

VARNOSTNA OBMOČJA

Projekt pri predmetu KITK 2

Mentor:
prof. dr. Aleksandar Jurišić

Gaja Velkavrh
63060248

Kazalo

1.UVOD.....	2
2.ZAKONODAJA.....	3
2.1.Uporabljeni izrazi v zakonu.....	3
2.2.Tipi zaupnosti podatkov.....	4
2.2.1.Stopnje tajnosti v EU in Nato.....	4
2.3.Dostop do tajnih podatkov.....	5
2.4.Varovanje tajnih podatkov.....	6
3.VARNOSTNO OBMOČJE.....	6
3.1.Izgradnja varnostnega območja.....	6
3.1.1.Zidovi.....	6
3.1.2.Protivlomna vrata.....	6
3.1.3.Okna.....	7
3.1.4.Prezračevanje.....	7
3.1.5.Blagajne.....	7
3.1.6.Blagajne za ključe ali sistem ključar.....	7
3.1.7.Rezalnik papirja.....	7
3.1.8.Prostor za odlaganje elektronskih naprav in prtljage.....	7
3.1.9.Detektorska vrata.....	8

3.1.10.Zunanja osvetlitev.....	8
3.1.11.Videonadzor in snemanje.....	8
3.1.12.Pristopna kontrola.....	8
3.1.13.Alarmni sistem.....	8
3.2.Varovanje tajnih podatkov – pravilnik.....	8
3.2.1.Splošni varnostni ukrepi.....	9
3.2.2.Varovanje oseb, ki imajo dostop do tajnih podatkov.....	9
3.2.3.Varovanje prostorov.....	10
3.2.4.Varovanje komunikacij, po katerih se prenašajo tajni podatki.....	10
3.2.5.Načini označevanja stopenj tajnosti.....	11
3.2.6.Varovanje opreme, s katero se obravnavajo tajni podatki.....	11
3.2.7.Izobraževanje uporabnikov z ukrepi in postopki varovanja tajnih podatkov	11
3.2.8.Kontrola in evidentiranje dostopov do tajnih podatkov.....	11
3.2.9.Kontrola in evidentiranje pošiljanja ter distribucije tajnih podatkov.....	11
3.3.Pridobitev dovoljenja za dostop do tajnih podatkov.....	12
3.3.1.Izdaja dovoljenja.....	12
3.3.2.Trajanje dovoljenj.....	12
3.3.3.Zavrnitev zahtevka.....	13
3.4.Primer Varnostnega območja.....	13
4.VARNA SOBA.....	15
4.1.Vrste varnih sob.....	15
4.2.Kaj je varna soba?.....	15
4.3.Varne sobe v Sloveniji.....	15
4.4.Načrt varne sobe.....	16
5.ZAKLJUČEK.....	17
6.LITERATURA.....	18
.....	18

1. UVOD

V Republiki Sloveniji (v nadaljevanju RS) za zakonodajo in varovanje tajnih podatkov skrbi Urad Vlade RS za varovanje tajnih podatkov (v nadaljevanju UVTP). Urad je bil ustanovljen leta 2002.

Čeprav varna soba ni neko novo področje, je na internetu zelo malo podatkov o gradnji in lokacijah. Vendar je dandanes varovanje informacij pri kriptografiji zelo pomembno.

V drugem poglavju Zakonodaja bom za začetek predstavila izraze, ki so uporabljeni v zakonu, nato stopnje zaupnosti podatkov, za konec pa še posameznike, ki imajo zaradi svoje funkcije omogočen dostop do tajnih podatkov.

Tretje poglavje Varnostno območje obsega podpoglavje o Izgradnji varnostnega območja, kjer je definirano kaj se lahko vgrajuje v varnostno območje in po katerem standardu. Poleg pravino zgrajenega varnostnega območja pa potrebujemo še interni Pravilnik, ki ga je potrebno priložiti na UVTP ob zahtevku za varnostno območje. V naslednjem podpoglavju je na kratko opisan postopek Kako pridobimo dovoljenja za dostop do tajnih podatkov. Za zaključek tretjega poglavja, pa sem si zamislila varnostno območje v velikosti 88 m².

Zadnje poglavje je namenjeno Varni sobi. Varna soba je soba v varnostnem območju, kjer v blagajnah hranimo tajne podatke. Tudi tu sem si za zaključek zamislila osnovno varno sobo (varnostno območje) v velikosti 6 m².

2. ZAKONODAJA

2.1. Uporabljeni izrazi v zakonu

- **tajni podatek** je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zavarovati pred nepoklicanimi osebami, in ki je označeno za tajno;
- **dokument** je vsak napisan, narisani, natisnjen, razmnožen, posnet, fotografiran, magneten, optičen ali kakšen drugačen zapis tajnega podatka;
- **medij** je vsako sredstvo, ki vsebuje tajne podatke;
- **določanje tajnih podatkov** je dejanje ali postopek, s katerim se podatek oceni za tajnega in se mu določi stopnja in rok tajnosti;
- **prenehanje tajnosti podatka** je zakonita sprememba tajnega podatka v podatek, ki je dostopen v skladu s splošnimi predpisi, ki urejajo poslovanje organa;
- **dostop** je seznanitev osebe s tajnim podatkom ali možnost osebe pridobiti tajni podatek na podlagi dovoljenja za dostop do tajnih podatkov;

- **varnostno preverjanje** osebe je poizvedba, ki jo pred izdajo dovoljenja za dostop do tajnih podatkov opravi 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;
- **obravnava tajnih podatkov** je določanje, označevanje, dostop do, uporaba, evidentiranje, razmnoževanje, posredovanje, prenos, uničevanje nosilcev tajnih podatkov, hramba, arhiviranje ter drugi ukrepi in postopki, s katerimi se zagotavlja njihova varnost.

2.2. Tipi zaupnosti podatkov

Stopnjo STROGO TAJNO lahko določi samo predsednik republike, predsednik državnega zbora, predsedniki komisije Državnega zbora RS za nadzor nad delom varnostnih in obveščevalnih služb, predsednik vlade, ministri, določeni vojaški poveljniki, določeni vodje diplomatsko-konzularnih predstavništev RS in pa predstojniki vladnih služb.

Ostale stopnje tajnosti podatka pa lahko določijo pooblaščen osebe ob njegovem nastanku oz. ob začetku izvajanja naloge organa, katere rezultat bo tajen podatek.

STOPNJE TAJNOSTI

- *STROGO TAJNO*: razkritje podatka bi ogrozilo vitalne interese RS ali jim nepopravljivo škodovalo
- *TAJNO*: razkritje podatka bi lahko hudo škodovalo varnosti ali interesom RS
- *ZAUPNO*: razkritje podatka bi lahko škodovalo varnosti ali interesom RS
- *INTERNO*: razkritje bi lahko škodovalo delovanju ali izvajanju nalog organa

Pooblaščen oseba mora tajne podatke stopnje tajnosti STROGO TAJNO pregledati enkrat letno, ostale stopnje tajnosti pa na tri leta in oceniti, ali še obstaja potreba po njihovi tajnosti.

2.2.1. Stopnje tajnosti v EU in Nato

Slovenija	EU	Nato
INTERNO	RESTREINT UE	NATO RESTRICTED
ZAUPNO	CONFIDENTIEL UE	NATO CONFIDENTAIL
TAJNO	SECRET UE	NATO SECRET
STROGO TAJNO	TOP SECRET UE	COSMIC TOP SECRET

2.3. Dostop do tajnih podatkov

V zvezi z opravljanjem svoje funkcije lahko do tajnih podatkov brez dovoljenj dostopajo: predsednik republike, predsednik vlade, poslanec, državni svetnik, župan in občinski svetnik, minister in predstojnik vladne službe, varuh človekovih pravic in

njegov namestnik, guverner, namestnik in vice guverner centralne banke, član računskega sodišča, sodnik, državni tožilec, generalni državni pravobranilec in informacijski pooblaščenec.

Te osebe dobijo dovoljenje z začetkom funkcije oziroma opravljanja dela in podpisom izjave, da so seznanjene z zakonom in drugimi predpisi, ki urejajo varovanje tajnih podatkov, in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi.

Dovoljenja za dostop ostalih oseb do tajnih podatkov izdajajo pristojni organi: Ministrstvo za notranje zadeve, Ministrstvo za obrambo, Slovenska obveščevalno-varnostna agencija in Policija.

2.4. Varovanje tajnih podatkov

Tajni podatki se hranijo v varnostnem območju, kjer sistem vhodnega nadzora zagotavlja popoln nadzor nad vstopom in izstopom vozil in oseb v to območje ter dovoljuje vstop samo osebam, ki imajo ustrezno dovoljenje. Vsi vstopi in izstopi pa so tudi evidentirani.

V varnostna območja je prepovedano vnašanje naprav, s katerimi bi bilo mogoče nepooblaščenoma posneti ali prenesti tajne podatke.

Zagotovljeno je neposredno in neprekinjeno fizično varovanje, lahko pa je tudi varovano le z alarmnim sistemom (intervencijski čas pa mora biti krajši od sedmih minut).

Varnostno območje mora biti jasno označeno in imeti redne protiprisluškovalne preglede. Podatki so shranjeni v blagajnah z ustrezno protivlomno zaščito. Nastavitve kombinacij elektronskih in mehanskih ključavnic se zamenjajo vsakih šest mesecev.

3. VARNOSTNO OBMOČJE

Varnostno območje je lahko I. ali II. stopnje. V varnostnem območju I. stopnje se obravnavajo podatki stopnje ZAUPNO ali višje stopnje tajnosti. V varnostnem območju II. stopnje pa se podatki stopnje ZAUPNO ali višje stopnje obravnavajo tako, da sam vstop in gibanje v tem območju, še ne omogoča dostop do teh podatkov.

3.1. Izgradnja varnostnega območja

Pri gradnji varnostnega območja se moramo držati Sklepa o določitvi pogojev za varnostno-tehnično opremo, ki se sme vgrajevati v varnostna območja. Sklep natančno določa kakšna vrata, okna, ključavnice,... se morajo vgrajevati v varnostna območja.

3.1.1. Zidovi

Armiran beton debeline vsaj 150 mm (lahko tudi drug material, a mora imeti enako mehansko trdnost). Če je varnostno območje v 2. nadstropju ali višje, mora biti debelina vsaj 100 mm.

Če so zidovi varnostnega območja hkrati tudi del zunanjih zidov objekta za katerim je prostor, ki ga organ ne nadzira ali opravlja, je potrebno nanj namestiti tipala alarmne naprave, ki zaznavajo tresenje in ustrezajo standardu SIST EN 50131 razreda 3.

3.1.2. Protivlomna vrata

Protivlomna vrata morajo imeti vsaj tritočkovno zaklepanje in ustrezati standardu SIST EN 1627 stopnje 4.

Zunanji del protivlomnih vrat mora imeti slepo kljuko in protivlomno zaščito ključavnice. Na protivlomnih vratih mora biti nameščen cilindrični vložek za ključavnico po standardu SIST EN 1303, ki mora ustrezati mehanski odpornosti stopnje 2.

Protivlomna vrata se z notranje strani opremijo s samodejnim zapiralom, ki zagotavlja, da se zapirajo za vsakim posameznim odpiranjem.

3.1.3. Okna

Kontaktni senzorji na oknih morajo ustrezati standardu SIST EN 50131 razreda 3 ali namesto tega okovje, ki omogoča zaklepanje.

Z notranje strani oken v pritličju ali kletnih prostorih varnostnega območja se mora vgradi kovinska zaščitna plošča debeline 2 mm z odprtinami 20 mm, ki preprečuje vnos ali iznos kakršnihkoli stvari ali predmetov.

Na okna varnostnega območja, ki mejijo na nenadzorovano površino, se do višine 5,5 m namestijo varnostne rešetke, tako, da so vzdane ali pritrjene z notranje strani oken. Izdelane morajo biti iz železnih elementov ali drugega materiala enake mehanske trdnosti premera najmanj 20 mm. Razmik med elementi rešetak ne sme biti večji od 150 mm.

Namesto varnostnih rešetak se steklene površine oken lahko izdelajo s protivlomnim steklom po standardu SIST EN 356 razreda P 8 B. Če je objekt zunanje fizično varovan, se lahko vgradi protivlomno steklo po standardu SIST EN 356 razreda P 6 B.

3.1.4. Prezračevanje

Površina s prezračevalnim oziroma klimatizacijskim sistemom povezanih odprtin za prezračevanje, ki sega iz varnostnega območja, ne sme biti večja od 200 cm². Če so odprtine za prezračevanje večje, je treba nanje namestiti varnostno rešetko, ki mora biti privarjena ali pritrjena z notranje strani, odprtine varnostne rešetke pa ne smejo biti večje od 200 cm².

Zunanji del klimatske naprave za zajem zraka in izpust vode mora biti ustrezno zavarovan tako, da se onemogočita nepooblaščen dostop do naprave in prenos zvoka iz varnostnega območja.

3.1.5. Blagajne

Tajni podatki stopnje tajnosti ZAUPNO in TAJNO se hranijo v blagajnah po standardu SIST EN 1143 ustrezne protivlomne stopnje.

Tajni podatki stopnje tajnosti STROGO TAJNO se hranijo v blagajnah po standardu SIST EN 1143 ustrezne protivlomne stopnje.

Na blagajnah mora biti nameščena elektronska ali mehanska ključavnica po standardu SIST EN 1300 razreda B.

3.1.6. Blagajne za ključke ali sistem ključar

Ključki varnostnega območja se hranijo v posebni blagajni po standardu SIST EN 1143 ustrezne protivlomne stopnje, ki mora biti nameščena v upravnem območju ali prostoru, ki je neprekinjeno fizično ali tehnično varovan.

Na blagajni mora biti nameščena elektronska ključavnica po standardu SIST EN 1300 razreda B.

Za shranjevanje ključev varnostnih območij se lahko namesto blagajn uporabi elektronski sistem za shranjevanje ključev (ključar) po standardu SIST EN 50131, ki mora biti nameščen v upravnem območju ali prostoru, ki je neprekinjeno fizično ali tehnično varovan.

3.1.7. Rezalnik papirja

Za uničevanje tajnih podatkov v papirni obliki se uporablja rezalnik papirja, ki zagotavlja razrez papirja velikosti 0,8 mm x 15 mm (vzdolžni in prečni razrez).

3.1.8. Prostor za odlaganje elektronskih naprav in prtljage

Ob vhodu v varnostno območje I. stopnje je treba namestiti omarice za shranjevanje mobilnih aparatov, torb ali kovčkov in drugih naprav, ki se v varnostno območje ne smejo vnašati.

3.1.9. Detektorska vrata

Nameščena morajo biti ob vhodu v varnostno območje I. stopnje. Namesto z detektorskimi vrati se pregledi lahko opravljajo z ročnimi detektorji. Če so detektorska vrata nameščena ob vhodu v objekt in osebo stalno spremljajo zaposleni, detektorskih vrat pred vhodom v I. varnostno območje ni treba nameščati.

3.1.10. Zunanja osvetlitev

Če se na objektu, v katerem je varnostno območje, namešča osvetlitev, je treba zagotoviti osvetljenost dostopov, vhodov in izhodov z najmanj 40 luksov. Osvetlitev objekta se lahko vključuje s senzorskim stikalom.

V objekt se lahko namesto tudi IR-reflektorje (za nočno osvetljevanje), če se opravlja videonadzor te vrste.

3.1.11. Videonadzor in snemanje

Če se namešča videonadzor, se namestijo visokoresolucijske kamere z najmanj 460 linij horizontalne resolucije. Videonadzor mora pokrivati vse vhode in izhode ter pripadajoči okoliš objekta.

Snemalna naprava nadzornega sistema mora biti nameščena v posebnem varovanem prostoru, do katerega imajo dostop samo za to pooblašene osebe.

Posnetki videonadzora se hranijo najmanj 60 dni. Do posnetkov imajo dostop samo za to pooblašene osebe

Za zunanji videonadzor je gostota posnetkov en posnetek na sekundo za vsako kamero, za notranji videonadzor pa dva posnetka na vsako kamero na sekundo. Kakovost posnetkov mora biti najmanj SVHS ali enakovreden drug format.

3.1.12. Pristopna kontrola

Če je na vhodu ali izhodu nameščen sistem pristopne kontrole, mora ustrezati standardu SIST EN 50133 razreda 3, kategorija pristopa B.

3.1.13. Alarmni sistem

Če se prostori opremijo s sistemom za samodejno zaznavanje gibanja oseb, se ta namesti v skladu s standardom SIST EN 50131 razreda 3 in mora biti vključen vedno, ko v prostoru ni pooblaščenih oseb.

Čas prenosa alarmnega signala, ki se mora prenašati po nadzorovani naročniški liniji od nastanka do prikaza alarma v varnostno-nadzornem centru, mora ustrezati standardu SIST EN 50136 razreda M 4.

Čas zaznave napake od nastanka do prikaza alarma v varnostno-nadzornem centru mora ustrezati standardu SIST EN 50136 razreda T 5.

3.2. Varovanje tajnih podatkov - pravilnik

Za hranjenje tajnih podatkov moramo tudi vnaprej pripraviti pravilnik, ki ga nato pošljemo vpogled na UVTP (Urad vlade RS za varovanje tajnih podatkov). Pri sestavi pravilnika moramo upoštevati naslednje oporne točke:

3.2.1. Splošni varnostni ukrepi

- implementacija potrebe po seznanitvi;
- dostop do tajnih podatkov je dovoljen le tistim osebam, ki morajo imeti vpogled v te podatke po svoji službeni dolžnosti zaradi izvajanja delovnih nalog / naročila / opravljanja funkcije;
- nihče ne sme dobiti tajnega podatka prej in v večjem obsegu, kot je to potrebno za opravljanje njegovih delovnih nalog ali funkcije;
- določitev delovnih mest, na katerih bodo imeli zaposleni, zaradi opravljanja funkcij ali izvajanja delovnih nalog, dostop do tajnih podatkov ali bodo seznanjeni z njihovo vsebino oziroma se bodo z njo lahko seznanili pri svojem delu;
- opredelitev dolžnosti varovanja tajnosti;
- opredelitev dolžnosti vseh zaposlenih upoštevati navedeni akt;
- med splošne varnostne ukrepe, kjer je to mogoče, spada npr. tudi določilo, da se obiskovalci v prostorih organizacije lahko gibljejo samo v spremstvu zaposlenega (leta npr. obiskovalca sprejme pri recepciji ipd). Ta ukrep je mogoče uvrstiti tudi v poglavje varovanja oseb;
- odgovornost presojanja varnostnega pomena podatkov in dolžnost predlagati njihovo ustrezno zaščito;

3.2.2. Varovanje oseb, ki imajo dostop do tajnih podatkov

- usposabljanje (osnovno, dodatno);
- posedovanje veljavnega dovoljenja za dostop do tajnih podatkov (stopnja tajnosti ZAUPNO in višje);
- imetnik dovoljenja za dostop je dolžan predstojnika organa obveščati o spremembah podatkov iz osnovnega in posebnega vprašalnika (določbe 25. d člena ZTP-ja);
- določitev odgovornih oseb (npr. 4. točka 35. b člena ZTP-ja, za notranji nadzor, ipd) ;

- vodenje evidence dovoljenj za dostop do tajnih podatkov;
- izvedba notranjega nadzora nad izvajanjem ZTP-ja in predpisov, sprejetih na njegovi podlagi;
- opredelitev odgovornosti zaradi kršitev ZTP-ja in podzakonski predpisov/tega akta (lahko se uvrsti tudi v kakšno drugo poglavje: npr. splošne/končne določbe ipd);

3.2.3. Varovanje prostorov

- obiski s spremstvom;
- določilo, kje se obravnavajo tajni podatki;
- pospravljene mize, zaprte omare ipd, v času, ko zaposleni niso na delovnem mestu;
- skrb, da v prisotnosti drugih oseb na mizah ni delovnih dokumentov oziroma preprečiti nepooblaščenim osebam vpogled v te dokumente;
- režim vstopanja in gibanja v upravnem/varnostnem območju (za zaposlene, obiskovalce, vzdrževalno osebje ipd);
- obveščanje ob sprožitvah alarmnega sistema;
- varovanje dokumentov in medijev, ki vsebujejo tajne podatke:
 - splošni varnostni ukrepi, ki so jih dolžni izvajati uslužbenci na svojih delovnih mestih (v času, ko niso na delovnem mestu, poskrbeti, da na mizah ni dokumentov s tajnimi podatki, da so odjavljeni s svojih računalnikov, blagajne, omare in predalniki pa zaklenjeni);
 - dolžnost obveščanja pooblaščenih oseb o ugotovljeni izgubi ali nepooblaščenem razkritju tajnih podatkov (40. člen ZTP-ja);
 - postopki ob izgubi, najdbi, nepooblaščenem razkritju tajnih podatkov;
 - način razmnoževanja (kopiranje, tiskanje, prevajanje ipd), določanja, uničevanja ipd tajnih podatkov;
 - vodenje evidence vpogledov iz katere je razvidno, kdaj in komu so bili podatki posredovani (vzpostavitev ažurnega pregleda in nadzora nad distribucijo tajnih podatkov);

3.2.4. Varovanje komunikacij, po katerih se prenašajo tajni podatki

- splošni ukrepi varovanja ključnih sestavin informacijskega sistema (fizični in organizacijski ukrepi varovanja);
- strojno in programsko opremo je dovoljeno uporabljati le za izvajanje delovnih nalog;
- poseg v sistem je dovoljen le z odobritvijo predstojnika;
- določitev osebe, odgovorne za izvajanje Uredbe o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih (Uradni list RS, št. 48/07) ter upravljanje in nadzor nad ukrepi in postopki varovanja tajnih podatkov v sistemu;

- splošni tehnični ukrepi in postopki varovanja sistema;
- prepoved posredovanja lastnega gesla ali omogočanje uporabe informacijskega sistema drugi osebi;

3.2.5. Načini označevanja stopenj tajnosti

- pooblaščen osebe za določanje tajnih podatkov opredeljuje 10. člen ZTP-ja, način označevanja pa predpisuje Uredba o varovanju tajnih podatkov (organizacije imajo odgovornost varnostnega presojanja pomena podatkov in pravico predlagati pooblaščenim osebam organov ustrezno zavarovanje podatkov (določitev podatkov za tajne));
- nekatere organizacije se odločijo za vzporeden postopek varovanja poslovnih skrivnosti (v skladu z določili Zakona o gospodarskih družbah) – svoje poslovne skrivnosti bodo ščitile na enak način kot tajne podatke; v tem primeru lahko v navedenem poglavju opredelijo način označevanja dokumentov, opredeljenih kot poslovna skrivnost;
- ne glede na določila prve alineje, je smiselno razmisliti o koristnosti vzorcev dokumentov s tajnimi podatki (npr. v prilogah akta), z namenom, da zaposleni znajo prepoznati tajne podatke v papirni obliki;

3.2.6. Varovanje opreme, s katero se obravnavajo tajni podatki

- način varovanja ključnih in nekaterih drugih sestavin sistema (II. poglavje Uredbe o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih (Uradni list RS, št. 48/07));
- implementacija drugih določb navede uredbe;

3.2.7. Izobraževanje uporabnikov z ukrepi in postopki varovanja tajnih podatkov

Izobraževanja nudijo nekatera za to klasificirana podjetja in tudi UVTP. Izobraževanja je priporočljivo izvajati vsaj enkrat letno.

3.2.8. Kontrola in evidentiranje dostopov do tajnih podatkov

- kombinacije elektronskih ključavnic na blagajnah, v katerih se hranijo tajni podatki, lahko poznajo samo pooblašчени uslužbenci (število oseb, ki so seznanjene s kombinacijami mora biti čim manjše);
- vodenje evidence posegov, ki se nanašajo na blagajno (servis, menjava šifer, ipd);
- varovanje ključev (ponekod je, iz varnostnih razlogov, podroben opis varovanja ključev, bolj smiselno urediti v načrtu varovanja);

3.2.9. Kontrola in evidentiranje pošiljanja ter distribucije tajnih podatkov

- določba kje se sprejemajo nosilci tajnih podatkov in kdo jih sprejema ter na kakšen način (podroben opis postopka, ki je odvisen od siceršnjega dokumentarnega

poslovanja oziroma od načina ureditve le-tega v skladu s potrebami in zahtevami pristojnega organa);

- evidentiranje tajnih podatkov;
- evidentiranje vsakega iznosa/vnosa nosilca tajnega podatka stopnje tajnosti ZAUPNO ali višje izven varnostnega območja;
- način prenosa tajnih podatkov;

3.3. Pridobitev dovoljenja za dostop do tajnih podatkov

Dovoljenja za dostop do tajnih podatkov stopenj ZAUPNO, TAJNO ali STROGO TAJNO izdaja Ministrstvo za notranje zadeve, Ministrstvo za obrambo, SOVA in Policija.

Pristojni organ opravi preverjanje:

- Osnovno varnostno preverjanje (tajni podatki stopnje ZAUPNO)
- Razširjeno varnostno preverjanje (tajni podatki stopnje TAJNO)
- Razširjeno varnostno preverjanje z varnostnim poizvedovanjem (tajni podatki stopnje STROGO TAJNO)

3.3.1. Izdaja dovoljenja

Postopek izdaje dovoljenja se začne na pisni predlog predlagatelja (predstojnik organa) za osebo, ki jo je treba preveriti (preverjena oseba).

Predlog mora vsebovati:

- podatke o stopnji tajnosti podatkov, za katere je bil predlog podan;
- pisno soglasje preverjene osebe za varnostno preverjanje
- dokazilo o opravljenem usposabljanju s področja obravnavanja tajnih podatkov
- pisno izjavo o seznanitvi z Zakonom o tajnih podatkih
- zaprto ovojnico z izpolnjenim varnostnim vprašalnikom preverjene osebe

Med postopkom varnostnega preverjanja lahko predlagatelj predlaga spremembo stopnje tajnosti, za katero je bil predlog podan. Če je predlagana stopnja višja, je potrebno zahtevku priložiti:

- izpolnjen ustrezeni varnostni vprašalnik
- pisno soglasje preverjene osebe, da soglaša s spremenjenim obsegom varnostnega preverjanja
- Če preverjena oseba, med postopkom preverjanja, dostopa do tajnih podatkov ne potrebuje več, predlagatelj umakne zahtevek.
- Predlagatelj mora ves čas postopka sodelovati s pristojnimi organi, saj se v nasprotnem primeru njegov molk šteje za umik predloga.
- Pristojni organ mora o zahtevi za izdajo dovoljenja odločiti najpozneje v treh mesecih od dneva, ko je prejel popolno vlogo.

3.3.2. Trajanje dovoljenj

Dovoljenje za dostop do tajnih podatkov stopnje ZAUPNO se izda za deset let. Dovoljenja za dostop do tajnih podatkov stopnje TAJNO in STROGO TAJNO pa le za dobo petih let.

3.3.3. Zavrnitev zahtevka

Če pristojni organ na podlagi zbranih podatkov oceni, da obstaja varnostni zadržek, izdajo dovoljenja zavrne. V zavrnitvi pa mu ni potrebno obrazložiti virov varnostnega preverjanja.

Varnostni zadržek je lahko:

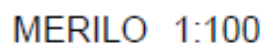
- Lažne navedbe podatkov v vprašalniku ali v razgovoru
- Neizbrisane pravnomočne obsodbe na najmanj tri mesece nepogojne zaporne kazni
- dokončen disciplinski ukrep zaradi težje disciplinske kršitve s področja obravnavanja in varovanja tajnih podatkov
- odvisnost od alkohola, drog oziroma druge zasvojenosti, ki bi lahko vplivale na zavrnitev izdaje dovoljenja
- članstvo ali sodelovanje v organizacijah ali skupinah, ki ogrožajo vitalne interese Republike Slovenije ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je Republika Slovenija
- Pristojni organ lahko izdajo dovoljenja zavrne tudi v primeru:
- pravnomočne obtožnice za kazniva dejanja, ki se preganjajo po uradni dolžnosti, razen za kazniva dejanja, kjer je kot glavna kazen predpisana denarna kazen ali zapor do treh let
- nepravnomočne obsodilne sodbe za kazniva dejanja, ki se preganjajo po uradni dolžnosti, in za katera je kot glavna kazen predpisana denarna kazen ali zapor do treh let
- neizbrisane pravnomočne obsodbe ali več izrečenih glob za prekrške, določene s tem zakonom;
- drugih ugotovitev varnostnega preverjanja, ki vzbujajo utemeljene dvome v posameznikovo verodostojnost, zanesljivost in lojalnost za varno obravnavanje tajnih podatkov;
- drugih varnostnih zadržkov, določenih z zakoni ali mednarodnimi pogodbami.
- Zoper odločbo pritožba ni dovoljena, dovoljen pa je upravni spor, ki ga lahko sproži predlagatelj ali preverjena oseba.

3.4. Primer Varnostnega območja

Na sliki je območje razdeljeno na dva dela: upravno in varnostno območje. Razlika med tema dvema območjema je v stopnji varnosti, ki jo želimo zagotoviti. V upravnem območju se lahko giblje več ljudi, v varnostnem območju pa samo tisti z dovoljenjem za dostop in posamezniki v spremstvu osebe, ki ima dovoljenje za dostop.

Na spodnjem primeru sem namenoma izpustila okna, saj se mi zdi, da so okna v varnostnem območju neuporabna, saj imamo ločeno prezračevanje in tudi svojo osvetlitev. Če bi hoteli vključiti še okna pa bi morali upoštevati tudi dodatne zahteve, kar pa bi nam še zvišalo stroške, poleg tega pa je priporočljivo, da je območje na sredini stavbe ali pa v kletnih prostorih. V kletnih prostorih pa moramo paziti tudi na možnost poplav, zato morajo biti na stenah nameščeni senzorji za vodo. V primeru

Varnostno območje na sliki spodaj je veliko $8 \times 11 \text{ m}^2 = 88 \text{ m}^2$. Od tega ima varna soba 12 m^2 , sejna soba v varnostnem območju 22 m^2 , oba vhoda po 6 m^2 , soba s strežniki 16 m^2 in tiha soba ali laboratorij 26 m^2 . V prvem prostoru ob vstopu v upravno območje so police, na katerih so natisnjene izjave v slovenskem in angleškem jeziku za spremljevalce, ki jih morajo podpisati. Police in omare v vhodu v varnostno območje pa so namenjene za odložišče vseh elektronskih naprav, ki jih v varno sobo ne smemo odnesti (mobitel, fotoaparat, ...).



4. VARNA SOBA

4.1. Vrste varnih sob

Poznamo 3 vrste varnih sob:

- a) Za hrambo podatkov (varna pred požarom, vdorom vode, ...)
- b) Pred naravnimi katastrofami (tornado, hurikani)
- c) Za lastno varnost (možnost preživetja tudi do 30 dni)

V tej seminarski nalogi se bom skoncentrirala na varne sobe tipa a).

4.2. Kaj je varna soba?

Že iz imena lahko sklepamo, da je varna. Obdajajo jo močne, debele stene in protivlomna vrata. Namenjena je predvsem varovanju nečesa, pa naj bodo to tajni podatki ali pa ljudi ob naravnih in drugih nesrečah.

Varno sobo potrebujemo za izdelovanje kripto naprav, hrambo CA master ključev,... Več v prosojnicah KITK2.

Varnostno območje je celo območje, kjer zagotavljamo zgoraj že omenjeno varovanje, varna soba pa je del varnostnega območja, kjer imamo v blagajnah shranjene tajne podatke.

4.3. Varne sobe v Sloveniji

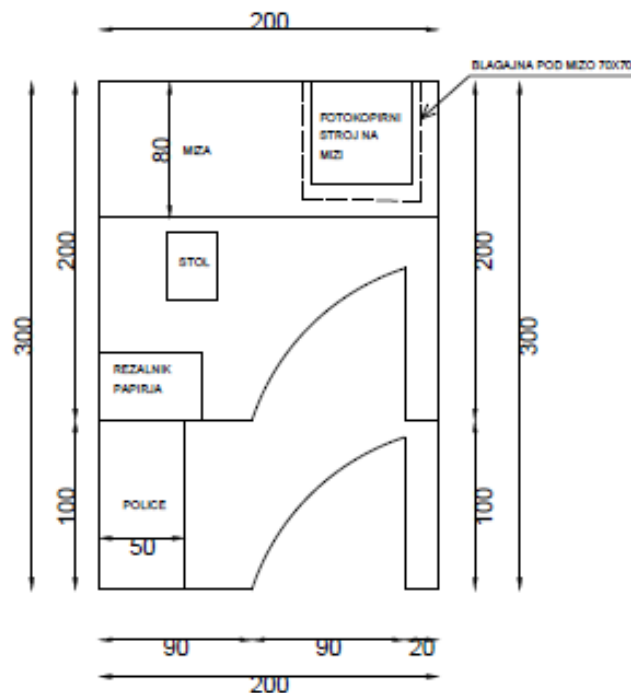
Točno število varnih sob v Sloveniji ni javno, saj je neznana lokacija velika prednost pri varovanju le te. Sigurno pa te podatke imajo na UVTP.

Podatki niso preverjeni, lahko pa z gotovostjo predvidevamo, da imajo varno sobo certifikatne agencije (Pošta, Halcom), Telekom, Banke (NLB) in državni organi (MNZ, MORS, SOVA, MZZ, Vlada).

4.4. Načrt varne sobe

Na spodnji sliki je načrt osnovne varne sobe oz. varnostnega območja, ki pa še vseeno pokrije vse najpomembnejše funkcije varnostnega območja. Vendar, ker je to celotno območje zelo majhno, bi mu lahko rekli le varna soba.

Celotno območje obsega 6 m², od tega varna soba 4 m². Police ob vhodu so namenjene za odlaganje vseh elektronskih naprav. Varna soba je predvidena za eno osebo, v sobi je pod mizo blagajna, na mizi pa fotokopirni stroj, v kotu pa še rezalnik papirja.



MERILO 1:200

5. ZAKLJUČEK

Videli smo dva načrta varnostnega območja, katerega želimo vgraditi pa je odvisno, za kaj ga potrebujemo in koliko denarja za tako investicijo imamo. Varnostno območje bi lahko na naši fakulteti (op. Fakulteta za računalništvo in informatiko) uporabljali za konkretne projekte, ki zahtevajo dostop do tajnih podatkov ali pa tudi za izobraževalne namene.

Kot smo omenili že zgoraj, mora biti varnostno območje tudi pod stalnim video nadzorom. Tu pa se zastavi že zelo znano vprašanje: »Kdo pa nadzira nadzornike?«

Za konec pa sem dolžna še zahvalo direktorju podjetja MIŠKA (FMC Group), g. Boštjanu Gruden, ki mi je za namene tega projekta razkazal njihovo varnostno območje in ga. Maji Rožaj, podsekretarki na UVTP, za podatke o izobraževanju, pravilnikih in še čem.

LITERATURA

- Spletna stran: Uradni list RS – zakoni:
 - Zakon o tajnih podatkih (<http://www.uradni-list.si/1/content?id=73346>)
 - Uredba o varovanju tajnih podatkov (<http://www.uradni-list.si/1/content?id=57489>)
 - Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade RS za varovanje tajnih podatkov (<http://www.uradni-list.si/1/content?id=21439>)
 - Sklep o določitvi pogojev za varnostno-tehnično opremo, ki se sme vgrajevati v varnostna območja (<http://www.uradni-list.si/1/content?id=75298>)
- Spletna stran: Organizacija vlade RS za varovanje tajnih podatkov (<http://www.uvtp.gov.si/si/>)
- Jurišić, A. in Golob, M. **Napredne metode varovanja podatkov in kriptografija**. Bilten: junij 2007, letnik 23, številka 2
- Ega, M. in Mather, T. **Varovanje informacij (grožnje, izzivi in rešitve)**. 1. izdaja Ljubljana: Založba Pasadena d.o.o., 2005
- Slolve J. D. **The future of reputation (gossip, rumor and privacy on the internet)**. Yale University Press, 2007
- Prosojnice pri predmetu KITK2

PRILOGA 1: Varnostni vprašalnik

PRILOGA 2: Načrt varnostnega območja