožjem in podobno zahteva tudi širše povezovanje ministrstva z drugimi državnimi organi oziroma Policijo (Čaleta, 2006: 2). Zato je treba pri zunanjem (posrednem) varovanju objektov vojaške infrastrukture doseči boljše sodelovanje med pristojnimi organi v ministrstvu ter Policijo na področju spremljanja razmer in dogodkov v bližnji in daljni okolici objektov vojaške infrastrukture ter zagotoviti hiter obojestranski prenos informacij v primeru zaznave nevarnosti ter v primerih izrednih dogodkov v objektu vojaške infrastrukture ali zunaj njega (Čaleta, 2006: 3 in 4).

Glavne naloge na področju zunanjega varovanja vojaške infrastrukture pri sodelovanju s Policijo so:

- preprečevanje in zatiranje kriminala,
- preprečevanje oškodovanja vojaškega premoženja,
- preprečevanje ilegalne trgovine prekupčevanja in trgovanja z orožjem,
- preprečevanje terorističnih akcij in
- preprečevanje nastanka drugih kaznivih dejanj.

Vzpostavitev stika med ministrstvom, Slovensko vojsko in Policijo na področju zunanjega (posrednega) varovanja objektov vojaške infrastrukture načrtuje in vodi pristojni organ v ministrstvu in Slovenski vojski. Skupaj s Policijo preuči možnosti sodelovanja ter

pripravi načrt, kje, kdaj, s kom in kako se lahko Policija vključi v posredno varovanje objektov vojaške infrastrukture.

5.5 TEHNIČNI NADZOR NAD FIZIČNIM VAROVANJEM

Zadnji dogodki v Sloveniji (rop banke v Ljubljani) narekujejo nadzor varnostnika operaterja, ki spremlja dogodke na monitorju. Varnostnik v dogovoru z roparji lahko izklopi določene kamere in alarmni sistem, s tem pa roparjem omogoči nenadzorovani pristop do varnostno nadzornega centra oziroma varnostno nadzorne točke. Po dogovorjenem obvladovanju varnostnika v varnostno nadzornem centru lahko roparji nemoteno izvedejo popoln rop.

Tak scenarij dogodkov se lahko prepreči z neposrednim nadzorom v varnostno nadzornem centru oziroma varnostno nadzorni točki.

Z neposrednim nadzorom varnostnika, ki upravlja in nadzoruje tehnične sisteme v varnostno nadzornem centu oziroma varnostno nadzorni točki, se zagotovi, da so vsi postopki varnostnika v varnostno nadzornem centru oziroma varnostno nadzorni točki arhivirani na trdem disku videonadzornega sistema. (UOOSV/osnutek, 2005: 2. člen, točka 4).

V vseh objektih vojaške infrastrukture je treba zagotoviti varnost moštev za varovanje; ta so lahko podvržena pritiskom nepooblaščenih oseb, ki vidijo v obvladovanju osebja možnost za končno dosego določenega cilja (dogodek Roje).

V objektih vojaške infrastrukture je posebej izpostavljen kritični čas, ko je prisotnost osebja minimalna oziroma najmanjša (na primer obhodi) in je manj možnosti za pomoč v primeru ogrožanja ali neposrednega napada.

Zato morata biti na objektu poleg operaterja, ki upravlja samo s tehničnimi sredstvi, še najmanj dva varnostnika, ki opravljata neposredni vizualni nadzor objektov 24 ur na dan vse leto. Delovni čas varnostnikov pa je treba organizirati po sistemu 12 ur dela, 24 ur počitka, 12 ur dela in 48 ur počitka.

Varnost osebja, ki varuje objekte vojaške infrastrukture, je treba povečati z naslednjimi dejavniki:

- varovanje zgradb in prostorov moštev za varovanje s sistemi tehničnega varovanja za zagotavljanje aktivne in pasivne varnosti,
- oborožiti operaterja, ki upravlja s tehničnimi sistemi,

- z uvajanjem sistema »stražar« (najmanj dve osebi v eni izmeni),
- brezžično povezovanje med operaterjem, varnostnikom in vodjo interventnih sil,
- reakcijski čas interventnih sil skrajšati na najkrajši možni čas.

5.6 UGOTOVITVE

Še tako učinkovita tehnika ne more nadomestiti človeka pri zagotavljanju varovanja tajnih podatkov, in obratno, samo tehnika lahko nadzira človeka pri varovanju tajnih podatkov. Ugotavljam, da eno brez drugega ne zagotavlja učinkovitega varovanja. Človek s pomočjo tehnike nadzira varnost oseb, premoženja in podatkov, s tem si je olajšal fizični del varovanja – obhodi, straže. Prav tako pa varnostniki s pomočjo tehnike komunicirajo med sabo in z izmenjavo informacij zagotavljajo učinkovitost varovanja.

Človek si pri varovanju že stoletja pomaga tudi s psi. Pes je čuvaj naših domov in nas opozarja na spremembe v okolici. Zato je uporaba službenih psov za varovanje objektov vojaške infrastrukture zelo učinkovita. Seveda pa ima uporaba psov za varovanje vojaških objektov tudi slabosti. Pse je treba negovati, hraniti, skratka skrbeti za njih. Pri tem ni dobro, da ima pes preveč skrbnikov. Skrbnike vodnike je treba zaposliti, kar pa je pogojeno s finančnimi sredstvi; teh ministrstvo nima, vse dokler se ne zgodi izredni dogodek, potem pa se vedno najdejo.

Pri varovanju objektov je v veliko pomoč tudi sodelovanje z lokalno policijo. Ta redno opravlja nadzore komunikacij in objektov. Informacija policije o dogajanju v bližji in daljni okolici je velikega pomena za varnost vojaških objektov pred terorističnimi dejanji, organiziranim kriminalom in vandalizmom določenih skupin in posameznikov. Tega sodelovanja med ministrstvom in policijo pa je vedno premalo.

Učinkovito varnost objekta pa zagotavlja tudi urejena okolica. Okolica nekaterih vojaških objektov je s stališča varnosti neprimerno urejena. Drevesa in visoka podrast sta preblizu varovalne ograje ali samega objekta. Požarne poti so na nekaterih objektih neurejene, manjkajo hidranti za gašenje požara, struge potokov in hudournikov se ne vzdržujejo redno, in ob večjih nalivih potoki in hudourniki povzročajo veliko škodo na infrastrukturi, predvsem pa pri zagotavljanju varnosti objekta in sredstev. Za učinkovito varovanje je treba zagotoviti dovolj finančnih sredstev in jih načrtno uporabljati. Brez denarja ni varnosti.

6 VARNOSTNI STANDARDI VAROVANJA TAJNIH PODATKOV V TERENSKIH POGOJIH

Za terenske ali bojne operacije se lahko predpišejo samo minimalni varnostni standardi, predvsem zaradi tega, ker se dejansko stanje spreminja. Trenutno stanje in dovoljeni čas vplivata na minimalne varnostne standarde, ki jih je treba sproti dopolnjevati z upoštevanjem varnostnih zadržkov in zahtev za vzpostavitev trajnih varnostnih območij kot končni cilj. Za varovanje tajnih podatkov na terenu je treba uporabljati trdne objekte. V primeru, da teh ni mogoče zagotoviti (hranjenje v šotoru, bivaku), je treba dvigniti fizično raven varovanja tajnih podatkov. Zagotoviti je treba stalno, 24-urno varovanje varnostnih območij. Odgovorno poveljstvo za varovanje tajnih podatkov mora zagotoviti maksimalno podporo varovanju (stražarji, varnostni vsebniki, vozila, generatorji, ograje, orožje), da se dosežejo varnostni standardi.

Minimalne zahteve fizične varnosti, ki jih je treba upoštevati med terenskimi/bojnimi operacijami, so:

- varnostno območje je fizično locirano v okviru varovanega območja poveljstva, najprimerneje v bližini ali v samem operativnem centru poveljstva;
- varnostno območje je locirano znotraj nadzorovanega območja, ki je obdano z mehanskimi ovirami, kot so različne žične ovire (ostrivci);
- območje je varovano z obhodnimi ali stacionarnimi stražarji, ki izvajajo stalen nadzor nad varovanim območjem. Stražarji so oboroženi z orožjem in strelivom;
- dostop v varnostno območje je omejen na en sam vhod v to območje;
- vhod v varovano območje je varovan v celotnem 24-urnem obdobju;
- ustrezen seznam oseb s pooblaščenim dostopom je omejen na tiste osebe, pri katerih obstaja ustrezna potreba po vedenju in imajo ustrezno dovoljenje za dostop do tajnih podatkov;
- v ustrezno varovanem objektu se ves čas minimalno nahajata dve oboroženi osebi;
- načrt za primer izrednih dogodkov je izdelan in vedno pripravljen za uporabo;
- kadar ustrezni tajni podatki niso v uporabi, jih je treba varovati v varnostnih vsebnikih.

Komunikacije, tako žične kot brezžične, so, če je le mogoče, vzpostavljene in zavarovane z ustreznimi rezervnimi silami za varovanje.

Pred vhodom v objekt je nameščen sod z mivko, ki služi za preverjanje oborožitve (poskusno proženje) pred vstopom v objekt. Na prostoru za preverjanje oborožitve se mora iz osebne oborožitve odstraniti shramba s strelivom in izvzeti naboj iz cevi.

Zmogljivosti varnostnih območij so lahko prestavljene v terenske pogoje, brez potrebnega običajnega pisnega spričevala za vzpostavitev začasnih zmogljivosti za hranjenje tajnih podatkov v terenskih pogojih.

Na terenu se lahko kot varnostna območja uporabljajo tudi bunkerji. Trdne konstrukcije bunkerjev z omejenim dostopom oseb, nadzornimi točkami za vstop ter stalnimi nadzornimi patruljami vojaške policije zagotavljajo minimalne možnosti ogrožanja s tehničnim opazovanjem. Tehnični sistemi, ki so namenjeni za varovanje tajnih podatkov v bunkerju, preprečujejo namerno ali nenamerno odkrivanje tajnih podatkov. Na terenu ni mogoče predpisati popolnega seznama fizičnih ali tehničnih varnostnih kriterijev, ki bi bili primerni za vsak objekt. Zaradi navedenega bodo bunkerji ocenjevani na podlagi dejstev od primera do primera. V dopolnilu minimalnih standardov, ki so predvideni za vzpostavitev varnostnih območij, je treba upoštevati še naslednje:

- *zračniki* v povezavi z gretjem in prezračevanjem omogočajo dovod svežega čistega zraka v bunker. Motenje tega uravnoteženega delovanja lahko pomeni preprečitev ustreznega dovoda čistega zraka v kompleks in s tem tudi možnost operativnega delovanja oseb v njem. Z upoštevanjem teh težav je treba zračnike načrtovati in zgraditi v taki obliki, ki bo onemogočala fizični, slušni in vizualni dostop v varovano območje;
- *cevi* imajo nameščene ustrezne sisteme za preprečevanje akustičnega prenosa zvoka. Potrebni ukrepi se izvedejo na podlagi navodil, temelječih na oceni aktualnih groženj, ki jih predstavljajo cevi;
- *vrata* v bunkerjih imajo vzpostavljen radijsko kemični in biološki sistem nadtlaka. Vrata so izhodna točka v zunanje območje. Prezračevanje prostora se lahko zagotovi skozi vrata. V tem primeru morajo biti vrata opremljena z ustreznim sistemom prezračevanja in napo, ki usmerja in dovoljuje dovod čistega zraka v notranjost prostora. Bunker mora imeti najmanj dvoje vrat, in sicer glavna vhodna vrata in zasilna vrata. Namesto zasilnih vrat ima lahko zasilno izstopno okno, ki se uporabi v primeru zasilnega izhoda iz bunkerja. Zasilna vrata ali zasilno okno se odpirajo samo iz notranjosti bunkerja.

7 IZOBRAŽEVANJE IN USPOSABLJANJE

Sistemi tehničnega varovanja zaradi svoje kompleksnosti zahtevajo usposobljeno varnostno osebje. Še tako dobra tehnika je v rokah neusposobljenega osebja nekoristna in neuporabna. Celovitost, uspešnost in učinkovitost varovanja je zagotovljena le v primerih usposobljenosti varnostnega osebja oziroma moštev za varovanje ter pravilne, pravočasne in usklajene uporabe tehničnih sredstev ter varnostnega osebja.

Vsi pripadniki ministrstva in civilno varnostno osebje, ki so vključeni v sistem tehničnega in fizičnega varovanja, morajo biti usposobljeni za izvajanje varovanja in za uporabo tehničnih sredstev v sistemu varovanja.

Pred uvedbo novih sistemov tehničnega varovanja je treba izvesti usposabljanje varnostnega osebja.[7] Če je potrebno, se dodatna usposabljanja izvedejo na zahtevo poveljnika varovanja, ki je odgovoren za usposobljenost moštva za varovanje.

Zakon o tajnih podatkih v 38. členu določa, da je predstojnik organa in organizacije enkrat letno dolžan zagotoviti dodatno usposabljanje oseb, ki opravljajo naloge na področju obravnavanja in varovanja tajnih podatkov stopnje tajnosti zaupno in više.

Dolžnost usposabljanja in izpopolnjevanja v ministrstvu ima Obveščevalno-varnostna služba, ki v sodelovanju z organizacijsko enoto ministrstva, pristojno za upravljanje človeških virov, in drugimi organizacijskimi enotami ministrstva organizira ter izvaja usposabljanje in izpopolnjevanje s področja varovanja tajnih podatkov za zaposlene v vseh organizacijskih enotah ministrstva, razen Generalštaba.

Obveščevalno-varnostna služba sodeluje pri načrtovanju vsebin za usposabljanje ter izpopolnjevanje iz prejšnjega odstavka, ki ju za pripadnike Slovenske vojske organizira in izvaja Generalštab (PVTP, 2006: 8. člen).

Pomemben element pri varovanja tajnih podatkov je odnos posameznika do varovanja tajnih podatkov in do tehničnih sistemov, ki zagotavljajo varnost tajnih podatkov. Zato je zelo pomembna varnostna kultura vseh zaposlenih na obrambnem področju, ki se kaže v odnosu posameznika do spoštovanja ukrepov, navodil in standardov. Menim, da je varnostna kultura nezadostna. Čim prej je treba izdelati učne načrte, ki bodo vsebovali izobraževanje in usposabljanje vseh zaposlenih v ministrstvu na področju varnostne kulture.

[7] Usposabljanje varnostnega osebja izvede organizacija, ki je namestila tehnične sisteme v objekte MORS.

8 ZAKLJUČEK

V nalogi sem prikazal tehnične sisteme, ki so nameščeni in jih bodo še nameščali v varnostna območja in objekte na obrambnem področju v Republiki Sloveniji. V njej sem opisal uporabo razsvetljave in urejenost okolice objektov ter fizično varovanje objektov in sodelovanje med ministrstvom in Policijo. Navedene pa so tudi naloge in odgovornosti organov za varovanje tajnih podatkov na ministrstvu.

8.1 VERIFIKACIJA HIPOTEZ

Hipoteza 1: Standardi in postopki za varovanje tajnih podatkov in objektov na obrambnem področju Republike Slovenije so delno usklajeni s standardi Nata.

Na področju varovanja tajnih podatkov je Slovenija poleg predpisov EU in Nata upoštevala tudi vse posebnosti varovanja tajnih podatkov, ki so značilni za stanje na tem področju v Sloveniji. Standardi so v določenih primerih strožji, kot jih predpisuje Nato, zato so na področju varovanja tajnih podatkov delno usklajeni z standardi Nata. Po vstopu Republike Slovenije v zvezo Nato je bilo treba spremeniti in dopolniti veljavno zakonodajo na področju varovanja tajnih podatkov. Komuniciranje z organi Nata, prenos in shranjevanje tajnih podatkov Nata so zahtevali dopolnitev Zakona o varovanju tajnih podatkov in spremembo Uredbe o varovanju tajnih podatkov ter spremembo drugih predpisov, ki urejajo varovanje tajnih podatkov. V parlamentu je pri sprejemanju in dopolnjevanju zakonodaje prišlo tudi do nekaterih kompromisov, zato se varovanje tajnih podatkov na obrambnem področju Republike Slovenije razlikuje v nekaterih segmentih varovanja. Natova direktiva AD 70-1 v dodatku C k prvemu poglavju II. dela na strani 41 določa, da morajo imeti varnostna območja, v katerih se obdelujejo podatki s stopnjo Cosmic top Secret ali se v njih o njih pogovarja, okna varovana s kovinsko mrežo. Žice v mreži morajo biti premera treh milimetrov in morajo biti med sabo oddaljene tri milimetre. Slovenska zakonodaja določa, da ima II. varnostno območje vsa okna varovana z varovalno rešetko. Palice v varovalni mreži morajo biti premera najmanj 20 milimetrov in morajo biti med sabo oddaljene 150 milimetrov. V Sloveniji se vstopi oseb in vozil v

upravno območje ter izstopi iz njega obvezno nadzirajo. Natova direktiva AD 70-1 nadzor predpisuje le, če je to mogoče, sama vzpostavitev upravnega območja pa ni obvezna. Razlika je tudi pri fizičnem varovanju: Natova direktiva fizično varovanje predpisuje samo za tiste države, kjer nacionalna zakonodaja omogoča fizično varovanje tajnih podatkov. V Sloveniji se tajni podatki varujejo tudi fizično. Fizično varovanje izvajata notranja ali stražarska služba. Po uveljavitvi dopolnitev in sprememb zakonodaje je bilo treba spremeniti tudi urejenost varnostnih območij. Varnostna območja je bilo treba posodobiti in opremiti skladno z ratificiranimi direktivami Nata. Posodobitev in izgradnja je terjala določene gradbene posege. Na objektih, kjer ni bilo mogoče zagotoviti predpisane gradbene ureditve (debelina sten), je bilo treba kupiti boljšo opremo. Pomanjkljivo določena je le razsvetljava, vendar si na tem področju lahko pomagajo s priporočili Slovenskega društva za razsvetljavo, ki v svoji drugi knjigi natančno priporoča načine in vrste razsvetljave za različne prostore in objekte.

Hipoteza 2: Standardi tehničnega varovanja tajnih podatkov in objektov na obrambnem področju Republike Slovenije so usklajeni s standardi Nata.

V specialističnem delu sem hipotezo popolnoma potrdil. Standardi tehničnega varovanja tajnih podatkov na obrambnem področju Republike Slovenije so popolnoma usklajeni z Natovimi standardi. Sprejeti standardi za varovanje tajnih podatkov omogočajo učinkovito varovanje nacionalnih tajnih podatkov ter tajnih podatkov EU in Nata. Sporazumevanje po elektronskih medijih med EU in Natom je postalo varno in zanesljivo. Na obrambnem področju Republike Slovenije so se uredila in skladno z Natovimi usmeritvami opremila varnostna območja, ki zagotavljajo varen sprejem, prenos, obdelavo in shranjevanje nacionalnih tajnih podatkov ter tajnih podatkov EU in Nata. Varnostna območja so organizirana in opremljena tako, da zagotavljajo slovenske in Natove standarde. Varnostno območje I. stopnje je označen prostor, v katerem se lahko obdelujejo tajni podatki stopnje zaupno ali višje stopnje tajnosti tako, da že sam vstop v varnostno območje pomeni dostop do tajnih podatkov. V varnostnem območju I. stopnje in pred njim so nameščeni naslednji varnostni sistemi: protivlomni sistemi, vstopna kontrola, sistem za odkrivanje in javljanje nepooblaščene prisotnosti, sistem za odkrivanje in javljanje požara in videonadzor. V varnostnem območju I. stopnje se izvajajo naslednji varnostni ukrepi: vodenje razvida tajnih podatkov, prepoved vnosa kakršnih koli mehanskih, elektronskih in optičnih sestavnih delov ter neposredno in neprekinjeno fizično varovanje varnostnega območja.

Varnostno območje II. stopnje je označen prostor, v katerem se tajni podatki stopnje zaupno ali višje stopnje obravnavajo tako, da sam vstop v to območje in gibanje v njem še ne omogočata dostopa do teh podatkov. V II. varnostnem območju in pred njim so nameščeni naslednji varnostni sistemi: protivlomni sistemi, vstopna kontrola, sistem za odkrivanje in javljanje nepooblaščene prisotnosti in sistem za odkrivanje in javljanje požara. Določena varnostna območja II. stopnje so varovana tudi z videonadzorom. V varnostnem območju II. stopnje se izvajajo naslednji varnostni ukrepi: vodenje razvida tajnih podatkov, prepoved vnosa kakršnih koli mehanskih, elektronskih in optičnih sestavnih delov ter neposredno in neprekinjeno fizično varovanje varnostnega območja. Okoli varnostnega območja I. ali II. stopnje ali na poti, ki vodi v varnostno območje, so vzpostavljena upravna območja. Upravna območja so vidno označena in nadzirana. Nadzira se vstopanje in izstopanje oziroma gibanje oseb in vozil. V upravnih območjih se lahko shranjujejo in obdelujejo samo tajni podatki stopnje interno. Z varnostnimi postopki in ukrepi pa se zagotavlja, da imajo dostop do teh podatkov samo osebe, ki so s pisno izjavo potrdile, da so seznanjene s predpisi, ki urejajo obravnavanje tajnih podatkov. V upravnem območju in pred njim so nameščeni naslednji varnostni sistemi: protivlomni sistemi, vstopna kontrola in sistem za odkrivanje in javljanje požara. Določena upravna območja imajo nameščen videonadzor.

S tem je Republika Slovenija v celoti ratificirala Natovo direktivo AD 70-1.

Hipoteza 3: Namestitev tehničnih sistemov na objekte in vanje zmanjšuje obseg fizičnega varovanja.

Na obrambnem področju Republike Slovenije je fizično varovanje še vedno osnova za varovanje tajnih podatkov in objektov. Fizično varovanje se dopolnjuje s tehničnimi sistemi. Učinkovitega varovanja brez prisotnosti človeškega vira ni, in obratno, učinkovitega fizičnega varovanja brez tehničnih sistemov ni. Glede stroškov je fizično varovanje dražje, vendar je za učinkovito varovanje tajnih podatkov in objektov treba zagotoviti minimalno še sprejemljivo prisotnost človeka za varovanje. Seveda pa se je z uporabo tehničnih sredstev število varnostnikov/stražarjev prepolovilo (slika 3.1: Deleži celovitega sistema varovanja, stran 18). Človek s pomočjo tehnike nadzira varnost oseb, premoženja in podatkov; s tem si je olajšal fizični del varovanja – obhode, straže. Prav tako pa varnostniki s pomočjo tehnike komunicirajo med sabo ter z izmenjavo informacij zagotavljajo učinkovitost varovanja. Človek si pri varovanju že stoletja pomaga tudi s psi.

Uporaba službenih psov za varovanje objektov vojaške infrastrukture je zelo učinkovita. Seveda pa ima uporaba psov za varovanje vojaških objektov tudi pomanjkljivosti. Pse je treba negovati, hraniti, skratka skrbeti zanje. Pri varovanju objektov je v veliko pomoč tudi sodelovanje z lokalno policijo. Policija redno opravlja nadzore komunikacij in objektov. Njihova informacija o dogajanju v bližji in daljni okolici je velikega pomena za varnost vojaških objektov pred terorističnimi dejanji, organiziranim kriminalom in vandalizmom določenih skupin in posameznikov. Učinkovito varnost objekta pa zagotavlja tudi urejena okolica. Okolica nekaterih vojaških objektov je s stališča varnosti neprimerno urejena.

»Tudi najsodobnejše tehnično sredstvo brez nadzora in upravljanja človeka izgubi svoj pomen in vrednost.« (Golob, 1997: 27)

Hipoteza 4: Samo enotno, učinkovito in sodobno tehnično in fizično varovanje bo zagotavljalo varnost tajnih podatkov in objektov na obrambnem področju Republike Slovenije.

Po zaključeni izgradnji tehničnega varovanja na obrambnem področju Republike Slovenije se bo dosegla višja stopnja varnosti tajnih podatkov in objektov. Zagotovil se bo enoten sistem, ki ga bo lažje nadzirati. Z enotnim sistemom tehničnega varovanja se bo zagotovila visoka učinkovitost varovanja tajnih podatkov in objektov. Nadzor nad varovanjem tajnih podatkov na obrambnem področju Republike Slovenije se bo izvajal iz varnostno nadzornega centra, v katerem bodo varnostniki operaterji upravljali in nadzirali tehnične sisteme za varovanje tajnih podatkov na obrambnem področju Republike Slovenije. V varnostno nadzornih centrih bodo trajno in kontinuirano spremljali dinamiko dogajanj v vseh varovanih območjih na obrambnem področju Republike Slovenije. Na monitorjih nadzornih naprav bodo zaznavali nepooblaščene prisotnosti v varnostnih območjih in drugih prostorih ter okolici, ki bodo pod tehničnim nadzorom. V nadzorno varnostnih centrih se bodo reševali izredni dogodki in odzivanja na alarmne situacije.

8.2 UPORABNOST UGOTOVITEV NA OBRAMBNEM PODROČJU

Za učinkovito varovanje tajnih podatkov na obrambnem področju Republike Slovenije predlagam naslednjo opremljenost varnostnih območij (slika 8.1).

Slika 8.1: Varnostna območja

Vir: Poveljniško štabna šola 2007. Poljče

8.2.1 Varnostno območje I. stopnje

Dostop do varnostnega območja I. stopnje je lahko tudi iz upravnega območja.

Prostor, v katerem je varnostno območje I. stopnje, ima zunanje stene iz betona. Stene so debele 150 mm. Če so stene zidane z zidakom debeline 250 mm, mora biti varnostno območje oddaljeno od zunanje ograje 100 m. Varovalna ograja okrog objekta je visoka najmanj 2,15 m. Strop varnostnega območja je iz armiranega betona ali podobnih materialov enake trdnosti in debeline 150 mm. Notranje stene so iz armiranega betona ali iz drugih materialov enake mehanske trdnosti debeline 100 mm. Vstopna vrata so masivna lesena, debela 40 mm, ali kovinska s kovinsko ploščo debeline 2 mm. Vrata so ozemljena ter ognjevzdržna (zadržujejo ogenj najmanj 30 minut), opremljena s standardiziranim protivlomnim ščitom ključavnice in ključavnico z varnostnim cilindričnim vložkom ter z večtočkovno prečno zaporo. Krilo vrat se odpira v prostor. Tečaji vrat so v varnostnem območju in varovani. Vrata so opremljena s samozapiralom in slepo kljuko na obeh straneh. Na vseh oknih varnostnega območja so kovinske rešetke. Material kovinskih rešetk je trd, odporen proti rezanju in žaganju ter v notranjosti žilav. Rešetke so nameščene na okna, ki so v višini 5,5 m od tal. Varovalna rešetka je sestavljena iz kovinskih palic, ki so debele najmanj 20 mm. Razdalja med palicami v varovalni rešetki je 150 x 150 mm.

Varovalna rešetka je sidrana v zid zgradbe, globina sidra pa je najmanj 150 mm. Varovalna rešetka je lahko pritrjena z vijaki tudi v notranjosti prostora, vendar pa je treba matico vijaka zavariti.

Prostor varnostnega območja ima nameščen sistem za avtomatsko zaznavanje požara in je varovan z alarmnim sistemom. Tipkovnica alarmnega sistema je pred vhodnimi vrati v prostor.

S sistemom videonadzora se nadzira vhod v varnostno območje, za kar se uporabljajo barvne kamere. Zunanje kamere so opremljene z dodatnimi halogenskimi reflektorji moči 500 W in vgrajenimi infrardečimi pasivnimi javljalniki, notranje kamere pa so opremljene s halogenskimi reflektorji moči 150 W. Snemanje se izvaja z DVD-snemalnikom z možnostjo priključitve 16 kamer.

Sistem kontrole vstopa je z magnetnimi karticami ali sistemom brez kontaktnih kartic v kombinaciji s kodo. Registratorji so na obeh straneh vrat.

Blagajna v varnostnem območju je protivlomna s sistemom javljanja, ognjevzdržna in z vgrajeno elektronsko ključavnico. Blagajna ima v levem zgornjem kotu nalepko z veliko črko T ali ST. Blagajna je lahko pritrjena na tla varnostnega območja. Za hrambo vseh ključev se uporablja posebna varnostna omara, ki je nameščena v upravnem območju.

Vse prezračevalne in inštalacijske poti, katerih premer je večji od 150 mm, so opremljene z rešetko, ki ima prečne palice debele 10 mm. Palice so zavarjene v mrežo 150 x 150 mm.

Rezalniki za uničevanje dokumentov režejo papir z vzdolžnim in prečnim rezom v merah 0,8 x 15 mm.

Vsi alarmni sistemi morajo biti speljani v varnostno nadzorno točko, od koder operater nadzoruje delovanje sistemov in spremlja dogodke na monitorju računalnika in javljalnikih signalov.

Slika iz videokamere se snema na trdi disk DVD-snemalnika, ki je nameščen v varnostno nadzornem centru ali varnostno nadzorni točki (upravno območje).

Varnostna območja, v katerih se obdelujejo in hranijo tajni podatki s stopnjo tajnosti tajno ali višje stopnje, se morajo zaščititi pred pasivnim ali aktivnim poskusi prisluškovanja. Prostor mora biti protiprislušno pregledan.

Enota ali poveljstvo določi odgovorno osebo za izdelavo načrta varovanja in odgovorno osebo za hranjenje, obdelavo in branje tajnih podatkov.

8.2.2 Varnostno območje II. stopnje

Dostop do varnostnega območja II. stopnje je skozi upravno območje.

Prostor, v katerem je varnostno območje II. Stopnje, ima zunanje stene iz betona. Stene so debele 150 mm. Če so stene zidane z zidakom debeline 250 mm, je varnostno območje oddaljeno od zunanje ograje 100 m. Varovalna ograja okrog objekta je visoka najmanj 2,15 m. Strop varnostnega območja je iz armiranega betona ali podobnih materialov enake trdnosti in debeline 150 mm. Notranje stene so iz armiranega betona ali iz drugih materialov enake mehanske trdnosti debeline 100 mm. Vstopna vrata so masivna lesena, debela 40 mm, ali kovinska s kovinsko ploščo debeline 2 mm. Vrata so ozemljena ter ognjevzdržna (zadržujejo ogenj najmanj 30 minut), opremljena s standardiziranim protivlomnim ščitom ključavnice in ključavnico z varnostnim cilindričnim vložkom ter z večtočkovno prečno zaporo. Krilo vrat se odpira v prostor. Tečaji vrat so v varnostnem območju in varovani. Vrata so opremljena s samozapiralom in slepo kljuko na obeh straneh. Vsa okna varnostnega območja imajo kovinske rešetke. Material kovinskih rešetk je trd, odporen proti rezanju in žaganju ter v notranjosti žilav. Rešetke so nameščene na okna, ki so v višini 5,5 m od tal. Varovalna rešetka je sestavljena iz kovinskih palic, ki so debele najmanj 20 mm. Razdalja med palicami v varovalni rešetki je 150 x 150 mm. Varovalna rešetka je sidrana v zid zgradbe, globina sidra je najmanj 150 mm. Varovalna rešetka je lahko tudi pritrjena z vijaki v notranjosti prostora, vendar pa mora biti matica vijaka zavarjena.

Prostor varnostnega območja ima nameščen sistem za avtomatsko zaznavanje požara in je varovan z alarmnim sistemom. Tipkovnica alarmnega sistema je pred vhodnimi vrati v prostor.

Vhod v varnostno območje se lahko varuje tudi s sistemom videonadzora, za kar se uporabljajo barvne kamere. Zunanje kamere so opremljene z dodatnimi halogenskimi reflektorji moči 500 W in vgrajenimi infrardečimi pasivnimi javljalniki, notranje kamere pa so opremljene s halogenskimi reflektorji moči 150 W. Snemanje se izvaja z DVD-snemalnikom z možnostjo priključitve 16 kamer.

Zasilni izhod iz varnostnega območja se varuje z zunanjo kamero, ki je nameščena na samostojnem stebru na višini 3 m in 3 m oddaljena od objekta.

Sistem kontrole vstopa je z magnetnimi karticami ali sistemom brez kontaktnih kartic v kombinaciji s kodo. S sistemom kontrole vstopa se opremijo naslednja vrata: glavni vhod,

zasilni izhod in vstop v varnostno območje II. stopnje. Vsa vrata so z obeh strani opremljena s slepo kljuko. Registratorji so na obeh straneh vrat.

Blagajna je protivlomna in ognjevzdržna. Blagajna ima v levem zgornjem kotu nalepko z veliko črko Z. Za hrambo vseh ključev se uporablja posebna varnostna omara, ki je nameščena v upravnem območju.

Vse prezračevalne in inštalacijske poti, katerih premer je večji od 150 mm, so opremljene z rešetko, ki ima prečke debele 10 mm in mrežo 150 x 150 mm. Aktivni prostori so opremljeni z varnostnimi blagajnami (protivlomna in protipožarna zaščita). Rezalniki za uničevanje dokumentov režejo papir vzdolžnim in prečnim rezom v merah 0,8 x 15 mm.

Vsi alarmni sistemi so speljani v varnostno nadzorni center ali varnostno nadzorno točko, od koder operater nadzoruje delovanje sistemov in spremlja dogodke na monitorju računalnika in javljalnikih signalov. Slika iz kamere pred vhodom v varnostno območje II. stopnje in iz kamere pred vrati za zasilni izhod je speljana v varnostni nadzorni center ali varnostno nadzorno točko.

Če se v varnostnem območju obdelujejo in hranijo tajnih podatkih s stopnjo tajnosti tajno, se mora prostor zaščititi pred pasivnimi ali aktivnimi poskusi prisluškovanja. Prostor mora biti protiprislušno pregledan.

Enota ali poveljstvo mora določiti odgovorno osebo za izdelavo načrta varovanja in odgovorno osebo za hranjenje, obdelavo in branje tajnih podatkov.

8.2.3 Upravno območje

Vstop v upravno območje in izstop iz njega potekata pod nadzorom. Vhodna vrata so zaprta in onemogočajo vstop v varnostno območje in izstop iz njega brez nadzora. Vrata so opremljena s samozapiralom in slepo kljuko na obeh straneh vrat. Glavna vhodna vrata v varnostno območje so opremljena z videofonom, domofonom ali zvoncem (signal je speljan v varnostno nadzorno točko, k dežurnemu ali v tajništvo poveljstva oziroma enote). Sistem kontrole vstopa in izstopa je z magnetnimi karticami. Prostori imajo nameščene sisteme za avtomatsko zaznavanje požara. Vstop drugih oseb v varnostno območje in izstop iz njega je mogoč ob navzočnosti oseb, ki so zaposlene v varnostnem območju.

8.3 KOMISIJA ZA TEHNIČNO IN FIZIČNO VAROVANJE

Na področju tehničnega in fizičnega varovanja bi bilo treba ustanoviti komisijo za tehnično in fizično varovanje. Komisijo bi na predlog J-2 imenoval minister za obrambo.

Komisijo bi sestavljali člani iz J-2, G-2, logistike GŠSV, Sektorja za gospodarjenje z nepremičninami in Obveščevalno-varnostne službe. Komisija bi imela predsednika in bi k sodelovanju povabila tudi druge strokovnjake na področju varovanja oziroma strokovnjake različnih strok, da bi s svojimi strokovnimi nasveti prispevali k večji varnosti.

Člani komisije bi imeli svoje namestnike, ki bi jih imenovala komisija. Namestniki bi zamenjevali člane v njihovi odsotnosti.

Vse osebe, ki bi bile imenovane v komisijo, bi se morale na svojem delovnem področju ukvarjati z varovanjem objektov in tajnih podatkov. Za realizacijo letnih nalog bi komisija izdelala načrt dela, v katerem bi opredelila naloge za posamezne sektorje v poveljstvih in enotah ter v notranjih organizacijskih enotah ministrstva.

Komisija bi bila odgovorna za sistemska vprašanja, ki opredeljujejo:

- kaj se bo varovalo,
- kako se bo varovalo,
- načrtovanje sredstev, ki se bodo vgrajevala v objekte in prostore za potrebe varovanja,
- načrtovanje usposabljanja,
- vzdrževanje tehničnih sistemov in
- opravljanje nadzorov nad varovanjem objektov vojaške infrastrukture in tajnih podatkov.

Komisija za tehnično in fizično varovanje bi imela naslednje naloge:

- podajala bi strokovne usmeritve za izdelavo študij za izgrajevanje sistemov tehničnega varovanja objektov na obrambnem področju,
- sprejemala bi strokovne odločitve o ustreznosti uporabniških zahtev za sisteme tehničnega varovanja na obrambnem področju,
- spremljala bi stanje na področju razvoja tehničnega varovanja in predlagala izboljšave,
- odobravala bi načrt celotnega servisiranja sistemov tehničnega varovanja na obrambnem področju,
- usklajevala bi vse dejavnosti na področju sistemov tehničnega varovanja z organi upravnega dela ministrstva,

- opredeljevala bi varnostne zahteve za pogodbene izvajalce v primeru, da se izvajanje dejavnosti veže na določila varovanja tajnih podatkov,
- sprejemala bi dolgoročne standarde in usmeritve pri vpeljevanju novosti na področju sistemov tehničnega varovanja na obrambnem področju,
- k sodelovanju bi vabila strokovnjake, ki lahko pripomorejo k izboljšanju strokovnih odločitev (informatika, zveze ipd.),
- izvajala bi nadzor nad rednim vzdrževanjem in vrednotenjem tehničnih sistemov in
- v sodelovanju z drugimi organi upravnega dela ministrstva bi spremljala realizacijo pogodbenih obveznosti s strani zunanjih pogodbenikov.

Poleg teh nalog pa bi komisija preučevala in določevala vključevanje tehničnih sistemov v sistem varovanja. Za preučevanje in določanje sistemov bi komisija kot temeljne akte upoštevala določila Zakona o obrambi, Zakona o tajnih podatkih, Zakona o varstvu osebnih podatkov, Uredbe o varovanju tajnih podatkov, Uredbe o obveznem organiziranju službe varovanja, Sklepa o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja, Pravil službe v Slovenski vojski (v Pravilih službe v Slovenski vojski je opredeljeno fizično varovanje – stražarska in dežurna služba) in drugih veljavnih predpisov v Sloveniji, ki določajo varovanje.

Komisija bi nadzirala:

- ali ima oprema, ki se vgrajuje oziroma instalira na objekte ministrstva in vanje, opravljene ustrezne ateste oziroma ima certifikat, ki ga je izdala ustrezna institucija v Sloveniji, in
- ali vsa varnostnotehnična oprema varnostnih območij ustreza pogojem, ki jih na predlog nacionalnega varnostnega organa določi s sklepom Vlada Republike Slovenije.

Komisija bi preverjala, da vsa podjetja oziroma zunanji izvajalci (ki pripravljajo projektno dokumentacijo za namestitev sistemov tehničnega varovanja, vgrajujejo opremo oziroma vzpostavljajo njeno delovanje) izpolnjujejo vse kriterije, ki so določeni z zakonodajo Republike Slovenije.

Komisija bi načrtovala:

- dolgoročne smernice za tehnično in fizično varovanje, zmanjševanje števila moštva za varovanje objektov ter
- zagotavljanje varovanja s pomočjo tehničnih sredstev in iskanje novih rešitev, s katerimi bi se zagotavljala kakovost varovanja.

Pri razvoju tehničnega in fizičnega varovanja bi komisija upoštevala dolgoročni razvoj Slovenske vojske in določala lokacije, ki se bodo tehnično in fizično varovale v prihodnosti (predvsem opremljanje objektov Slovenske vojske s sistemi tehničnega varovanja).

Za kratkoročno načrtovanje tehničnega in fizičnega varovanja bi komisija izdelala načrt prioritet za tehnično in fizično varovanje. Ta načrt bi vseboval količinske in osnovne tehnične podatke o sistemih in lokacijah. Iz celotnega načrta bi bila razvidna pot oblikovanja tehničnega varovanja kot elementa varovanja. Na podlagi predvidenih finančnih sredstev bi se oblikoval spisek prioritetnih enot in mest, kjer bi se začeli postavljati tehnični sistemi varovanja (dograjevati obstoječi ali graditi novi).

Komisija bi določevala tudi nosilce za prevzem sistemov tehničnega varovanja, ki so odgovorni za delovanje sistemov in usposabljanje neposrednih uporabnikov sistemov za tehnično varovanje.

Komisija bi bila za svoje delo odgovorna ministru za obrambo. O svojem delu bi poročala ministru za obrambo dvakrat na leto.

8.4 SKLEPNA MISEL

Varnostna območja so ključni element varnostne politike držav članic zveze Nato. Urejen sistem varnostnih območij v evro-atlantski povezavi je zelo pomemben za njeno varnost, predvsem pa za varnost tajnih podatkov pred zlorabami. Za učinkovito delovanje sistema varovanja je pomembna postavitev vseh delov tega sistema v vseh državnih organih, predvsem pa na obrambnem področju. Država, ki ustrezno varuje svoje tajne podatke, v mednarodni skupnosti velja za zaupanja vredno in za enakovrednega partnerja.

Ob strateškem in operativnem kreiranju varnostnih območij se država lahko vključi v mednarodni sistem izmenjave tajnih podatkov na dvostranski ravni ali na ravni mednarodnih organizacij, kot sta EU in Nato.

Osnovna naloga politike varnostnih območij je, da prepreči nepooblaščen dostop do tajnih podatkov in da se varnostna območja izolirajo od drugih območij predvsem zaradi nevarnosti groženj, ki prihajajo iz okolja. Organizacije na obrambnem področju Republike Slovenije z varnostnimi območji pridobijo boljši nadzor nad shranjevanjem tajnih podatkov in poslovanjem z njimi.

Varnostna območja, ki preprečujejo nedovoljen dostop do tajnih podatkov, so ključnega pomena za varnostno politiko države. Varnostna območja prinašajo višjo raven varnostne kulture in usklajenost nacionalne zakonodaje s predpisi Nata.

V letu 2006 je Slovenija uskladila predpise na področju tehničnega varovanja z Natom. S sprejetjem zakonodaje si je zagotovila pogoje za izmenjavo tajnih podatkov v EU in zvezi Nato.

Človek kot posameznik, vsako poveljstvo in enota (organizacija) morajo težiti k varnosti in kreiranju varnostnih območjih, da se lahko dosežejo boljši rezultati dela in učinkovitost.

9 LITERATURA IN VIRI

9.1 KNJIGE

1. Čas, Tomaž (1995): Zasebno varovanje in pooblastila varnostnikov. Ljubljana. CIP.
2. Fluri, Phillip, in Johnsson, Andres B., ter sodelavci (2003): Parlamentarni nadzor nad varnostnim sektorjem: načela, mehanizmi in praksa. Ljubljana: CIP.
3. Furlan, Branimir, in drugi (2006): Vojaška doktrina. Ljubljana: Defensor.
4. Golob, Renato (1997): Sistemi zaščite in varovanja oseb in premoženja. Ljubljana. Samozaložba.
5. Grizold, Anton (1999): Evropska varnost. Ljubljana: FDV.
6. Grizold, Anton (1999): Obrambni sistemi Republike Slovenije. Ljubljana: VPŠ.
7. Grizold, Anton (2005): Slovenija v spremenjenem varnostnem okolju. Ljubljana: FDV.
8. Grizold, Anton, in drugi (1999): Suvremeni sistemi nacionalne sigurnosti. Zagreb: CIP.
9. Huntington, P. Samuel (2005): Spopad civilizacij. Ljubljana: Mladinska knjiga Založba.
10. Jelušič, Ljubica (1997): Legitimnost sodobnega vojaštva. Ljubljana: FDV.
11. Marjan, Malešič (2002): Nacionalna in mednarodna varnost. Ljubljana: CIP.
12. Neumüller, Smiljan, Planinšek, Vlado, in sodelavci (2004): Notranja razsvetljava in vzdrževanje razsvetljave (druga izdaja). Maribor: Slovensko društvo za razsvetljavo.
13. Prezelj, Iztok (2005): Nacionalna in mednarodna varnost. Poljče.

9.2 STROKOVNI IN ZNANSTVENI ČLANKI

1. Anžič, Andrej, Božič, Liliana (2006): Obveščevalno varnostni interesi Republike Slovenije po vstopu v zvezo NATO in Evropsko unijo. Dnevi varstvoslovja 2006, VPVŠ, cd.
2. Balant, Marjan, Čaleta, Denis (2006): Varnostna dejavnost v Slovenski vojski – nove dimenzije razvoja. Dnevi varstvoslovja 2006, VPVŠ, cd.
3. Cvelkar, Branko (2006): Upravljanje z viri pri zagotavljanju varnosti. Dnevi varstvoslovja 2006, VPVŠ, cd.

4. Čaleta, Denis (2004): Varovanje tajnih podatkov v zvezi Nato. Ljubljana. Bilten Slovenske vojske.
5. Čaleta, Denis (2006): Sodelovanje med policijo in vojsko na področju boja proti terorizmu – Realnost ali zgolj želja? Dnevi varstvoslovja 2006, VPVŠ, cd.
6. Faganel, Roman, Anžič, Andrej (2006): NATO in nacionalna varnostna območja. Dnevi varstvoslovja 2006, VPVŠ, cd.
7. Prezelj, Iztok (2006): Modeliranje celovitega ocenjevanja ogrožanja nacionalne varnosti. Dnevi varstvoslovja 2006, VPVŠ, cd.
8. Rogers, S. (1999): Computer System Security, International Security Review, št 110.
9. Rozman, Janez (2006): Merila za določanje tajnosti. Dnevi varstvoslovja 2006, VPVŠ, cd.

9.3 DOKUMENTI

1. Ustava Republike Slovenije. Uradni list RS/I, št. 33/1991 in 24/2003.
2. Kazenski zakonik Republike Slovenije. Uradni list RS, št. 63/1994, 23/1999 in 40/2004.
3. Resolucija o nacionalni varnosti Republike Slovenije. Uradni list RS, št. 56/2001.
4. Zakon o obrambi. Uradni list RS, št 103/2004.
5. Zakon o javnih uslužbencih. Uradni list RS, št. 56/2002.
6. Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb. Uradni list RS, št. 26/2003.
7. Zakon o tajnih podatkih. Uradni list RS, št. 87/2001 in 101/2003 – dopolnitve ter 28/2006 – spremembe.
8. Zakon o zasebnem varovanju in obveznem organiziranju službe varovanja. Uradni list RS, št. 32/1994, 23/1997 in 9/1998.
9. Zakon o osebnem varovanju. Uradni list RS, št. 126/2003.
10. Zakon o Slovenski obveščevalno-varnostni agenciji. Uradni list RS, št. 23/1999 in 126/2003.
11. Zakon o dostopu do informacij javnega značaja. Uradni list RS, št. 8/2005.
12. Zakon o policiji. Uradni list RS, št. 3/2006.
13. Zakon o arhivskem gradivu. Uradni list RS, št. 20/1997.

14. Zakon o ratifikaciji Sporazuma med pogodbenicami Severnoatlanske pogodbe o varnosti podatkov. Uradni list RS, št. 83/2004.
15. Zakon o varstvu pred požarom. Uradni list RS, št. 71/93 in 87/2001.
16. Zakon o varnosti in zdravju pri delu. Uradni list RS, št. 56/1999.
17. Zakon o eksplozivnih snoveh, vnetljivih tekočinah, plinih in drugih nevarnih snoveh. Uradni list SRS, št. 18/1977.
18. Zakon o prevozu nevarnega blaga. Uradni list RS, št. 79/1999.
19. Zakon o kemikalijah. Uradni list RS, št. 36/1999.
20. Zakon o varstvu osebnih podatkov. Uradni list RS, št. 86/2004.
21. Zakon o varstvu pred naravnimi in drugimi nesrečami. Uradni list RS, št. 64/1994 in dopolnilo 2006.
22. Uredba o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov. Uradni list RS, št. 70/2002.
23. Uredba o varovanju tajnih podatkov. Uradni list RS, št. 74/2005.
24. Uredba o obveščevalno-varnostni službi Ministrstva za obrambo. Uradni list RS, št. 63/1999 in 2000 – sprememba.
25. Uredba o obveznem organiziranju službe varovanja. 2005 – osnutek.
26. Uredba o določitvi objektov in okolišev, ki so posebnega pomena za obrambo, in ukrepih za njihovo varovanje. Uradni list RS, št. 7/1999 in 67/2003 – sprememba.
27. Uredba o notranjem nadzoru nad izvajanjem Zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi. Uradni list RS, št. 106/2002.
28. Uredba o upravnem poslovanju. Uradni list RS, št. 20/2005.
29. Uredba o pisarniškem poslovanju in o dolžnostih upravnih organov do dokumentarnega gradiva. Uradni list RS, št. 72/1994 in 82/1994.
30. Uredba o določitvi obrambnih potreb. Uradni list RS, št. 30/2003.
31. Uredba o načinu in postopku varnostnega preverjanja. Uradni list RS, št. 110/2003.
32. Uredba o ugotavljanju izpolnjevanja pogojev za posredovanje tajnih podatkov drugi organizaciji. Uradni list RS, št. 106/2002.
33. Uredba o organih v sestavi ministrstev. Uradni list RS, št. 58/2003.
34. Uredba o varovanju določenih oseb, objektov in okolišev objektov, v katerih so sedeži državnih organov. Uradni list RS, št. 103/2000.
35. Pravila službe v Slovenski vojski. Uradni list RS, št. 49/1996 in 82/2003.

36. Pravilnik o varovanju podatkov na Ministrstvu za obrambo. Šifra 0070-5/2006-4, z dne 21. 2. 2006.
37. Pravilnik o zaščiti in varovanju informacijskega sistema MORS. MORS, št. 012-59/96, z dne 5. 6. 2006.
38. Pravilnik o skladiščnem poslovanju. MORS, št. 017-02-4/99, z dne 21. 9. 1999.
39. Odlok o varnostnih ukrepih na obrambnem področju. Uradni list RS, št. 49/1992.
40. Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov. Uradni list RS, št. 6/2002.
41. Sklep o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja. Uradni list RS, št. 94/2006.
42. Navodilo za izvajanje uredbe o pisarniškem poslovanju in dolžnostih upravnih organov do dokumentarnega gradiva. Uradni list RS, št. 41/1995.
43. Navodilo za izvajanje posebnih ukrepov za varovanje dokumentov in drugih zapisov, ki so določeni kot obramba – državna skrivnost oziroma vojaška ali uradna skrivnost s stopnjo »strogo zaupno«. Uradni list RS, št. 38/1993.
44. Navodilo o pisarniškem poslovanju v MORS. Ministrstvo za obrambo, št. 017-04-29/97, z dne 4. 12. 1997.
45. Navodilo o medsebojnem sodelovanju Obveščevalno-varnostne službe Ministrstva za obrambo in vojaške policije pri preiskovanju kaznivih dejanj. MORS, šifra 017-04-28/2004-4, z dne 21. 6. 2005.
46. Izjava o varnosti v Ministrstvu za obrambo. Ministrstvo za obrambo, št. 102-00-1/01-32, z dne 1. 8. 2001.
47. Pravila štabnega dela. GŠSV, šifra 017-02-1/00-1, z dne 5. 6. 2000.
48. Direktiva o pristojnostih GŠ in PS SV. GŠSV, šifra I 802-00-2/2003-29-35, z dne 10. 4. 2003.
49. Direktiva za ravnanje z vojaškim strelnim orožjem in strelivom v silah Slovenske vojske, šifra 0070-4/2006-1, z dne 22. 2. 2006.
50. Direktiva za obveščevalno zagotovitev ter za uresničevanje štabno varnostnih nalog v Slovenski vojski. GŠSV, šifra Z 017-03-1/01-12, z dne 20. 11. 2001.
51. Direktiva o postopkih v zvezi z dogodki. GŠSV, šifra 804-034/681, z dne 30. 12. 1997.
52. Ukaz za organiziranje in izvajanje dežurstva v Slovenski vojski. PSSV, šifra 804-08-1/2005-12, z dne 25. 2. 2005.
53. Ukaz za izboljšanje varovanja objektov SV, PSSV, šifra 242-2/2006-4, z dne 18. 1. 2006.

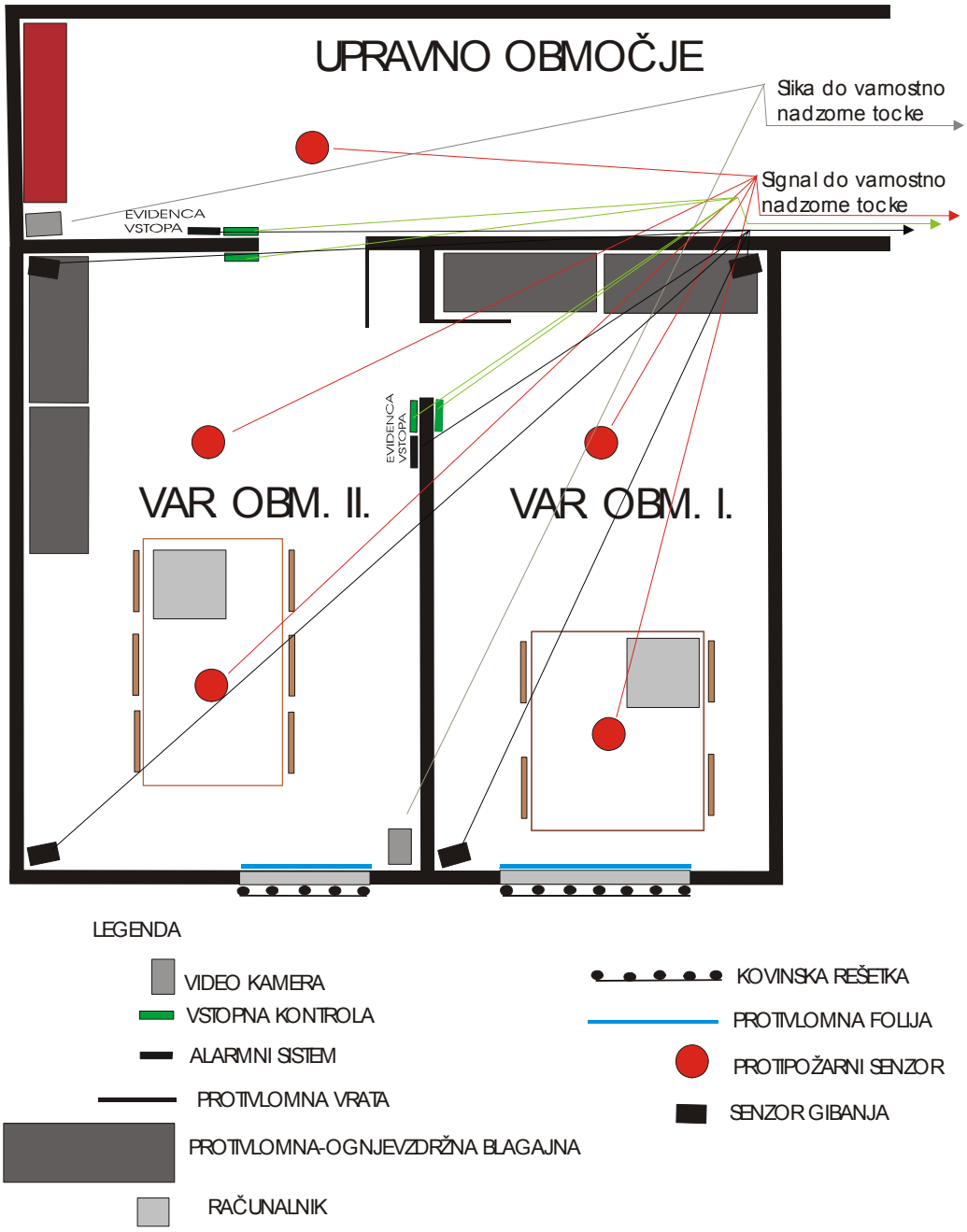
54. Ukaz za organiziranje in izvajanje varovanja objektov GŠSV. GŠSV, šifra SZ 854-03-1/01-84-398, z dne 2. 10. 2001.
55. Varnost v zvezi NATO. C-M (2002)49.
56. AJP-2 Skupna zavezniška obveščevalna, protiobveščevalna in varnostna doktrina. NATO, julij 2003.
57. AJP-2.2 Protiobveščevalni in varnostni postopki. NATO, november 2001.
58. ACE varnostna direktiva. NATO, AD 70-1, januar 1997.
59. APP-6 Nato Glosary of Terms and Definitions, 2003.
60. Dokument Severnoatlanskega sveta C-M 2002 49, 17. 6. 2002, str. 60–64.
61. Council Decision of March 19, 2001, adopting the Council's security regulations (2001/264/EC) s spremembami.
62. NATO, 2004. Security Risk Management Process, AC/35 (AHWG-SPG) WP(2004) 0010, Annex 1.
63. DoD Instruction 2000.16. DoD Antiterrorism Standards, 8. januar 2001.
64. DoD Directive 2000.12, DoD Antiterrorism/Force Protection Program, 13. april 1999.
65. DoD 0-2000.12-H, Protection of DoD Personnel and Activities Against of Terrorism and political Turbulence, 19. februar 1993.
66. DoD Instruction 5210.84, Security of DoD Personnel at U.S. Missions Abroad, 22. januar 1992.

9.4 INTERNETNI VIRI

1. Vlada Republike Slovenije, Urad za varovanje tajnih podatkov. Dostop na: http://www.uvtp.gov.si/si/delovna_podrocja/fizicna_varnost/ (22. januar 2007).
2. Vlada Republike Slovenije, Urad za varovanje tajnih podatkov. Dostop na: http://www.uvtp.gov.si/si/delovna_podrocja/fizicna_varnost/varnostno_obmocje/ (22. januar 2007).
3. Vlada Republike Slovenije, Urad za varovanje tajnih podatkov. Dostop na: http://www.uvtp.gov.si/si/delovna_podrocja/fizicna_varnost/nacrt_varovanja/ (22. januar 2007).
4. ITS Security Areas. Dostop na: http://www.google.com/search?q=%22term+security+area%22&hl=en&lr=&start=10sa=N (15. januar 2007).

5. Answers. Dostop na: http://www.answers.com/security&r=67 (15. januar 2007).
6. Vlada Republike Slovenije, Urad za varovanje tajnih podatkov. Dostop na: http:/www.uvtp.gov.si/index.php?id=705 (23. december 2006).
7. VTZ, d. o. o. Dostop na: http://www.vtz.si (3. januar 2007).
8. Varnost Maribor, d. o. o. Dostop na: http://www.varnost.si (3. januar 2007).
9. Sintal, d. d. Dostop na: http://www.sintal.si (4. januar 2007).
10. Četrta pot, d. o. o. Dostop na: http://www.cetrtapot.si (4. januar 2007).
11. Palsit, d. o. o. Dostop na: http://www.palsit.com/slo/izobrazevanje.php?c_id=2&v=course_list (9. januar 2007).

PREDLOG VZSPOSTAVITVE VARNOSTNIH OBMOČIJ



VAROVALNE OGRAJE

SV-A.1 Varovalna ograja brez nadgradnje in z možnostjo vgraditve elektronske zaščite:

Tip	Vrsta	Višina	mere mreže	Opomba
tip ograje	Varovalna ograja MO90103	2015 mm		razdalja med zemljo in najnižjo točko ograje 50 mm
tip mreže	Strojkovina		50 x 50 mm	
tip stebra	pokončni	2600 mm		

SV-A.2 Varovalna ograja z nadgradnjo in z možnostjo vgraditve elektronske zaščite:

Tip	Vrsta	Višina	mere mreže	Opomba
tip ograje	Varovalna ograja MO90103	3640 mm		razdalja med zemljo in najnižjo točko ograje 50 mm
tip mreže	Strojkovina		50 x 50 mm	
tip stebra	pokončni z V nastavkom	2500 mm		+ dolžina stebra v temelju
nadgradnja	ostrivci			

SV-A.3 Varovalna ograja z nadgradnjo in elektronsko zaščito:

Tip	Vrsta	Višina	mere mreže	Opomba
tip ograje	Varovalna ograja MO90103	3640 mm		razdalja med zemljo in najnižjo točko ograje 50 mm
tip mreže	Strojkovina		50 x 50 mm	
tip stebra	pokončni z V nastavkom	2500 mm		+ dolžina stebra v temelju
nadgradnja	ostrivci			

SV-A.4 Varovalna ograja z nadgradnjo in elektronsko zaščito:

Tip	Vrsta	Višina	mere mreže	Opomba
tip ograje	NEKSecurity	3640 mm		razdalja med zemljo in najnižjo točko ograje 50 mm
tip panela	Strojkovina		50 x 50 mm	
tip stebra	pokončni z V nastavkom	3100 mm		+ dolžina stebra v temelju
nadgradnja	ostrivci	1000mm		

SV-B.1 Varovalna ograja z nadgradnjo in elektronsko zaščito:

Tip	Vrsta	Višina	mera med latami	Opomba
tip ograje	MS-90103,V.1.0	2400 mm		razdalja med zemljo in najnižjo točko ograje 50 mm
tip polja	profil S355J2WP		70 mm	
tip stebra	2 x U profil	2600 mm		
nadgradnja	ostrivci	1000 mm		

SV-C.1 Žična varovalna ograja:

Tip	Vrsta	Višina	mere mreže	Opomba
tip ograje	BEKAERT Fortinet super	2010 mm		razdalja med zemljo in najnižjo točko ograje 50 mm
tip mreže	elektrovarjena mreža, pocinkana in plastificirana		50 x 50 mm	
tip stebra	pokončni pocinkani	2500 mm		

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
(glava enote/organizacije)

Datum:

POROČILO O OKVARI SISTEMOV TEHNIČNEGA VAROVANJA

ENOTA		
POOBLAŠČENEC		tel:
SKRBNIK		tel:

Lokacija	
Objekt	
Datum/ura nastanka okvare	
Kdo in kdaj je obveščen o nastanku okvare, datum/ura prijave okvare	
Datum/ura prihoda servisne službe	
Datum /čas odprave napake	
Skupen čas ovkare	
Vrsta alarmnega sistema	a.) sistem protivlomnega varovanja b.) sistem kontrole vstopa c.) sistem požarnega varovanja d.) sistem televizije zaprtega kroga e.) sistem senzorirane ograje
Kratek opis okvare	
Izvedeni ukrepi	
Poročilo izdelal	

Poslano:
- (POVC)
- (PSSV / G-2)

Način odprave:
- E-pošta/faks

Priloga D

TV-2
Priloga:
k mesečnemu poročilu (*XX)*

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
(glava enote/organizacij)

(datum)

MESEČNO POROČILO

o delovanju sistemov tehničnega varovanja za _____ (*leto)*
(mesec)

Enota /podenota	Objekt	Lokacija	Delovanje sistema	Opomba
			a.) brezhibno b.) v okvari c.) servisirano	
			a.) brezhibno b.) v okvari c.) servisirano	

Poročilo pripravil:_____
(čin, Ime in Priimek, tel.)

_____
(podpis NS-2)

Dodatek:
- delovni izkaz VTZ

OZNAČEVANJE VARNOSTNIH OBMOČIJ

Priloga 2: Označevanje varnostnih območij

(naziv organa ali organizacije)

OBMOČJE JE VAROVANO Z VIDEO NADZORNIM SISTEMOM.

◆

THE AREA IS EQUIPPED WITH THE VIDEO CONTROL PROTECTION.

Za dodatne informacije v zvezi z video nadzorom pokličite na telefonsko številko XXX.

Napisne table velikosti 300 x 210 mm

VSTOPATE V

VARNOSTNO OBMOČJE I. STOPNJE

IZVAJAJO SE PREDPISANI UKREPI.

ENTERING CLASS I SECURITY AREA

OBLIGATORY SAFETY PROCEDURES AND MEASURE ARE BEING CARRIED OUT.

VSTOPATE V

VARNOSTNO OBMOČJE II. STOPNJE

IZVAJAJO SE PREDPISANI UKREPI.

ENTERING CLASS II SECURITY AREA

OBLIGATORY SAFETY PROCEDURES AND MEASURE ARE BEING CARRIED OUT.

ozadje v rdeči barvi, napis bele barve

Napisni tablici ali nalepki velikosti 38 x 160 mm

ZAČASEN PREGLED
SLOVENSKIH STANDARDOV NA PODROČJU TEHNIČNIH SISTEMOV ZA VAROVANJE

	VLOM:
SIST BS 5979:2000	Code of practice for remote centres for alarm systems
SIST CLC/R 079-001:1997	Guidelines to achieving compliance with EC directives for alarm systems
SIST CLC/R 079-001:1999	Guidelines to achieving compliance with EC directives for alarm systems
SIST EN 50130-4:1997	Alarm systems - Part 4: Electromagnetic compatibility - Product safety standard: Immunity requirements for components of fire, intruder and social alarm systems
SIST EN 50130-4:1997/A1:1999	Alarm systems – Part 4: Electromagnetic compatibility – Product family standard: Immunity requirements for components of fire intruder and social alarm systems - Amendment 1
SIST EN 50130-4:2000	Alarm systems - Part 4: Electromagnetic compatibility - Product familiy standard: Immunity requirements for components of fire, intruder and social alarm systems
SIST EN 50130-5:2001	Alarm systems - Part 5: Environmental test methods
SIST EN 50131-1:1999	Alarm systems - Intrusion systems - Part 1: General requirements
SIST EN 50131-6:1999	Alarm systems - Intrusion systems - Part 6: Power supplies
SIST EN 50132-2-1:1999	Alarm systems - CCTV surveillance systems for use in security applications -- Part 2-1: Black and white cameras
SIST EN 50132-2-1:1999	Alarm systems - CCTV surveillance systems for use in security applications - Part 2-1: Black and white cameras
SIST EN 50132-4-1:2001	Alarm systems - CCTV surveillance systems for use in security applications - Part 4-1: Black and white monitors
SIST EN 50132-5:2001	Alarm systems - CCTV surveillance systems for use in security applications - Part 5: Video transmission
SIST EN 50132-7:1997	Alarm systems - CCTV surveillance systems for use in security applications - Part 7: Application guidelines
SIST EN 50133-1:1999	Alarm systems - Access control systems for use in security applications - Part 1: System requirements
SIST EN 50133-2-1:2001	Alarm systems - Access control systems for use in security applications - Part 2-1: General requirements for components
SIST EN 50133-7:2000	Alarm systems - Access control systems for use in security applications - Part 7: Application guidelines

SIST EN 50134-1:2003	Alarm systems - Social alarm systems -- Part 1: System requirements
SIST EN 50134-2:2000	Alarm systems - Social alarm systems - Part 2: Trigger devices
SIST EN 50134-3:2001	Alarm systems - Social alarm systems - Part 3: Local unit and controller
SIST EN 50134-7:1997	Alarm systems - Social alarm systems - Part 7: Application guidelines
SIST EN 50136-1-1:1999	Alarm systems - Alarm transmission systems and equipment - Part 1-1: General requirements for alarm transmission systems
SIST EN 50136-1-1:1999/A1:2001	Alarm systems - Alarm transmission systems and equipment - Part 1-1: General requirements for alarm transmission systems
SIST EN 50136-1-2:1999	Alarm transmission systems and equipment - Part 1-2: Requirements for systems using dedicated alarm paths
SIST EN 50136-1-3:1999	Alarm systems - Alarm transmission systems and equipment - Part 1-3: Requirements for systems with digital communicators using the public switched telephone network
SIST EN 50136-1-4:1999	Alarm systems - Alarm transmission systems and equipment - Part 1-4: Requirements for systems with voice communicators using the public switched telephone network
SIST EN 50136-2-1:1999	Alarm systems - Alarm transmission systems and equipment - Part 2-1: General requirements for alarm transmission equipment
SIST EN 50136-2-1:1999/A1:2001	Alarm systems - Alarm transmission systems and equipment - Part 2-1: General requirements for alarm transmission equipment - Amendment 1
SIST EN 50136-2-2:1999	Alarm systems - Alarm transmission systems and equipment - Part 2-2: Requirements for equipment used in systems using dedicated alarm paths
SIST EN 50136-2-3:1999	Alarm systems - Alarm transmission systems and equipment - Part 2-3: Requirements for equipment used in systems with digital communicators using the public switched telephone network
SIST EN 50136-2-4:1999	Alarm systems and equipment - Alarm transmission systems and equipment - Part 2-4: Requirements for equipment used in systems with voice communicators using the public switched telephone network
SIST ENV 50131-1:1997	Alarm systems - Intrusion systems - Part 1: General requirements
SIST IEC 60839-10-1:1999	Alarm systems - Part 10: Alarm systems for road vehicles - Section 1: Passenger cars
SIST IEC 60839-1-1:1995	Alarm systems - Part 1: General requirements - Section One: General
SIST IEC 60839-1-2:1995	Alarm systems - Part 1: General requirements - Section Two: Power units, test methods and performance criteria
SIST IEC 60839-1-3:1995	Alarm systems - Part 1: General requirements - Section Three: Environmental testing
SIST IEC 60839-1-4:1995	Alarm systems - Part 1: General requirements - Section Four: Code of practice
SIST IEC 60839-2-2:1995	Alarm systems - Part 2: Requirements for intruder alarm systems - Section Two: Requirements for detectors - General

SIST IEC 60839-2-3:1995	Alarm systems - Part 2: Requirements for intruder alarm systems - Section Three: Requirements for infrared beam interruption detectors in buildings
SIST IEC 60839-2-4:1995	Alarm systems - Part 2: Requirements for intruder alarm systems - Section Four: Ultrasonic doppler detectors for use in buildings
SIST IEC 60839-2-5:1995	Alarm systems - Part 2: Requirements for intruder alarm systems - Section Five: Microwave doppler detectors for use in buildings
SIST IEC 60839-2-6:1995	Alarm systems - Part 2: Requirements for intruder alarm systems - Section Six: Passive infra red detectors for use in buildings
SIST IEC 60839-2-7:1995	Alarm systems - Part 2: Requirements for intruder alarm systems - Section 7: Passive glass break detectors for use in buildings
SIST IEC 60839-5-1:1995	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 1: General requirements for systems
SIST IEC 60839-5-1:2002	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 1: General requirements for systems
SIST IEC 60839-5-2:1995	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 2: General requirements for equipment
SIST IEC 60839-5-2:2002	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 2: General requirements for equipment
SIST IEC 60839-5-4:1995	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 4: Alarm transmission systems using dedicated alarm transmission paths
SIST IEC 60839-5-4:2002	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 4: Alarm transmission systems using dedicated alarm transmission paths
SIST IEC 60839-5-5:1995	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 5: Requirements for digital communicator systems using the public switched telephone network
SIST IEC 60839-5-5:2002	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 5: Requirements for digital communicator systems using the public switched telephone network
SIST IEC 60839-5-6:1995	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 6: Requirements for voice communicator systems using the public switched telephone network
SIST IEC 60839-5-6:2002	Alarm systems - Part 5: Requirements for alarm transmission systems - Section 6: Requirements for voice communicator systems using the public switched telephone network
SIST IEC 60839-7-1:2002	Alarm systems - Part 7-1: Message formats and protocols for serial data interfaces in alarm transmission systems - General
SIST IEC 60839-7-2:2002	Alarm systems - Part 7-2: Message formats and protocols for serial data interfaces in alarm transmission systems - Common application layer protocol
SIST IEC 60839-7-3:2002	Alarm systems - Part 7-3: Message formats and protocols for serial data interfaces in alarm transmission systems - Common data link layer protocol
SIST IEC 60839-7-4:2002	Alarm systems - Part 7-4: Message formats and protocols for serial data interfaces in alarm transmission systems - Common transport layer protocol

SIST IEC 60839-7-5:2002	Alarm systems - Part 7-5: Message formats and protocols for serial data interfaces in alarm transmission systems - Alarm system interfaces employing a two-wire configuration in accordance with ISO/IEC 8482
	POŽAR:
SIST EN 54-1:2001	Odkrivanje in javljanje požara in alarmiranje - 1. del: Uvod
SIST EN 54-2:1997	Sistemi za odkrivanje in javljanje požara - 2. del: Oprema za kontrolo in indikacijo
SIST EN 54-2:1997/AC:2000	Sistemi za odkrivanje in javljanje požara ter alarmiranje – 2. del: Požarna centrala
SIST EN 54-3:2001	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 3. del: Naprave za alarmiranje - Zvočne naprave
SIST EN 54-3:2001/A1:2002	Sistemi za odkrivanje in javljanje požara ter alarmiranje – 3. del: Naprave za alarmiranje – Zvočne naprave
SIST EN 54-4:1997	Sistemi za odkrivanje in javljanje požara - 4. del: Oprema za napajanje
SIST EN 54-4:1997/A1:2003	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 4. del: Oprema za napajanje
SIST EN 54-4:1997/AC:2000	Sistemi za odkrivanje in javljanje požara ter alarmiranje – 4. del: Oprema za napajanje
SIST EN 54-5:2000/A1:2002	Sistemi za odkrivanje in javljanje požara ter alarmiranje – 5. del: Toplotni javljalniki – Točkovni javljalniki
SIST EN 54-5:2001	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 5. del: Toplotni javljalniki - Točkovni javljalniki
SIST EN 54-6:2001	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 6. del: Toplotni javljalniki - Termo točkovni javljalniki brez statičnega elementa
SIST EN 54-7:2000/A1:2002	Sistemi za odkrivanje in javljanje požara ter alarmiranje – 7. del: Dimni javljalniki - Točkovni javljalniki na principu sipanja svetlobe, prepuščene svetlobe ali ionizacije
SIST EN 54-7:2001	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 7. del: Dimni javljalniki -Točkovni javljalniki na principu sipanja svetlobe, prepuščene svetlobe ali ionizacije
SIST EN 54-8:2003	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 8. del: Termični javljalniki za visoke temperature
SIST EN 54-9:2003	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 9. del: Test občutljivosti na požar
SIST EN 54-10:2002	Odkrivanje in javljanje požara ter alarmiranje - 10. del: Plamenski javljalniki - Točkovni javljalniki
SIST EN 54-11:2001	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 11. del: Ročni javljalniki
SIST EN 54-12:2003	Sistemi za odkrivanje in javljanje požara ter alarmiranje - 12. del: Dimni javljalniki - Linijski javljalniki z optičnim žarkom
SIST EN 54-13:2003	Sistemi za odkrivanje in javljanje požara ter alarmiranje – 13. del: Sistemske zahteve in ugotavljanje združljivosti

SIST EN 54-14:2003	Sistemi za odkrivanje in javljanje požara ter alarmiranje – 14. del: Smernice za načrtovanje, projektiranje, vgradnjo, preverjanje, uporabo in vzdrževanje
SIST EN 54-xx: ???	Sistemi za odkrivanje in javljanje požara ter alarmiranje – xx. del: Oprema za požarno zaščito - Samozadostni dimni alarmi
SIST EN 54-17:2003	Sistemi za odkrivanje in javljanje požara ter alarmiranje – 17. del: Kratkostični ločilniki
DETEKCIJSKO MERJENJE EKSPOZIJSKIH SNOVI:	
SIST EN 50054:1997	Electrical apparatus for the detection and measurement of combustible gases - General requirements and test methods
SIST EN 50054:1997/A1:1997	Electrical apparatus for the detection and measurement of combustible gases - General requirements and test methods - Amendment 1
SIST EN 50054:2000	Electrical apparatus for the detection and measurement of combustible gases - General requirements and test methods
SIST EN 50055:1997	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for group I apparatus indicating up to 5 % (v/v) methane in air
SIST EN 50055:1997/A1:1997	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for group I apparatus indicating up to 5 % (v/v) methane in air - Amendment 1
SIST EN 50055:2000	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for Group I apparatus indicating up to 5 % (v/v) methane in air
SIST EN 50056:1997	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for group I apparatus indicating up to 100 % (v/v) methane in air
SIST EN 50056:1997/A1:1997	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for group I apparatus indicating up to 100 % (v/v) methane in air
SIST EN 50056:2000	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for Group I apparatus indicating up to 100 % (v/v) methane in air
SIST EN 50057:1997	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for group II apparatus indicating up to 100 % (v/v) lower explosive limit
SIST EN 50057:2000	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for Group II apparatus indicating up to 100 % lower explosive limit
SIST EN 50058:1997	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for group II apparatus indicating up to 100 % (v/v) gas
SIST EN 50058:2000	Electrical apparatus for the detection and measurement of combustible gases - Performance requirements for Group II apparatus indicating up to 100 % (v/v) gas
SIST EN 50059:2001	Specification for electrostatic hand-held spraying equipment for non-flammable material for painting and finishing

SIST EN 50073:2000	Guide for the selection, installation, use and maintenance of apparatus for the detection and measurement of combustible gases or oxygen
SIST EN 50104:2000	Electrical apparatus for the detection and measurement of oxygen - Performance requirements and test methods
SIST EN 50104:2002	Electrical apparatus for the detection and measurement of oxygen - Performance requirements and test methods
MEHANSKA ZAŠČITA: (ni popoln)	
SIST DIN 18251:1996	Ključavnice – Vdolbene stavbne ključavnice
SIST DIN 18257:1996	Stavbno okovje - Varnostno okovje - Pojmi, mere, zahteve, preskusi in označevanje
SIST EN 1047-1:1997	Varnostne shranjevalne enote - Klasifikacija in metode preskušanja požarne odpornosti - 1. del: Omare za zaščito nosilcev podatkov
SIST EN 1047-2:2000	Varnostne shranjevalne enote - Zahteve, klasifikacija in metode preskušanja požarne odpornosti - 2. del: Prostori in vsebniki za shranjevanje podatkov
SIST EN 1143-1:1998	Varnostne shranjevalne enote - Zahteve, klasifikacija in metode preskušanja protivlomne odpornosti - 1. del: Blagajne, vrata trezorskih prostorov in trezorski prostori
SIST EN 1143-1:1998/A1:2002	Varnostne shranjevalne enote - Zahteve, klasifikacija in metode preskušanja protivlomne odpornosti - 1. del: Blagajne, vrata trezorskih prostorov in trezorski prostori - Dodatek A1
SIST EN 1143-1:1998/A2:2002	Varnostne shranjevalne enote - Zahteve, klasifikacija in metode preskušanja protivlomne odpornosti - 1. del: Blagajne, vrata trezorskih prostorov in trezorski prostori - Dodatek A2
SIST EN 1143-2:2002	Varnostne shranjevalne enote - Zahteve, klasifikacija in metode preskušanja protivlomne odpornosti - 2. del: Depozitni sistemi
SIST ENV 1300:1999	Varnostne shranjevalne enote – Klasifikacija visoko varnostnih ključavnic po odpornosti proti nepooblaščenemu odpiranju

TABELARNI PRIKAZ OPREMLJENOSTI VARNOSTNIH OBMOČIJ

VARNOSTNI POSTOPKI	UPRAVNO OBMOČJE	VARNOSTNO OBMOČJE II. STOPNJE	VARONOSTNO OBMOČJE I. STOPNJE
označeno varnostno območje.	DA	DA	DA
zunanji zidovi varnostnega območja so iz armiranega betone 150 mm ali drugega materiala enake mehanske trdnosti.		DA	DA
notranji zidovi, ki mejijo na upravno območje so iz armiranega betona debeline 100 mm ali drugega materiala enake mehanske trdnosti.		DA	DA
protivlomna vrata.	DA*	DA	DA
slepa kljuka na obeh straneh protivlomnih vrat in protivlomna zaščita ključavnice.	DA	DA	DA
samodejno zapiralo na notranji strani protivlomnih vrat.	DA	DA	DA
kovinska rešetka na oknih do 5,5 m višine od tal.		DA	DA
zavarovane prezračevalne odprtine.		DA	DA
varovanje ključev blagajn v upravnem območju.		DA	DA
prostor za odlaganje elektronskih naprav in prtljage.		DA*	DA
detektorska vrata ali ročni detektor za odkrivanje orožja in kovin.			DA
osvetlitev dostopov do varnostnega območja.	DA	DA	DA
roloji, rolete na oknjih.	DA	DA	DA
protivlomna folija na okenskih steklih.		DA	DA
videodomofon na vhodu v	DA		

VARNOSTNI POSTOPKI	UPRAVNO OBMOČJE	VARNOSTNO OBMOČJE II. STOPNJE	VARONOSTNO OBMOČJE I. STOPNJE
objekt.			
vstopna kontrola.	DA	DA	DA
sistem za odkrivanje in javljanje nepooblaščene prisotnosti.	DA*	DA	DA
sistem za odkrivanje in javljanje požara.	DA*	DA	DA
videonadzor.		DA*	DA
neprekinjeno fizično varovanje.			DA
občasni fizični pregledi varnostnega območja.	DA	DA	
evidenca vstopov in izstopov.	DA	DA	DA
osebe v varnostnem območju morajo vidno nositi identifikacijsko izkaznico.	DA	DA	DA
prepovedan vnos mehanskih, elektronskih in magnetno optičnih sestavnih delov, s katerimi bi bilo mogoče nepooblaščeno posneti, odnesti ali prenesti tajne podatke.		DA*	DA
izključeni vsi mehanski, elektronski in magnetno optični sestavni deli, s katerimi bi bilo mogoče nepooblaščeno posneti, odnesti ali prenesti tajne podatke.		DA	
okrog varnostnega območja mora biti vzpostavljeno upravno območje.		DA	DA
vsa oprema v varnostnih območjih mora biti zavarovana (fotokopirni stroji, telefaksi, …).	DA	DA	DA
opravljen protiprisluškovalni pregled.		DA če se v varnostnem območju hranijo tajni podatki	DA
lesena ali kovinska omara.	DA		
blagajna, najmanj s stopnjo		DA	

VARNOSTNI POSTOPKI	UPRAVNO OBMOČJE	VARNOSTNO OBMOČJE II. STOPNJE	VARONOSTNO OBMOČJE I. STOPNJE
protivlomne varnosti II.			
blagajna, najmanj s stopnjo protivlomne varnosti III.			DA
Označena blagajna z nalepko stopnje tajnosti	DA	DA	DA
Elektronska ali mehanska ključavnica		DA	DA
Načrt varovanja tajnih podatkov		DA	DA

Opomba:

* - ni predpisano.

ZNANSTVENO POROČILO
O IZBIRI VAROVALNE/VARNOSTNE OGRAJE V SLOVENSKI VOJSKI

Drevo kriterijev

Kriterij	Opis
Varnostna ograja SV	Perimetralna zaščita oseb, sredstev in objektov SV
├**Tehnične lastnosti**	Zagotavljanje kvalitete ograje
├Konstrukcija	Zagotavljanje trdnosti, stabilnosti in kompaktnosti ograje
├Elektronika	Vgradnja ali namestitev elektronike v/na ograjo
├Nadgradnja	Namestitev nadgradnje z ostrivci
└Prilagojenost zemljišču	Postavitev ograje na različne naklone zemljišča
├**Funkcionalnost**	Ograja zagotavlja učinkovito varovanje
├Občutljivost	Na različne vremenske in druge vplive
├Spodkopavanje	Premagovanje varnostne ograje je mogoče pod ograjo
├Preplezanje	Premagovanje varnostne ogreje je mogoče nad ograjo
└Varnost	Elementi ograje so zavarovani proti poškodbam
├**Vzdrževanje**	Pripravljenost ograje za zagotavljanje učinkovite zaščite oseb, sredstev in o
├Rezervni deli	Zagotovitev rezervnih delov v obtimalnem času
└Odzivni čas	Odzivni čas servisne službe
└**Vrednost**	Cena ograje zagotavlja zadovoljivo kvaliteto
└Servisna ura	Cena servisiranja brez rezervnih delov

Zaloge vrednosti

Kriterij	Zaloga vrednosti
Varnostna ograja SV	**ne ustreza**; delno ustreza; ***ustreza***
├**Tehnične lastnosti**	**slabe**; zadovoljive; ***dobre***
├Konstrukcija	**slaba**; zadovoljiva; ***dobra***
├Elektronika	**ni mogoče**; delno mogoče; ***mogoče***
├Nadgradnja	**ni mogoče**; delno mogoče; ***mogoče***
└Prilagojenost zemljišču	**ni mogoče**; delno mogoče; ***mogoče***
├**Funkcionalnost**	**slabe**; zadovoljive; ***dobre***
├Občutljivost	**slaba**; zadovoljiva; ***dobra***
├Spodkopavanje	**velika**; srednja; ***mala***
├Preplezanje	**velika**; srednja; ***mala***
└Varnost	**ne ustreza**; delno ustreza; ***ustreza***
├**Vzdrževanje**	**slabo**; zadovoljivo; ***dobro***
├Rezervni deli	**slaba**; zadovoljiva; ***dobra***
└Odzivni čas	**velik**; srednji; ***kratek***
└**Vrednost**	**ne ustreza**; delno ustreza; ***ustreza***
└Servisna ura	**ne ustreza**; delno ustreza; ***ustreza***

Varnostna ograja SV

Perimetralna zaščita oseb, sredstev in objektov SV

1. **ne ustreza** Ograja ne ustreza kriterijem SV: ograja je visoka do 2,15 m, ne omogoča nadgradnje z ost
2. delno ustreza Ograja delno ustreza kriterijem SV:ograja je visoka 2,15 mm, omogoča nadgradnjo z ostri
3. ***ustreza*** Ograja v celoti ustreza kriterijem SV: ograja je visoka več kot 2, 25 m, nadgradnja z ostri

Tehnične lastnosti

Zagotavljanje kvalitete ograje

1. **slabe** Varnostna ograja je visoka do 2,15 m, ne omogoča nadgradnje z ostrivci, višina temelja je
2. zadovoljive Varnostna ograja je visoka 2, 15 m, omogoča delno nadgradnjo, temelj je visok 600 mm
3. ***dobre*** Varnostna ograja je visoka 2, 15 mm, omogoča nadgradnjo z ostrivci, temelj je visok 800 m

Konstrukcija

Zagotavljanje trdnosti, stabilnosti in kompaktnosti ograje

1. **slaba** Mrežni del ograje je visok do 2, 15 m, kvadrat mreže je večji od 50x50 mm, žica mreže je t
2. zadovoljiva Mrežni del ograje je visok 2,15 m, kvadrat mreže je 50x50 mm, žica je debeline 3 mm, bet
3. ***dobra*** Mrežni del ograje je višji od 2,15 m, kvadrat mreže je 50x50 mm, debilina žice je debelejša

Elektronika

Vgradnja ali namestitev elektronike v/na ograjo

1. **ni mogoče** Elektronike ni možno namestiti v/na ograjo
2. delno mogoče Elektroniko je možno namestiti na ograjo
3. ***mogoče*** Elektoniko je možno namestiti v konstrukcijo ograje

Nadgradnja

Namestitev nadgradnje z ostrivci

1. **ni mogoče** Nadgradnja ograje ni možna
2. delno mogoče Nadgradnja z ostrivci je nižja od 500 mm
3. ***mogoče*** Nadgradnja z ostrivci je visoka najmanj 500 mm in omogoča namestitev elektornike

Prilagojenost zemljišču

Postavitev ograje na različne naklone zemljišča

1. **ni mogoče** Ograjo je možno pastaviti samo na ravnem zemljišču
2. delno mogoče S predelavo ograje je možna postavitev na zemljišču z naklonom manjšimi od 25%
3. ***mogoče*** Ograjo je možno postaviti na naklonih, ki so večji od 25%

Funkcionalnost

Ograja zagotavlja učinkovito varovanje

1. **slabe** Ograja ne zagotavlja učinkovitega varovanja
2. zadovoljive Ograja zagotavlja delno učinkovito varovanje
3. ***dobre*** Ograja zagotavlja učinkovito varovanje

Občutljivost

Na različne vremenske in druge vplive

1. **slaba** Občutljivost na vremenske in druge vplive
2. zadovoljiva Občutljivost na druge vplive
3. ***dobra*** Ograja ni občutljiva na vremenske druge vplive

Spodkopavanje

Premagovanje varnostne ograje je mogoče pod ograjo

1. **velika** Spodkopavanje ograje je možno na globini 100 mm
2. srednja Spodkopavanje ograje je možno na globini 600 mm
3. ***mala*** Spodkopavanje je možno na globini 800 mm

Preplezanje

Premagovanje varnostne ogreje je mogoče nad ograjo

1. **velika** Ograjo je možno preplezati
2. srednja Ograjo je možno preplezati s pomagali
3. ***mala*** Ograje ni mogoče preplezati

Varnost

Elementi ograje so zavarovani proti poškodbam

1. **ne ustreza** Elementi ograje niso zavarovani
2. delno ustreza Elementi ograje so slabo zavarovani
3. ***ustreza*** Elementi ograje so zavarovani

Vzdrževanje

Pripravljenost ograje za zagotavljanje učinkovite zaščite oseb, sredstev in objektov

1. **slabo** Slabo vzdrževanje ne zagotavlja učinkovitega varovanja
2. zadovoljivo Delno vzdrževanje zagotavlja delno učinkovito varovanje
3. ***dobro*** Periodično vzdrževanje ograje in okolice zagotavlja učinkovito varovanje

Rezervni deli

Zagotovitev rezervnih delov v obtimalnem času

1. **slaba** Čas zagotovitve je več kot 14 dni
2. zadovoljiva Čas zagotovitve je več kot 7 dni
3. ***dobra*** Čas zagotovitve je več kot 24 ur

Odzivni čas

Odzivni čas servisne službe

1. **velik** Odzivni čas je več kot 12 ur
2. srednji Odzivni čas je več kot 6 ur
3. ***kratek*** Odzivni čas je do 6 ur

Vrednost

Cena ograje zagotavlja zadovoljivo kvaliteto

1. **ne ustreza** Cena ograje je previsoka glede na kvaliteto in lastnosti
2. delno ustreza Visoka varnost in učinkovitost ograje opravičuje visoko ceno
3. ***ustreza*** Cena ograje ustreza kvaliteti in lastnostim ograje

Servisna ura

Cena servisiranja brez rezervnih delov

1. **ne ustreza** Servisna ura je predraga
2. delno ustreza Cena servisne ure je delno sprejemljiva glede na kvaliteto dela
3. ***ustreza*** Cena servisne ure v popolnosti ustreza opravljenemu delu

Tabele odločitvenih pravil

	Tehnične lastnosti	Funkcionalnost	Vzdrževanje	Vrednost	Varnostna ograja SV
	25%	36%	32%	7%	
1	**slabe**	**slabe**	<=zadovoljivo	*	**ne ustreza**
2	**slabe**	<=zadovoljive	**slabo**	<=delno ustreza	**ne ustreza**
3	<=zadovoljive	**slabe**	**slabo**	*	**ne ustreza**
4	*	**slabe**	**slabo**	**ne ustreza**	**ne ustreza**
5	*	***dobre***	***dobro***	***ustreza***	***ustreza***
6	>=zadovoljive	***dobre***	***dobro***	*	***ustreza***
7	***dobre***	>=zadovoljive	***dobro***	>=delno ustreza	***ustreza***
8	***dobre***	***dobre***	>=zadovoljivo	*	***ustreza***

	Konstrukcija	Elektronika	Nadgradnja	Prilagojenost zemljišču	Tehnične lastnosti
	25%	25%	25%	25%	
1	**slaba**	**ni mogoče**	**ni mogoče**	*	**slabe**
2	**slaba**	**ni mogoče**	<=delno mogoče	<=delno mogoče	**slabe**
3	**slaba**	**ni mogoče**	*	**ni mogoče**	**slabe**
4	**slaba**	<=delno mogoče	**ni mogoče**	<=delno mogoče	**slabe**
5	**slaba**	<=delno mogoče	<=delno mogoče	**ni mogoče**	**slabe**
6	**slaba**	*	**ni mogoče**	**ni mogoče**	**slabe**
7	<=zadovoljiva	**ni mogoče**	**ni mogoče**	<=delno mogoče	**slabe**
8	<=zadovoljiva	**ni mogoče**	<=delno mogoče	**ni mogoče**	**slabe**
9	<=zadovoljiva	<=delno mogoče	**ni mogoče**	**ni mogoče**	**slabe**
10	*	**ni mogoče**	**ni mogoče**	**ni mogoče**	**slabe**
11	*	***mogoče***	***mogoče***	***mogoče***	***dobre***
12	>=zadovoljiva	>=delno mogoče	***mogoče***	***mogoče***	***dobre***
13	>=zadovoljiva	***mogoče***	>=delno mogoče	***mogoče***	***dobre***
14	>=zadovoljiva	***mogoče***	***mogoče***	>=delno mogoče	***dobre***
15	***dobra***	*	***mogoče***	***mogoče***	***dobre***
16	***dobra***	>=delno mogoče	>=delno mogoče	***mogoče***	***dobre***
17	***dobra***	>=delno mogoče	***mogoče***	>=delno mogoče	***dobre***
18	***dobra***	***mogoče***	*	***mogoče***	***dobre***
19	***dobra***	***mogoče***	>=delno mogoče	>=delno mogoče	***dobre***
20	***dobra***	***mogoče***	***mogoče***	*	***dobre***

	Občutljivost	Spodkopavanje	Preplezanje	Varnost	Funkcionalnost
	25%	25%	25%	25%	
1	**slaba**	**velika**	**velika**	*	**slabe**
2	**slaba**	**velika**	<=srednja	<=delno ustreza	**slabe**
3	**slaba**	**velika**	*	**ne ustreza**	**slabe**
4	**slaba**	<=srednja	**velika**	<=delno ustreza	**slabe**
5	**slaba**	<=srednja	<=srednja	**ne ustreza**	**slabe**
6	**slaba**	*	**velika**	**ne ustreza**	**slabe**
7	<=zadovoljiva	**velika**	**velika**	<=delno ustreza	**slabe**
8	<=zadovoljiva	**velika**	<=srednja	**ne ustreza**	**slabe**
9	<=zadovoljiva	<=srednja	**velika**	**ne ustreza**	**slabe**
10	*	**velika**	**velika**	**ne ustreza**	**slabe**
11	*	***mala***	***mala***	***ustreza***	***dobre***
12	>=zadovoljiva	>=srednja	***mala***	***ustreza***	***dobre***
13	>=zadovoljiva	***mala***	>=srednja	***ustreza***	***dobre***
14	>=zadovoljiva	***mala***	***mala***	>=delno ustreza	***dobre***
15	***dobra***	*	***mala***	***ustreza***	***dobre***
16	***dobra***	>=srednja	>=srednja	***ustreza***	***dobre***
17	***dobra***	>=srednja	***mala***	>=delno ustreza	***dobre***
18	***dobra***	***mala***	*	***ustreza***	***dobre***
19	***dobra***	***mala***	>=srednja	>=delno ustreza	***dobre***
20	***dobra***	***mala***	***mala***	*	***dobre***

	Rezervni deli	Odzivni čas	Vzdrževanje
	50%	50%	
1	**slaba**	<=srednji	**slabo**
2	<=zadovoljiva	**velik**	**slabo**
3	>=zadovoljiva	***kratek***	***dobro***
4	***dobra***	>=srednji	***dobro***

	Servisna ura	Vrednost
	100%	
1	**ne ustreza**	**ne ustreza**
2	***ustreza***	***ustreza***

Povprečne uteži

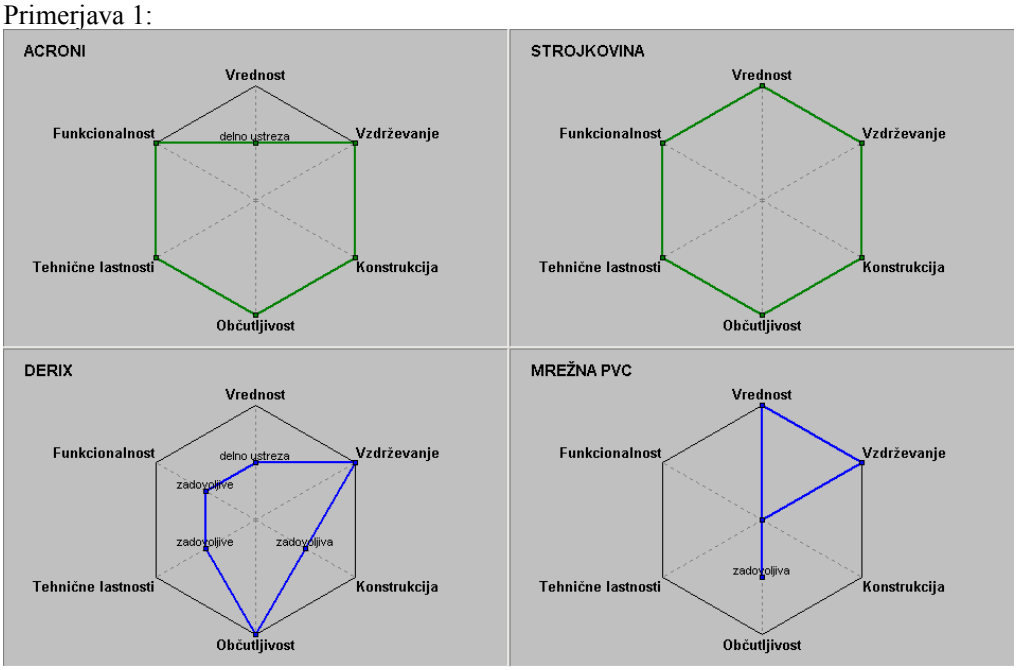
Kriterij	Lokalne	Globalne	Lok.norm.	Glob.norm.
Varnostna ograja SV				
├**Tehnične lastnosti**	25,0	25,0	25,0	25,0
│ ├Konstrukcija	25,0	6,3	25,0	6,3
│ ├Elektronika	25,0	6,3	25,0	6,3
│ ├Nadgradnja	25,0	6,2	25,0	6,2
│ └Prilagojenost zemljišču	25,0	6,2	25,0	6,2
├**Funkcionalnost**	35,7	35,7	35,7	35,7
│ ├Občutljivost	25,0	8,9	25,0	8,9
│ ├Spodkopavanje	25,0	8,9	25,0	8,9
│ ├Preplezanje	25,0	8,9	25,0	8,9
│ └Varnost	25,0	8,9	25,0	8,9
├**Vzdrževanje**	32,1	32,1	32,1	32,1
│ ├Rezervni deli	50,0	16,1	50,0	16,1
│ └Odzivni čas	50,0	16,1	50,0	16,1
└**Vrednost**	7,1	7,1	7,1	7,1
└Servisna ura	100,0	7,1	100,0	7,1

Rezultati vrednotenja

Kriterij	ACRONI	STROJKOVINA	DERIX	MREŽNA PVC
Varnostna ograja SV	***ustreza***	***ustreza***	delno ustreza	delno ustreza
├**Tehnične lastnosti**	***dobre***	***dobre***	zadovoljive	**slabe**
│ ├Konstrukcija	***dobra***	***dobra***	zadovoljiva	**slaba**
│ ├Elektronika	***mogoče***	***mogoče***	delno mogoče	**ni mogoče**
│ ├Nadgradnja	***mogoče***	***mogoče***	***mogoče***	**ni mogoče**
│ └Prilagojenost zemljišču	***mogoče***	delno mogoče	delno mogoče	***mogoče***
├**Funkcionalnost**	***dobre***	***dobre***	zadovoljive	**slabe**
│ ├Občutljivost	***dobra***	***dobra***	***dobra***	zadovoljiva
│ ├Spodkopavanje	***mala***	srednja	srednja	**velika**
│ ├Preplezanje	***mala***	srednja	srednja	**velika**
│ └Varnost	***ustreza***	***ustreza***	delno ustreza	**ne ustreza**
├**Vzdrževanje**	***dobro***	***dobro***	***dobro***	***dobro***
│ ├Rezervni deli	***dobra***	***dobra***	***dobra***	***dobra***
│ └Odzivni čas	srednji	***kratek***	srednji	srednji
└**Vrednost**	delno ustreza	***ustreza***	delno ustreza	***ustreza***
└Servisna ura	delno ustreza	***ustreza***	delno ustreza	***ustreza***

Primerjava grafov lastnosti različnih varovalnih ograj

Primerjava 1:



Primerjava 2: