



Laidiens: 03.08.2015., Nr. 149

Oficiālās publikācijas Nr.: 2015/149.7

Ministru kabineta noteikumi Nr. 442

Rīgā 2015. gada 28. jūlijā (prot. Nr. 36 63. §)

Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām

Izdoti saskaņā ar Informācijas tehnoloģiju drošības likuma 8. panta piekto daļu un Valsts informācijas sistēmu likuma 4. panta otro daļu

I. Vispārīgie jautājumi

1. Noteikumi nosaka:

1.1. valsts un pašvaldību institūciju informācijas un komunikācijas tehnoloģiju minimālās drošības prasības un kārtību, kādā tiek nodrošināta valsts un pašvaldību institūciju (turpmāk – institūcijas) pārziņā vai turējumā esošo informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām prasībām;

1.2. valsts informācijas sistēmu vispārējās drošības prasības.

2. Noteikumi neattiecas uz informācijas un komunikācijas tehnoloģiju sistēmām, kurās tiek veikta valsts noslēpuma, Ziemeļatlantijas līguma organizācijas (turpmāk – NATO), Eiropas Savienības un ārvalstu institūciju klasificētās informācijas vai informācijas dienesta vajadzībām apstrāde vai uzglabāšana, kā arī uz kritiskās infrastruktūras informācijas sistēmām.

3. Noteikumi attiecas uz informācijas un komunikācijas tehnoloģiju sistēmām, tai skaitā valsts informācijas sistēmām (turpmāk – sistēmas), kas ir testēšanas stadijā, kā arī sistēmām, kas nodotas lietošanā. Citās sistēmas stadijās (plānošana, projektēšana, izstrāde) jānodrošina atbilstoša sistēmā esošas informācijas aizsardzība.

4. Šajos noteikumos minētos par informācijas tehnoloģiju drošības pārvaldību atbildīgās personas pienākumus attiecībā uz valsts informācijas sistēmu veic sistēmas drošības pārvaldnieks.

5. Sistēmas drošībai īsteno pasākumu kopumu, lai:

5.1. nodrošinātu informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);

5.2. nodrošinātu informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu);

5.3. nodrošinātu informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);

5.4. aizsargātu sistēmas informācijas resursus (datnes, arī tās, kuras satur sistēmā glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju, un sistēmas dokumentāciju);

5.5. aizsargātu sistēmas tehniskos resursus (datorus, programmatūru, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību);

5.6. noteiktu sistēmas drošības apdraudējumu (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 kura dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama);

5.7. novērtētu sistēmas drošības risku;

5.8. atklātu sistēmas drošības incidentu;

5.9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.

6. Sistēmas iedala divās kategorijās – pamata un paaugstinātas drošības sistēmas.

7. Lai sistēmu iedalītu pamata vai paaugstinātas drošības sistēmā, par informācijas tehnoloģiju drošības pārvaldību atbildīgā persona (turpmāk – atbildīgā persona) to izvērtē atbilstoši šādai metodikai:

7.1. izvērtē šo noteikumu 13.5. apakšpunktā minēto risku pieņemamo līmeni un piešķir atbilstošo drošības (pieejamības, integritātes un konfidencialitātes) klasi:

7.1.1. ja sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī (summāri), sistēmai piešķir C pieejamības klasi;

7.1.2. ja sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par 24 stundām (summāri) mēnesī, bet tas pieļaujams lielāks par četrām stundām (summāri) mēnesī, sistēmai piešķir B pieejamības klasi;

7.1.3. ja sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par četrām stundām mēnesī (summāri), sistēmai piešķir A pieejamības klasi;

7.1.4. ja sistēmā glabāto datu integritātes apdraudējums nerada risku institūcijas pamatfunkciju nodrošināšanai, sistēmai piešķir C integritātes klasi;

7.1.5. ja atsevišķu sistēmā glabāto datu integritātes apdraudējums rada risku institūcijas pamatfunkciju nodrošināšanai, sistēmai piešķir B integritātes klasi;

7.1.6. ja sistēmā glabāto datu integritātes apdraudējums rada risku institūcijas pamatfunkciju nodrošināšanai vai atsevišķu sistēmā glabāto datu integritātes apdraudējums var apdraudēt Latvijas Republikas nacionālās intereses un pamatvērtības vai izraisīt katastrofu, sistēmai piešķir A integritātes klasi;

7.1.7. ja sistēma satur tikai publiski pieejamu informāciju vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde nerada risku institūcijai, sistēmai piešķir C konfidencialitātes klasi;

7.1.8. ja sistēmā tiek apstrādāta ierobežotas pieejamības informācija, izņemot sensitīvus personas datus, vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūdes vienīgās sekas ir iespējamais kaitējums institūcijas, citu institūciju vai Latvijas Republikas reputācijai, sistēmai piešķir B konfidencialitātes klasi;

7.1.9. ja sistēmā tiek apstrādāti sensitīvi personas dati vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde var radīt smagākas sekas nekā kaitējums institūcijas, citu institūciju vai Latvijas Republikas reputācijai,

sistēmai piešķir A konfidencialitātes klasi;

7.2. ja sistēmai piešķirtas trīs B drošības klases vai vismaz viena A drošības klase, sistēma ir uzskatāma par paaugstinātas drošības sistēmu;

7.3. pārējos gadījumos sistēma ir uzskatāma par pamata drošības sistēmu.

8. Katra institūcija izstrādā šādus dokumentus katrai sistēmai, kā arī nodrošina tajos noteikto prasību izpildes uzraudzību un kontroli:

8.1. sistēmas drošības politika;

8.2. sistēmas drošības iekšējie noteikumi;

8.3. sistēmas lietošanas noteikumi;

8.4. sistēmas drošības riska pārvaldības plāns;

8.5. sistēmas darbības atjaunošanas plāns.

9. Uz pamata drošības sistēmām nav attiecināmas prasības, kas minētas šo noteikumu 8.2., 8.3., 8.4. un 8.5. apakšpunktā.

10. Šo noteikumu 8. punktā minētos dokumentus apstiprina institūcijas vadītājs. Institūcija visus šo noteikumu 8. punktā minētos dokumentus pārskata vismaz reizi gadā, kā arī šādos gadījumos:

10.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;

10.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;

10.3. ja pēkšņi pieaug sistēmas drošības incidentu skaits vai ir noticis nozīmīgs sistēmas drošības incidents;

10.4. ja izmaiņas institūcijas organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;

10.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.

11. Ja institūcijas pārziņā vai turējumā ir vairāk nekā viena sistēma, katru šo noteikumu 8. punktā minēto dokumentu var izstrādāt vairākām vai visām pārziņā vai turējumā esošajām sistēmām vienotu, ja nepieciešams, norādot specifiskās prasības katrai sistēmai.

12. Sistēmas drošības pasākumu atbilstību šo noteikumu 5. punktā minētajām prasībām novērtē, pamatojoties uz sistēmas drošības pārbaudes rezultātiem. Ja šīs pārbaudes laikā konstatēti būtiski trūkumi, institūcija veic pasākumus to novēršanai atbilstoši Informācijas tehnoloģiju drošības likumā noteiktajām prasībām.

II. Sistēmas drošības politika un iepirkumu prasības

13. Sistēmas drošības politika ietver:

13.1. sistēmas drošības politikas mērķus un pamatnostādnes;

13.2. sistēmas raksturojumu un analīzi drošības jomā;

13.3. sistēmas drošības pārvaldības organizācijas principus;

13.4. sistēmas drošības atbilstību normatīvajiem aktiem un standartiem;

13.5. sistēmas drošības principus, sistēmas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamo līmeni atbilstoši šo noteikumu 7. punktā minētajai metodikai un citus sistēmas drošības kritērijus (piemēram, sistēmas nepārtrauktās darbības laiks, sistēmas darbības atjaunošanas laiks, nosacījumi, pie kuriem ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām).

14. Institūcija nodrošina, ka šo noteikumu 13.5. apakšpunktā minētā informācija ir pieejama sistēmas lietotājiem.

15. Izstrādājot sistēmas drošības politiku, paredz, ka:

15.1. sistēmas lietotāji, kas veic sistēmas administrēšanas darbu, izmanto īpašus lietotāju kontus (turpmāk – sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;

15.2. katrs lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai (turpmāk – sistēmkonti), tad sistēmā jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju lietotājiem izmantot sistēmkontus;

15.3. ja sistēmā netiek izmantota daudzfaktoru autentifikācija, tas ir, viens atribūts, kam nav statiska daba (piemēram, kodu kalkulators, vienreiz lietojams izziņas kods), un vismaz viens cits atribūts, tad sistēmas lietotājiem obligāti jālieto paroles;

15.4. sistēmas lietotāja paroles garums nav mazāks par deviņiem simboliem un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un speciālu simbolu;

15.5. sistēmas lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros, izņemot šo noteikumu 15.7. apakšpunktā minēto gadījumu;

15.6. sistēmas lietotāja parole ievadišanas brīdī lietotājam netiek pilnībā attēlota;

15.7. sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir lietojama vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;

15.8. sistēmā nav pieļaujama funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;

15.9. iekārtām, tai skaitā infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;

15.10. tiek nodrošināta sistēmas auditācijas pierakstu (turpmāk – sistēmas pieraksti) veidošana un uzglabāšana vismaz sešus mēnešus pēc ieraksta izdarišanas;

15.11. jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei;

15.12. sistēmai jābūt uzliktiem visiem pieejamiem programmatūras atjauninājumiem, iepriekš izvērtējot to nepieciešamību;

15.13. visās institūcijas valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, jābūt iekļautai pretvīrusu funkcionalitātei;

15.14. sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām.

16. Sistēmas drošības politikā var paredzēt arī stingrākas drošības prasības, nekā noteikts šajos noteikumos, ciktāl tas nav pretrunā ar citiem normatīvajiem aktiem.