


APSTIPRINU
Satversmes aizsardzības biroja direktors


2004.gada 22. jūlijā.

Noteiktas saskaņā ar Ministru kabineta 06.01.2004.
noteikumu nr.21 "Valsts noslēpuma, Ziemeļatlantijas līguma
organizācijas, Eiropas Savienības un ārvalstu institūciju klasificētās
informācijas aizsardzības noteikumi" 26.11.punktu.

**Signalizācijas iekārtu drošības prasības, ar kurām aprīko telpas,
kurās uzglabā valsts noslēpuma objektus, NATO un
Eiropas Savienības klasificēto informāciju.**

1. Nacionālās drošības iestāde rekomendē institūcijām telpas, kurās tiks uzglabāti valsts noslēpuma objekti, NATO un Eiropas Savienības klasificēta informācija, aprīkojot ar signalizācijas iekārtām, izvēlēties uzņēmumus, kuri pārstāv šo iekārtu ražotājus un var atbildēt par to projektēšanu, ierīkošanu, nodošanu, un apkopi.

2. Ja signalizācijas sistēmas ierīkošanu un apkopi apakšlīguma ietvaros veic cits uzņēmums, ražotāja pārstāvis ir atbildīgs par iekārtu darbību uz līgumā paredzēto laiku.

3. Signalizācijas sistēmām tiek piešķirta kopējā aizsardzības spēja pamatojoties uz šādiem parametriem:

- 3.1. "authorisation" (tiesības ieiet telpā);
- 3.2. "access levels" (pieejamības pakāpes);
- 3.3. "operations" (darbības veids);
- 3.4. "processing" (informācijas apstrāde);
- 3.5. "detection" (atklāšanas veids);
- 3.6. "notification" (paziņojums par ielaušanos vai sistēmas bojājumu);
- 3.7. "power supply" (elektropiegādes drošība);
- 3.8. "tamper security" (spēja sistēmu neitralizēt);
- 3.9. "monitoring of interconnections" (savienojumu kontroles iespēja, ja savienotas vairākas sistēmas);
- 3.10. "event recording" (kā tiek konstatēta personas nonākšana sistēmā).

4. Signalizācijas sistēmu aizsardzība saskaņā ar Eiropas Savienības standarta EN 50133-1 prasībām tiek noteikta 4 pakāpēs:

- 4.1. "Zemu riska aizsardzība", ja iespējamai personai, kura vēlas piekļūt valsts noslēpuma objektiem, NATO un Eiropas Savienības klasificētai informācijai (turpmāk- persona) ir ierobežotas zināšanas par signalizācijas sistēmām un ierobežoti darba instrumenti;
- 4.2. "Zema līdz vidēja riska aizsardzībai"- personai ir ierobežotas zināšanas par signalizācijas iekārtām un vispārēja līmeņa darba instrumenti;

4.3. "Vidēja līdz augsta riska aizsardzībai"- persona labi pazīst signalizācijas sistēmas, tai pilns darba instrumentu komplekts un pārnēsājama tehnika;

4.4. "Augstu riska aizsardzībai"- persona var precīzi plānot iespējamo ielaušanos, tai ir specializēti darba instrumenti un zināšanas, kā neitralizēt signalizācijas sistēmu darbību.

5. Nacionālā drošības iestāde nosaka, ka glabātuves, kurās tiek uzglabāti valsts noslēpuma objekti, NATO un Eiropas Savienības klasificētā informācija, ir pakļautas "zemā līdz vidējam riskam" un jāaprīko ar otrās pakāpes signalizācijas sistēmām.

6. Nacionālā drošības iestāde nosaka minimālās signalizācijas sistēmu drošības prasības. Institūcijas atkarībā no konkrētās situācijas var iegādāties arī augstākas pakāpes sistēmas.

7. Signalizācijas sistēmai ir jābūt savienotai ar apsardzes posteni, kas patstāvīgi var pārbaudīt sistēmas darbotiespēju un reaģēt uz nepamatotu tās iedarbošanos.

8. 3.punktā minētie parametri ir noteikti 4 pakāpēs. Katram parametram ir vairāki kvalitatīvi līmeņi (kategorijas), tāpēc signalizācijas sistēmas var piemērot konkrētu institūciju vajadzībām, nepieciešamības gadījumā nosakot atsevišķa parametra līmeni (kategoriju) augstāku kā noteiktās pakāpes signalizācijas sistēmai.

9. Lai institūcijas varētu nodrošināt, ka paredzētā signalizācijas sistēma atbilst noteiktajām drošības prasībām un piemērot konkrētiem apstākļiem, Nacionālās drošības iestādē ir iespējams iepazīties ar standarta prasībām vai saņemt standarta EN-50133-1 kopiju latviešu vai angļu valodā.