



Laidiens: 15.02.2011., Nr. 25

Ministru kabineta noteikumi Nr.100

Rīgā 2011.gada 1.februārī (prot. Nr.7 18.§)

Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība

Izdoti saskaņā ar Informācijas tehnoloģiju drošības likuma 3.panta trešo daļu

I. Vispārīgie jautājumi

1. Noteikumi nosaka informācijas tehnoloģiju kritiskās infrastruktūras (turpmāk – kritiskā infrastruktūra) drošības pasākumu plānošanas un īstenošanas kārtību.
2. Kritisko infrastruktūru apzina un nosaka kritisko infrastruktūru reglamentējošos normatīvajos aktos paredzētajā kārtībā.

II. Kritiskās infrastruktūras drošības pasākumu plānošanas kārtība

3. Satversmes aizsardzības birojs informē kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju par to informācijas tehnoloģiju iekļaušanu kritiskās infrastruktūras kopumā.
4. Kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs norīko par kritiskās infrastruktūras drošību atbildīgo personu. Par kritiskās infrastruktūras drošību nedrīkst būt atbildīga persona:
 - 4.1. kura nav pilngadīga vai nav Latvijas pilsonis;
 - 4.2. kura ir sodīta par tīšu noziedzīgu nodarījumu;
 - 4.3. kura ir notiesāta par tīšu noziedzīgu nodarījumu, atbrīvojot no soda;
 - 4.4. kura ir saukta pie kriminālatbildības par tīša noziedzīga nodarījuma izdarīšanu, izņemot gadījumu, ja kriminālprocess pret to izbeigts uz rehabilitējoša pamata;
 - 4.5. kura ir atzīta par rīcībnespējīgu likumā noteiktajā kārtībā;
 - 4.6. kura ir vai ir bijusi PSRS, Latvijas PSR vai kādas ārvalsts drošības dienesta štata vai ārštata darbinieks, aģents, rezidents vai konspiratīvā dzīvokļa turētājs;
 - 4.7. kura ir vai ir bijusi ar Latvijas Republikas likumiem, Augstākās Padomes lēmumiem vai tiesas nolēmumiem aizliegto organizāciju dalībnieks (biedrs) pēc šo organizāciju aizliegšanas;
 - 4.8. kurai ir diagnosticēti psihiski traucējumi vai alkohola, narkotisko, psihotropo vai toksisko vielu atkarība;
 - 4.9. kura saskaņā ar valsts drošības iestādes vai Valsts policijas rīcībā esošajām ziņām pieder pie organizētās noziedzības grupējuma, nelikumīga militarizēta vai bruņota formējuma, kā arī pie nevalstiskās organizācijas vai

nevalstisko organizāciju apvienības, kas uzsākusi darbību (juridisko) pirms tās reģistrācijas vai turpina darboties pēc tam, kad tās darbība ir apturēta vai izbeigta ar tiesas nolēmumu.

5. Satversmes aizsardzības birojs pārbauda un apstiprina par kritiskās infrastruktūras drošību atbildīgās personas atbilstību šo noteikumu 4.punktā minētajām prasībām.

6. Satversmes aizsardzības birojs var pārbaudīt ar kritiskās infrastruktūras darbības nodrošināšanu saistītos darbiniekus, kuriem ir pieeja nozīmīgai kritiskās infrastruktūras informācijai vai tehnoloģiskajām iekārtām, un izvērtēt informāciju attiecībā uz personas sodāmību par tišu noziedzīgu nodarījumu un faktiem, kas dod pamatu apšaubīt tās spēju saglabāt ierobežotas pieejamības un klasificētu informāciju. Pamatojoties uz pārbaudes rezultātiem, Satversmes aizsardzības birojs sniedz ieteikumus kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam.

7. Par kritiskās infrastruktūras drošību atbildīgā persona:

7.1. plāno kritiskās infrastruktūras drošības pasākumus;

7.2. sadarbībā ar Satversmes aizsardzības biroju un Informācijas tehnoloģiju drošības incidentu novēršanas institūciju (turpmāk – Drošības incidentu novēršanas institūcija) nodrošina kritiskās infrastruktūras aktuālo risku novērtēšanu un pārvaldīšanu.

III. Kritiskās infrastruktūras drošības pasākumu īstenošanas kārtība

8. Kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs kritiskās infrastruktūras drošības pasākumus reglamentējošo dokumentu vai dokumentus (turpmāk – drošības pasākumu dokumenti) izstrādā, pamatojoties uz šo noteikumu 7.2.apakšpunktā identificētajiem riskiem un ievērojot Drošības incidentu novēršanas institūcijas un Satversmes aizsardzības biroja ieteikumus. Pēc Satversmes aizsardzības biroja pieprasījuma kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs iesniedz Satversmes aizsardzības birojam drošības pasākumu dokumentus.

9. Ja kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs ir Latvijā reģistrēts finanšu un kapitāla tirgus dalībnieks vai par kritisko infrastruktūru ir noteikta valsts informācijas sistēma, vai uz attiecīgo kritisko infrastruktūru attiecas citas speciālās prasības informācijas tehnoloģiju drošības jomā, drošības pasākumu dokumentus izstrādā atbilstoši attiecīgo nozari reglamentējošajām prasībām, pamatojoties uz šo noteikumu 7.2.apakšpunktā identificētajiem riskiem un ievērojot Drošības incidentu novēršanas institūcijas un Satversmes aizsardzības biroja ieteikumus.

10. Kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs izstrādā drošības pasākumu dokumentus un iekļauj tajos šādu informāciju:

10.1. vispārīgas ziņas par kritisko infrastruktūru – nosaukums, īpašnieks vai tiesiskais valdītājs, kritiskās infrastruktūras atrašanās vieta (adrese), dokumenta mērķis;

10.2. struktūrvienība, kas nodrošina drošības pasākumu īstenošanu;

10.3. kritiskās infrastruktūras uzdevumi;

10.4. kritiskās infrastruktūras sistēmas detalizēts tehniskais apraksts un shēma;

10.5. aktuālo risku pārvaldīšanas plāns;