

Sistēmas drošības iekšējie noteikumi paaugstinātas drošības informācijas sistēmai

1. Vispārīgie jautājumi

- 1.1. Sistēmas nosakums
- 1.2. Sistēmas apraksts
- 1.3. Sistēmas funkcijas
- 1.4. Sistēmas informācijas resursu apraksts
- 1.5. Sistēmas tehnisko resursu apraksts

2. Informācijas sistēmas dzīves cikls

Šajā nodaļā tiek noteikta (25.1) sistēmas informācijas resursu izveidošanas, papildināšanas, mainīšanas, apstrādes, pārraidīšanas, glabāšanas, atjaunošanas un iznīcināšanas kārtība

2.1.

3. Piekļuves kontrole (25.2 ; 25.3)

Šajā nodaļā tiek noteikta (25.2.) sistēmas informācijas un tehnisko resursu lietošanas un tās kontroles kārtība un (25.3.) kārtība, kādā tiek nodrošināta piekļūšana sistēmas informācijas un tehniskajiem resursiem

3.1. .

4. Informācijas resursu rezerves kopijas (25.4)

Šajā nodaļā tiek noteikta (25.4.) sistēmas informācijas resursu rezerves kopiju izgatavošanas un glabāšanas kārtība, kā arī kārtība, kādā pārbauda, vai ar sistēmas informācijas resursu rezerves kopijām iespējams atjaunot sistēmas informācijas resursus;

5. Datu nesēji (25.5)

Šajā nodaļā tiek noteikta (25.5.) datu nesēju lietošanas, pārvietošanas, glabāšanas un iznīcināšanas kārtība.

6. Piekļuves dati un sistēmas informācija (25.6)

Šajā nodaļā tiek noteikta (25.6) kārtība, kādā lieto un glabā informāciju vai datus, kas nepieciešami, lai piekļūtu sistēmas informācijas un tehniskajiem resursiem. Kā arī kārtība kādā uzglabā, pārveido un/vai dzēš sistēmas poierakstu datnes (25.15.).

6.1.

7. Loģiskā aizsardzība (25.7)

Šajā nodaļā ir noteiktas (25.7.) 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 tīšas vai nejaušas bojāšanas vai iznīcināšanas).

7.1.

8. Fiziskā aizsardzība

Šajā nodaļā tiek noteiktas (25.8.) 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).

8.1.

9. Apdraudējumu un incidentu pārvaldība

Šajā nodaļā tiek noteikta (25.9.) kārtība, kādā novēro sistēmas drošības apdraudējuma tuvošanās pazīmes un (25.10.) kārtība, kādā atklāj un pārvalda sistēmas drošības incidentus.

9.1.

10. Sistēmas darbība ja resursi pieejami nepilnā apjomā

Šajā nodaļā tiek noteikta (25.11) kārtība, kādā sistēma darbojas, ja sistēmas informācijas vai tehniskie resursi nav pieejami pilnā apjomā.

10.1.

11. Tehnisko resursu izmaiņu pārvaldība

Šajā nodaļā tiek noteikta (25.12) kārtība, kādā maina sistēmas tehniskos resursus.

11.1.

12. Darbinieku apmācības

Šajā nodaļā tiek noteiktas Iestādes (25.13) darbinieku apmācības un zināšanu pārbaudes kārtība sistēmas drošības jomā.

13. Atjauninājumu pārvaldība

Šajā nodaļā tiek noteikta kārtība, kādā Iestāde (25.14) izvērtē jauninājumu ietekmi uz sistēmas drošību.

14. Auditācija

14.1.

15. Noslēguma jautājumi

15.1. Noteikumus pārskata vismaz reizi gada, ka arī šādos gadījumos:

15.1.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;

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

15.1.3. ja pieaug sistēmas drošības incidentu skaits vai noticis nozīmīgs sistēmas drošības incidents.

15.2. Ja, pārskatot noteikumus, konstatēta atbilstoša nepieciešamība, tos aktualizē.