



Laidiens: 24.03.2000., Nr. 109/110

Ministru kabineta noteikumi Nr. 106

Rīgā 2000.gada 21.martā (prot. Nr. 13, 4.§)

Informācijas sistēmu drošības noteikumi

Izdoti saskaņā ar Ministru kabineta iekārtas likuma 14.panta 3.punktu

I. Vispārīgie jautājumi

1. Noteikumos lietotie termini:

1.1. **auditācijas pieraksti** — pieraksti, kuros reģistrēti dati par noteiktiem notikumiem informācijas sistēmā;

1.2. **fiziskā aizsardzība** — tehnisko resursu aizsardzība pret fiziskas iedarbības radītu informācijas sistēmas apdraudējumu (piemēram, ugunsgrēks, plūdi, sprieguma pazemināšanās vai pārspriegums enerģijas pievades tīklā, tehnisko resursu zādzība, ekspluatācijas noteikumiem neatbilstošs mitrums, gaisa temperatūra);

1.3. **informācijas resursi** — informācijas sistēmas sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, sistēmfaili un datu faili (arī tie, kas satur informācijas sistēmā glabājamo, apstrādājamo un informācijas sistēmas lietotājiem pieejamo informāciju);

1.4. **informācijas resursu turētājs** — persona, kas rīkojas ar informācijas resursiem informācijas sistēmas organizācijas uzdevumā;

1.5. **informācijas sistēma** — datu ievadišanas, uzglabāšanas un apstrādes sistēma, kas paredz lietotājpieeju tajā glabātajiem datiem vai informācijai;

1.6. **informācijas sistēmas apdraudējums** — ar nodomu (tiši) vai aiz neuzmanības izdarīta darbība vai bezdarbība, vai iespējams notikums, kas var izraisīt informācijas dzēšanu, noklusēšanu, informācijas resursu vai tehnisko resursu maiņu, bojāšanu vai informācijas nonākšanu tādu personu rīcībā, kas nav tam pilnvarotas;

1.7. **informācijas sistēmas drošība** — informācijas pieejamības (pēc informācijas sistēmas lietotāja pieprasījuma noteiktā laikposmā viņš var piekļūt informācijai), integritātes (pilnīgas un neizmainītas informācijas saglabāšana) un konfidencialitātes (informāciju saņem tikai tam pilnvarotas personas) nodrošināšana informācijas sistēmā;

1.8. **informācijas sistēmas lietotājs** — persona, kurai ir pieejama informācijas sistēmā glabātā informācija vai kura saņem informācijas sistēmas pakalpojumus;

1.9. **informācijas sistēmas organizācija** — valsts vai pašvaldības institūcija, sabiedriska organizācija vai uzņēmums (uzņēmējsabiedrība), kura īpašumā vai valdījumā ir informācijas resursi un tehniskie resursi;

1.10. **loģiskā aizsardzība** — datu vai informācijas resursu aizsardzība, kuru realizē ar programmatūras līdzekļiem, identificējot informācijas sistēmas lietotāju, pārbaudot viņa pilnvaru atbilstību attiecīgajām darbībām informācijas

sistēmā, pasargājot informāciju no tīšas vai nejaušas maiņas vai dzēšanas;

1.11. **parole** — personai zināma simbolu virkne, kuras kopija atrodas informācijas sistēmā un kuru izmanto šīs personas identitātes pierādīšanai;

1.12. **tehniskie resursi** — informācijas sistēmas sastāvdaļa, kurā ietilpst datori, datortīklu aparatūra un citas tehniskās iekārtas;

1.13. **tehnisko resursu turētājs** — persona, kas rīkojas ar tehniskajiem resursiem informācijas sistēmas organizācijas uzdevumā;

1.14. **ugunsmūris** — programmatūras un aparatūras komplekss, kas savieno lokālo tīklu ar ārējiem tīkliem, nodrošinot lokālajā tīklā savienoto informācijas sistēmu aizsardzību.

2. Šie noteikumi nosaka informācijas sistēmu drošības tiesiskās, tehniskās un organizatoriskās pamatprasības, ko ievēro informācijas sistēmas organizācija, tās vadītājs, informācijas resursu turētājs, tehnisko resursu turētājs, informācijas sistēmas lietotājs un citas personas, kuras ir atbildīgas par informācijas sistēmu drošību.

3. Šie noteikumi attiecas uz informācijas sistēmām:

3.1. kuru valdītājs ir valsts institūcija, kas izveidota saskaņā ar Saeimas vai Ministru kabineta izdotu aktu;

3.2. kurās glabā un apstrādā informāciju saskaņā ar starptautiskiem līgumiem, likumiem un Ministru kabineta noteikumiem;

3.3. kuru informācijas sistēmas organizāciju pilnīgi vai daļēji finansē no valsts vai pašvaldības budžeta līdzekļiem.

4. Šajos noteikumos noteikto prasību ieviešanu informācijas sistēmu organizācijās metodiski vada Satiksmes ministrija.

II. Informācijas klasifikācija

5. Persona, kura nodod informāciju informācijas sistēmā (turpmāk — informācijas devējs), nosaka, vai informācijai ir nepieciešams piešķirt šo noteikumu 9. vai 10.punktā minēto vērtības vai konfidencialitātes pakāpi, kā arī nosaka šo pakāpi.

6. Informācija, kurai nav piešķirta kāda vērtības vai konfidencialitātes pakāpe, ir neklasificējama informācija.

7. Vērtības pakāpi informācijai piešķir atkarībā no kaitējuma, kas varētu tikt nodarīts informācijas devējam vai informācijas sistēmas organizācijai, ja netiek nodrošināta informācijas integritāte vai pieejamība.

8. Konfidencialitātes pakāpi informācijai piešķir atkarībā no kaitējuma, kas varētu tikt nodarīts informācijas devējam vai informācijas sistēmas organizācijai, ja netiek nodrošināta informācijas konfidencialitāte.

9. Informācijai var piešķirt vienu no šādām vērtības pakāpēm:

9.1. augsta riska;

9.2. vidēja riska.

10. Informācijai var piešķirt vienu no šādām konfidencialitātes pakāpēm:

10.1. sevišķi slepena;

10.2. slepena;

10.3. konfidenciāla.

11. Informācijai, kuras konfidencialitāti aizsargā likums, piešķir konfidencialitātes pakāpi saskaņā ar šo noteikumu 10.punktu.

III. Riska analīze

12. Riska analīze nepieciešama, lai novērtētu:

12.1. informācijas sistēmas apdraudējuma īstenošanās varbūtību;

12.2. iespējamo kaitējumu informācijas devējam vai informācijas sistēmas organizācijai, ja nav nodrošināta informācijas sistēmas drošība.

13. Riska analīzi veic saskaņā ar Ministru kabineta apstiprinātu riska analīzes metodiku. Veicot riska analīzi:

13.1. nosaka iespējamās informācijas sistēmas apdraudējumus, arī tos, ko var radīt paši informācijas resursu turētāji, tehnisko resursu turētāji un informācijas sistēmas lietotāji, un novērtē šo apdraudējumu īstenošanās varbūtību;

13.2. novērtē iespējamo kaitējumu, ko var nodarīt informācijas devējam vai informācijas sistēmas organizācijai, ja īstenojies informācijas sistēmas apdraudējums;

13.3. nosaka informācijas sistēmas apdraudējuma novēršanai izmantojamās līdzekļus;

13.4. novērtē, vai pēc veiktajiem informācijas sistēmas drošības pasākumiem informācijas sistēmas apdraudējuma varbūtība un iespējamais kaitējums ir pieņemams informācijas sistēmas drošībai;

13.5. novērtē veikto informācijas sistēmas drošības pasākumu lietderību.

14. Riska analīze nepieciešama katram jaunam ar informācijas resursiem un tehniskajiem resursiem saistītam projektam.

15. Riska analīze nepieciešama, ja informācijas sistēmā notikušas izmaiņas, kuras var ietekmēt informācijas sistēmas drošību.

IV. Informācijas resursu un tehnisko resursu pārvalde

16. Informācijas sistēmas organizācija izstrādā iekšējos informācijas sistēmas drošības noteikumus, kā arī norīko personas, kas atbild par informācijas sistēmas drošību.

17. Informācijas sistēmas organizācijas vadītājs rakstiski norīko informācijas resursu un tehnisko resursu turētāju vai arī pats uzņemas veikt attiecīgos uzdevumus.

18. Informācijas sistēmas organizācijas vadītājs nodrošina informācijas resursu un tehnisko resursu turētāju ar līdzekļiem, kas nepieciešami informācijas sistēmas drošības pasākumiem.

19. Informācijas resursu turētājs:

19.1. kopīgi ar tehnisko resursu turētāju un (ja iespējams) ar informācijas devēju veic ar informācijas resursiem saistītā riska analīzi;

19.2. nodrošina loģiskās aizsardzības pasākumus;

19.3. nodrošina informācijas sistēmas auditācijas pierakstus, kā arī to saglabāšanu un pieejamību pārbaudei saskaņā ar iekšējiem informācijas sistēmas drošības noteikumiem;

19.4. nosaka kārtību, kādā informācijas sistēmas lietotājiem piešķir tiesības piekļūt informācijas resursiem un rīkoties ar tiem, un organizē šo resursu izmantošanas kontroli;

19.5. nodrošina informācijas resursu rezerves kopiju izgatavošanu un glabāšanu, kā arī informācijas resursu atjaunošanu, ja informācijas sistēmas funkcionēšana tehnisko resursu bojājumu vai citu iemeslu dēļ bijusi traucēta vai neiespējama.

20. Tehnisko resursu turētājs:

20.1. nodrošina fiziskās aizsardzības pasākumus;

20.2. piedalās riska analizē, nosaka ar tehniskajiem resursiem saistītus informācijas sistēmas apdraudējumus un novērtē šo apdraudējumu īstenošanās varbūtību;

20.3. nodrošina tehnisko resursu atjaunošanu, ja tie ir bojāti.

21. Informācijas resursu un tehnisko resursu turētājs rakstiski nosaka darbinieku pienākumus informācijas sistēmas drošības jomā un nodrošina darbinieku apmācību un zināšanu pārbaudi informācijas resursu un tehnisko resursu aizsardzības jomā.

V. Informācijas resursu un tehnisko resursu aizsardzība

22. Izvēloties informācijas sistēmas drošības līdzekļus un pasākumus, ievēro informācijai piešķirto konfidencialitātes un vērtības pakāpi.

23. Jebkurai informācijai un datiem, kas nepieciešami, lai piekļūtu informācijas sistēmā glabātajai informācijai ar konfidencialitātes pakāpi, piešķir tādu pašu pakāpi, kāda ir šai informācijai.

24. Dators, kurā ir sevišķi slepenas pakāpes informācija, nedrīkst būt pieslēgts ārējiem tīkliem vai lokālajam tīklam, no kura ir iespējama izeja uz ārējiem tīkliem.

25. Sevišķi slepenas pakāpes informāciju nepārraida pa ārējiem tīkliem.

26. Ja lokālajam tīklam pieslēgti datori, kuros ir sevišķi slepenas vai slepenas pakāpes informācija, lokālā tīkla kabeļi nedrīkst šķērsot teritoriju, kurai nav nodrošināta informācijas sistēmas apdraudējumam atbilstoša fiziskā aizsardzība, un tīkla aparātūrai jāatrodas telpās ar informācijas sistēmas apdraudējumam atbilstošu fizisko aizsardzību.

27. Telpām, kurās atrodas datori ar sevišķi slepenas, slepenas vai augsta riska pakāpes informāciju, nodrošina informācijas sistēmas apdraudējumam atbilstošu fizisko aizsardzību.

28. Sevišķi slepenas un slepenas pakāpes informācija visā glabāšanas laikā ir šifrēta.

29. Augsta riska un vidēja riska pakāpes informācija visā glabāšanas laikā ir aizsargāta ar kriptogrāfisko aizsardzību.

30. Ja lokālajam tīklam pieslēgti datori, kuros ir informācija ar konfidencialitātes vai vērtības pakāpi, lokālo tīklu var pieslēgt ārējiem tīkliem tikai ar ugunssmūri (izņemot šo noteikumu 24.punktā noteikto gadījumu), nodrošinot informācijas sistēmas apdraudējumam atbilstošu lokālā tīkla loģisko aizsardzību.

31. Datorus, kas veic ugunssmūra funkcijas, izmanto tikai šim nolūkam.

32. Ugunssmūris pārbauda elektroniskā pasta sūtījumus (arī pielikumu failus), vai tajos nav datora vīrusu. Datori, kas ārējiem tīkliem pieslēgti bez ugunssmūra, ir apgādāti ar datora vīrusu aizsardzības programmatūru, kas