Vides aizsardzības un reģionālās attīstības ministrija

Valsts informācijas sistēmu drošība

Publicēts: 05.04.2020.

Valsts informācijas sistēmu drošība

Iespējamie apdraudējumi valsts informācijas sistēmu (VIS), kurās tiek apstrādāta valsts interesēm svarīga un ar likumiem, starptautiskajiem līgumiem un citiem normatīvajiem aktiem aizsargāta, kā arī iestādes sekmīgai darbībai nozīmīga informācija, drošībai ir viens no pamatfaktoriem, kas jāievēro VIS izveidē un uzturēšanā.

VIS drošību nodrošina pasākumu kopums, kurus īsteno, lai:

1) nodrošinātu sistēmas darbību atbilstoši normatīvajos aktos noteiktajām funkcijām;
2) nodrošinātu piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas;
3) nodrošinātu pilnīgas un nemainītas informācijas saglabāšanu;
4) nodrošinātu informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot;
5) aizsargātu VIS programmatūru, datnes (failus) un sistēmas dokumentāciju;
6) aizsargātu datorus, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina VIS darbību;
7) noteiktu sistēmas drošības apdraudējumu, atklātu sistēmas drošības incidentu (ar nodomu (tīši) 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 kuru dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama);
8) novērtētu iespēju, ka, īstenojoties drošības apdraudējumam, VIS informācija vai tehniskie resursi (datori , datu nesēji utt.) varētu mainīties, sabojāties, tikt iznīcināti vai nonākt tādu personu rīcībā, kuras nav tam pilnvarotas vai kuru dēļ piekļūšana sistēmas informācijas resursiem varētu būt traucēta vai neiespējama;
9) atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.

VIS drošības apdraudējums var būt gan ārējs, gan iekšējs (iestādes ietvaros) un to var iedalīt šādās grupās:

1) ārējo cilvēku radītie apdraudējumi (neautorizēta piekļuve, datu bojāšana utt.);
2) iekšējie cilvēku radītie apdraudējumi (darbinieka vai administratora kļūda, informācijas nesankcionēta izpaušana utt.);
3) iekārtu, programmatūras līniju, servisa atteice (bojāts serveris, nedarbojas datu pārraides tīkls utt.);
4) dabas un citi iepriekš neminētie apdraudējumi (ugunsgrēks, zibens radīts pārspriegums, vētra utt.).

Par VIS drošību iestādē atbild iestādes vadītājs. Drošības pārvaldnieks organizē drošības prasību izpildi un iestādei, kura uztur VIS, ir pienākums katru gadu veikt VIS drošības auditu.

Valsts iestādē esošajam drošības pārvaldniekam, ņemot vērā vadlīnijās ieteikto, jāievieš un jāorganizē VIS drošības pārvaldība atbilstoši MK 28.07.2015. noteikumiem Nr. 442 " Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām", starptautiskajiem standartiem un labai praksei IS drošības pārvaldības jomā.

https://www.varam.gov.lv/lv/valsts-informacijas-sistemu-drosiba