



Laidiens: 14.10.2005., Nr. 164

Ministru kabineta noteikumi Nr.765

Rīgā 2005.gada 11.oktobrī (prot. Nr.58 28.§)

Valsts informācijas sistēmu vispārējās drošības prasības

Izdoti saskaņā ar Valsts informācijas sistēmu likuma 4.panta otro daļu

- 1.Noteikumi nosaka valsts informācijas sistēmu vispārējās drošības prasības.
- 2.Valsts informācijas sistēmas (turpmāk — sistēma) drošību nodrošina pasākumu kopums, kurus īsteno, lai:
 - 2.1.nodrošinātu sistēmas darbību atbilstoši normatīvajos aktos noteiktajām funkcijām;
 - 2.2.nodrošinātu informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);
 - 2.3.nodrošinātu informācijas veselumu (pilnīgas un nemainītas informācijas saglabāšanu);
 - 2.4.nodrošinātu informācijas slepenību (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);
 - 2.5.aizsargātu sistēmas informācijas resursus (programmatūru, datnes (arī tās, kuras satur sistēmā glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju) un sistēmas dokumentāciju);
 - 2.6.aizsargātu sistēmas tehniskos resursus (datorus, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību);
 - 2.7.noteiktu sistēmas drošības apdraudējumu (ar nodomu (tiši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas var izraisīt sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama);
 - 2.8.novērtētu sistēmas drošības risku (iespēju, ka, īstenojoties drošības apdraudējumam, sistēmas informācija vai tehniskie resursi varētu mainīties, sabojāties, tikt iznīcināti vai nonākt tādu personu rīcībā, kuras nav tam pilnvarotas, vai piekļūšana sistēmas informācijas resursiem varētu būt traucēta vai neiespējama);
 - 2.9.atklātu sistēmas drošības incidentu (ar nodomu (tiši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas izraisījis sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem ir traucēta vai neiespējama);
 - 2.10.atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.
- 3.Sistēmas pārzinis nodrošina:

3.1.sistēmas drošības politikas izstrādi un īstenošanu;

3.2.iekšējo sistēmas drošības noteikumu izstrādi un ievērošanu;

3.3.sistēmas lietošanas noteikumu izstrādi un ievērošanu;

3.4.sistēmas drošības riska pārvaldības plāna izstrādi un izpildi;

3.5.sistēmas atjaunošanas plāna izstrādi un izpildi;

3.6.apmācību sistēmas drošības jautājumos.

4.Sistēmas pārzinis ieceļ sistēmas drošības pārvaldnieku. Sistēmas drošības pārvaldnieks organizē un vada sistēmas drošības pasākumu īstenošanu, ievērojot šajos noteikumos noteiktās prasības.

5.Sistēmas drošības politika ietver:

5.1.sistēmas drošības politikas mērķus un pamatnostādnes;

5.2.sistēmas raksturojumu un analīzi drošības jomā;

5.3.sistēmas drošības vadības organizācijas principus;

5.4.sistēmas drošības atbilstību normatīvajiem aktiem un standartiem;

5.5.sistēmas drošības principus un kritērijus (piemēram, sistēmas nepārtrauktās darbības laiks, sistēmas darbības atjaunošanas laiks, sistēmas drošības riska pieņemamais līmenis, sistēmas drošības incidenta atklāšanas laiks, pieļaujamais neveiksmīgo piekļūšanas mēģinājumu skaits).

6.Iekšējie sistēmas drošības noteikumi nosaka:

6.1.sistēmas informācijas resursu izveidošanas, papildināšanas, mainīšanas, apstrādes, pārraidīšanas, glabāšanas, atjaunošanas un iznīcināšanas kārtību;

6.2.sistēmas informācijas un tehnisko resursu lietošanas un tās kontroles kārtību;

6.3.kārtību, kādā tiek nodrošināta piekļūšana sistēmas informācijas un tehniskajiem resursiem;

6.4.sistēmas informācijas resursu rezerves kopiju izgatavošanas un glabāšanas kārtību, kā arī kārtību, kādā pārbauda, vai ar sistēmas informācijas resursu rezerves kopijām iespējams atjaunot sistēmas informācijas resursus;

6.5.datu nesēju lietošanas, pārvietošanas, glabāšanas un iznīcināšanas kārtību;

6.6.kārtību, kādā lieto un glabā informāciju vai datus, kas nepieciešami, lai piekļūtu sistēmas informācijas un tehniskajiem resursiem;

6.7.prasības sistēmas informācijas resursu aizsardzībai, kuru īsteno, izmantojot programmatūras līdzekļus (piemēram, sistēmas lietotāja atpazīšana un viņa pilnvaru atbilstības pārbaude attiecīgajām darbībām sistēmā, pasargājot sistēmas informācijas resursus no tišas vai nejaušas bojāšanas vai iznīcināšanas);

6.8.prasības sistēmas tehnisko resursu aizsardzībai pret fiziskas iedarbības radītu sistēmas drošības apdraudējumu (piemēram, ugunsgrēks, plūdi, sprieguma pazemināšanās vai pārspriegums enerģijas pievades tīklā, sistēmas tehnisko resursu zādzība, gaisa mitrums vai temperatūra, kas neatbilst ekspluatācijas noteikumiem);

6.9.kārtību, kādā novēro sistēmas drošības apdraudējuma tuvošanās pazīmes;

6.10.kārtību, kādā atklāj un pārvalda sistēmas drošības incidentus;