Izdevējs: Ministru kabinets
Veids: noteikumi
Numurs: 822
Pieņemts: 19.12.2023.
Stājas spēkā: 01.01.2024.

Publicēts:
Latvijas Vēstnesis, 251, 29.12.2023.
OP numurs: 2023/251.8

Attēlotā redakcija: 11.06.2026. - ...

Grozījumi:

Ministru kabineta 09.06.2026. noteikumi Nr.320 / LV, 110, 10.06.2026. / Stājas spēkā 11.06.2026.

Ministru kabineta noteikumi Nr. 822

Rīgā 2023. gada 19. decembrī (prot. Nr. 62 48. §)

Valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu institūciju klasificētās informācijas aizsardzības noteikumi

Izdoti saskaņā ar likuma "Par valsts noslēpumu" 6. panta trešo daļu, 7. panta otro, ceturto un astoto daļu, 9. panta septīto un astoto daļu, 11. panta ceturto daļu un 15. panta otro daļu

1. Vispārīgie jautājumi

1. Noteikumi nosaka vienotas valsts noslēpuma, Ziemeļatlantijas līguma organizācijas (turpmāk – NATO), Eiropas Savienības un ārvalstu institūciju klasificētās informācijas aizsardzības prasības par:

1.1. gadījumiem un kārtību, kādā valsts noslēpuma objekts var būt kādas personas valdījumā vai lietošanā;

1.2. kārtību, kādā organizē valsts noslēpuma aizsardzību jeb valsts noslēpuma objektu klasificēšanas, deklasificēšanas, saņemšanas, reģistrēšanas, glabāšanas, izsniegšanas, izmantošanas, nosūtīšanas, pārvēršanas elektroniskā formā un iznīcināšanas (sevišķās lietvedības) kārtību, šā procesa dokumentāro noformējumu, speciālu apzīmējumu, šifru (kodu) lietošanu, kā arī citu tehniska un organizatoriska rakstura pasākumu kārtību;

1.3. kārtību, kādā notiek ārvalstu, starptautisko organizāciju un to institūciju klasificētās informācijas saņemšana, nodošana un izmantošana;

1.4. kārtību, kādā notiek klasificētās informācijas nodošana ārvalstu pārstāvjiem Latvijas Republikas un ārvalstu sadarbības ietvaros;

1.5. nosacījumiem, termiņiem un kārtību, kādā institūcijas vadītājs ārkārtējās situācijas, kara vai izņēmuma stāvokļa laikā var atļaut personai, kurai ir izsniegta speciālā atļauja, iepazīties ar augstākas slepenības pakāpes valsts noslēpumu vai ārvalstu, starptautisko organizāciju un to institūciju klasificēto informāciju vai atļaut iepazīties ar konfidenciālu, slepenu un sevišķi slepenu valsts noslēpumu vai ārvalstu, starptautisko organizāciju un to institūciju klasificēto informāciju personai, kurai nav izsniegta speciālā atļauja;

1.6. kārtību speciālo atļauju uzskaitei un izsniegšanai;

1.7. dienesta izmeklēšanas kārtību gadījumos, ja ir pārkāpti valsts noslēpuma izmantošanas vai aizsardzības noteikumi.

(Grozīts ar MK 09.06.2026. noteikumiem Nr. 320)

2. Noteikumos lietotie termini:

2.1. **akreditēta informācijas sistēma** – Satversmes aizsardzības biroja noteiktā kārtībā reģistrēta un akreditēta informācijas sistēma, kurā apstrādā klasificēto informāciju, vai Militārās izlūkošanas un drošības dienesta noteiktā kārtībā reģistrēta un akreditēta informācijas sistēma, kurā apstrādā signālu izlūkošanas informāciju;

2.2. **apakšreģistrs** – institūcijas struktūrvienība, kas nodrošina konfidenciālas un augstākas slepenības pakāpes NATO un Eiropas Savienības klasificētās informācijas reģistrāciju, uzskaiti, saņemšanu, glabāšanu, pavairošanu, izsniegšanu, nosūtīšanu, iznīcināšanu un deklasificēšanu un kas uzrauga un koordinē institūcijas teritoriālajās struktūrvienībās izveidoto kontrolpunktu darbu;

2.3. **autorizēta persona** – institūcijas amatpersona vai darbinieks, kam institūcijas vadītājs ir uzdevis noteiktu šajos noteikumos minētu funkciju izpildi;

2.4. **centrālā reģistra birojs** – Nacionālās drošības iestādes struktūrvienība, kas nodrošina Latvijai nodotās un Latvijā radītās konfidenciālas un augstākas slepenības pakāpes NATO un Eiropas Savienības klasificētās informācijas kopējo kontroli un aprites uzraudzību valstī, kā arī uzrauga un koordinē visu apakšreģistru un kontrolpunktu darbu;

2.5. **deklasificēšana** – klasificētās informācijas slepenības pakāpes atcelšana;

2.6. **dokumenta digitalizācija** – dokumenta pārvēršana elektroniskā formā glabāšanai elektroniskā datu nesējā un attiecīgā papīra dokumenta iznīcināšana šajos noteikumos noteiktajā kārtībā;

2.7. **iepirkums** – pretendentu atlase, lai noslēgtu iepirkuma līgumu ar pasūtītāju vai vienošanos ar atbildīgo projektā vai programmā, kas paredz klasificētās informācijas apstrādi iepirkuma norises vai iepirkuma līguma izpildes posmā;

2.8. **informācijas sistēma** – elektroniska, atsevišķi stāvoša datu ievadīšanas, uzglabāšanas un apstrādes iekārta vai sistēma, kas paredz lietotāja pieeju tajā glabātajiem datiem vai informācijai;

2.9. **institūcija** – iestāde, privāto tiesību juridiskā persona vai to struktūrvienība, kas saskaņā ar likuma "Par valsts noslēpumu" 2. panta otro daļu ir valsts noslēpuma subjekts;

2.10. **klasificētā informācija** – valsts noslēpuma objekts, NATO, Eiropas Savienības vai ārvalstu klasificēts dokuments, elektroniskais datu nesējs, tehnika, aprīkojums vai ieroči, kas jau ir saražoti vai vēl atrodas ražošanas procesā, attiecībā uz ko ir noteikta vajadzība aizsargāt to pret nesankcionētu atklāšanu, izpaušanu vai izplatīšanu, uz ko norāda tā slepenības pakāpe;

2.11. **klasificētās informācijas dzīves cikls** – laikposms no klasificētās informācijas radīšanas līdz deklasificēšanai vai iznīcināšanai;

2.12. **klasificētās informācijas valdītājs** – institūcija, kuras darbības nodrošināšanai nepieciešams radīt vai izmantot valsts noslēpumu, NATO vai Eiropas Savienības klasificēto informāciju;

2.13. **kompetentā valsts drošības iestāde** – valsts drošības iestāde, kas atbilstoši likumā "Par valsts noslēpumu" noteiktajai kompetencei veic attiecīgās institūcijas telpu un personu drošības pārbaudi;

2.14. **kontrolpunkts** – struktūrvienība, kas nodrošina konfidenciālas un augstākas slepenības pakāpes NATO un Eiropas Savienības klasificētās informācijas reģistrāciju, uzskaiti, saņemšanu, glabāšanu, pavairošanu, izsniegšanu, nosūtīšanu, iznīcināšanu un deklasificēšanu institūcijas teritoriālajā struktūrvienībā un šajos jautājumos pakļaujas institūcijas apakšreģistram;

2.15. **Nacionālā drošības iestāde** – Satversmes aizsardzības biroja struktūrvienība, kas veic un kontrolē klasificētās informācijas apmaiņu ar ārvalstīm, starptautiskajām organizācijām un to institūcijām, kā arī veic šīs informācijas aizsardzības pasākumus;

2.16. **nepiederoša persona** – persona, kas nav institūcijas darbinieks vai amatpersona vai kurai tiešo amata vai dienesta pienākumu izpildei piekļuve klasificētai informācijai, paaugstinātās drošības zonai vai akreditētai informācijas sistēmai nav piešķirta;

2.17. **paaugstinātas drošības zona** – 1. un 2. drošības zona atbilstoši fiziskās drošības vides iedalījumam;

2.18. **par informācijas sistēmu atbildīgā persona** – persona institūcijā, kas veic informācijas sistēmas tehniskās uzturēšanas, administratora vai drošības pārziņa funkcijas;

2.19. **pasūtītājs** – institūcija, kas veic iepirkumu savām vai cita klasificētās informācijas valdītāja vajadzībām vai ir atbildīgais projektā vai programmā, kas saistīts ar klasificētās informācijas izmantošanu;

2.20. **pretendents** – fiziska vai juridiska persona, kas piedalās iepirkumā, kas saistīts ar klasificētās informācijas apstrādi;

2.21. **princips "nepieciešamība zināt"** – pieeja valsts noslēpumam personai ir tikai tādā apjomā, kādā tas nepieciešams saskaņā ar amata (dienesta) pienākumiem vai konkrētu darba (dienesta) uzdevumu veikšanai, kas saistīta ar valsts noslēpuma izmantošanu vai tā aizsardzību;

2.22. **reģistrācijas un uzskaites sistēma** – institūcijas izveidota un uzturēta kārtība (papīra formas žurnāli) vai informācijas sistēma, kas nodrošina institūcijas klasificētās informācijas reģistrāciju, pārvaldību un uzskaiti;

2.23. **sertifikāts** – Nacionālās drošības iestādes izsniegts apliecinājums, kas apliecina personas pieejas tiesības konfidenciālai un augstākas slepenības pakāpes NATO vai Eiropas Savienības klasificētai informācijai;

2.24. **sevišķā lietvedība** – kārtība, kādā veic konfidenciālu un augstākas slepenības pakāpes valsts noslēpuma objektu saturošu dokumentu un ārvalstu klasificētās informācijas reģistrāciju, uzskaiti, noformēšanu, saņemšanu, nosūtīšanu, transportēšanu, pavairošanu, tulkošanu, glabāšanu, iznīcināšanu un deklasificēšanu, ko organizē institūcijas darbinieks, amatpersona vai struktūrvienība;

2.25. **slepenības režīma nodrošinātājs** – institūcijas darbinieks, amatpersona vai struktūrvienība, kas institūcijā organizē personāla, informācijas, fizisko, industriālo un informācijas sistēmu drošību un ir atbildīga par to;

2.26. **speciālā atļauja** – kompetentās valsts drošības iestādes izsniegts dokuments, kas apliecina personas pieejas tiesības konfidenciāliem un augstākas slepenības pakāpes valsts noslēpuma objektiem vai attiecīgai ārvalstu klasificētai informācijai.

2. Personāla drošība

2.1. Amatu saraksti, speciālās atļaujas un sertifikāti

3. Personāla drošība ir procedūru kopums, kādā pieprasa un piešķir tiesības darbam ar konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju, veic apmācību vai instruktāžu darbam ar klasificēto informāciju.

4. Personai nav nepieciešama speciālā atļauja un sertifikāts darbam, kas saistīts ar dienesta vajadzībām klasificētās informācijas izmantošanu vai tās aizsardzību. Persona, kurai nav izsniegta speciālā atļauja, uzsākot pildīt amata vai dienesta pienākumus, institūcijas vadītājam rakstveidā apliecina, ka ir iepazinusies ar dienesta vajadzībām klasificētās informācijas aizsardzības kārtību un noteikto atbildību par tās pārkāpšanu, kā arī apņemas ievērot minēto kārtību (1. pielikums).

5. Institūcija izstrādā institūcijas amatu sarakstu darbam ar konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju, kurā norāda, ar kādas slepenības pakāpes klasificēto informāciju darbu veiks amatā esošā persona. Amatu saraksta pozīciju pamato ar konkrētiem pienākumiem, kas paredz nepieciešamību saņemt speciālo atļauju vai sertifikātu. Kompetentajai valsts drošības iestādei ir tiesības pieprasīt pamatojumu amatu sarakstā iekļautā amata saistībai ar konfidenciālu vai augstākas slepenības pakāpes klasificēto informāciju.

6. Personai pirms amata vai dienesta pienākumu uzsākšanas, kas saistīti ar konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas izmantošanu vai tās aizsardzību, speciālo atļauju vai sertifikātu izsniedz:

6.1. Satversmes aizsardzības birojs – pirmās kategorijas speciālo atļauju pieejai sevišķi slepeniem valsts noslēpuma objektiem;

6.2. kompetentā valsts drošības iestāde – otrās kategorijas speciālo atļauju pieejai slepeniem valsts noslēpuma objektiem un trešās kategorijas speciālo atļauju pieejai konfidenciāliem valsts noslēpuma objektiem;

6.3. Nacionālā drošības iestāde – sertifikātu pieejai konfidenciālai un augstākas slepenības pakāpes NATO vai Eiropas Savienības klasificētai informācijai.

7. Lai persona saņemtu speciālo atļauju vai sertifikātu, institūcija nodrošina, ka persona iepazīstas ar normatīvajiem aktiem par klasificētās informācijas aizsardzību.

8. Personas pārbaudes uzsākšanai institūcija sagatavo un nosūta kompetentajai valsts drošības iestādei pieprasījumu par speciālās atļaujas un/vai sertifikāta piešķiršanu. Pieprasījumā:

8.1. norāda speciālās atļaujas un/vai sertifikāta izsniegšanas pamatojumu, kā arī tās klasificētās informācijas slepenības pakāpi, kurai nepieciešama piekļuve;

8.2. norāda speciālās atļaujas un/vai sertifikāta izsniegšanas veidu;

8.3. pievieno personas personīgi aizpildītu un parakstītu aptaujas lapu (2. pielikums);

8.4. norāda informāciju par to, vai persona ir veikusi iekšējās kārtības un drošības normu pārkāpumus, un par to, vai pret personu kādreiz ir tikusi uzsākta dienesta pārbaude vai disciplinārlieta, kas saistīta ar informācijas aizsardzību, ja vien šī informācija jau iepriekš nav nosūtīta kompetentajai valsts drošības iestādei.

9. Persona aizpilda aptaujas lapas visas ailes, parakstoties apliecina tajā norādīto ziņu patiesumu un piekrīt pēc valsts drošības iestādes pieprasījuma iesniegt bankas un citu kredītiestāžu vai maksājumu platformu informāciju par saviem naudas uzkrājumiem un finanšu darījumiem, kā arī citu nepieciešamo informāciju, kurai pēc valsts drošības iestādes ieskatiem var būt būtiska nozīme, vērtējot personas atbilstību speciālās atļaujas saņemšanai.

10. Personai, kura ir saņēmusi atbilstošas kategorijas speciālo atļauju un par kuru Nacionālajā drošības iestādē ir veikta papildu pārbaude, sertifikātu izsniedz uz termiņu, kas nav garāks par personai izsniegtās speciālās atļaujas derīguma termiņu.

11. Kompetentā valsts drošības iestāde personas pārbaudes ietvaros veic pārrunas, to norisi dokumentējot rakstveidā, audioierakstā vai videoierakstā, ja:

11.1. persona pirmo reizi pretendē uz pieeju sevišķi slepenai klasificētajai informācijai;

11.2. nepieciešams precizēt vai pārbaudīt pārbaudes laikā atklāto informāciju;

11.3. persona var sniegt būtisku informāciju pārbaudes veikšanai.

12. Kompetentā valsts drošības iestāde par speciālās atļaujas vai sertifikāta piešķiršanu informē pārbaudes iniciatoru:

12.1. izsniedzot vai nosūtot noteikta parauga speciālo atļauju (3. pielikums);

12.2. izsniedzot vai nosūtot noteikta parauga sertifikātu (4. un 5. pielikums);

12.3. neizsniedzot noteikta parauga speciālo atļauju vai sertifikātu, bet veicot ierakstu par attiecīgās kategorijas speciālās atļaujas vai sertifikāta piešķiršanu un laikposmu, uz kādu speciālā atļauja vai sertifikāts piešķirts, institūcijas personāla uzskaites un vadības sistēmā tiešsaistes režīmā, ja pirms tam starp institūciju un kompetento valsts drošības iestādi ir noslēgta vienošanās, kas nosaka šā procesa kārtību.

13. Institūcijā saņemto speciālo atļauju vai sertifikātu izsniedz personai, ja speciālā atļauja vai sertifikāts nepieciešams amata vai dienesta pienākumu veikšanai ārpus institūcijas. Amata vai dienesta pienākumu pildīšanai nederīgu vai nevajadzīgu speciālo atļauju un sertifikātu institūcija iznīcina.

14. Atkārtotai speciālās atļaujas izsniegšanai uz jaunu termiņu šo noteikumu 8. punktā minētos dokumentus kompetentajā valsts drošības iestādē iesniedz vismaz septiņus mēnešus pirms spēkā esošās speciālās atļaujas derīguma termiņa beigām.

15. Institūcija ne vēlāk kā mēneša laikā no dienas, kad kļuvis zināms, ka personai piešķirtā speciālā atļauja vai sertifikāts vairs nav nepieciešams, rakstveidā par to informē kompetento valsts drošības iestādi.

16. Izmaiņu pieteikumus aptaujas lapā persona iesniedz ar institūcijas starpniecību vai nepastarpināti kompetentai valsts drošības iestādei. Ja persona izmaiņu pieteikumus iesniedz nepastarpināti kompetentai valsts drošības iestādei, tad par šo faktu informē institūciju.

17. Personas pārbaudes materiālus glabā kompetentā valsts drošības iestāde.

18. Lai apkopotu informāciju par tām personām, kurām ir piešķirta speciālā atļauja darbam ar valsts noslēpumu saturošu informāciju un Eiropas Savienības un NATO klasificēto informāciju, Satversmes aizsardzības birojs uztur vienotu speciālo atļauju un sertifikātu uzskaites sistēmu, nodrošinot valsts drošības iestādēm pieeju šiem datiem.

19. Starptautiskās sadarbības savstarpējo vizīšu ietvaros, kas saistītas ar konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas izmantošanu, Latvijas Republikā vai ārvalstīs personai izsniegtas speciālās atļaujas vai sertifikāta derīgumu pārbauda, izmantojot Nacionālās drošības iestādes izstrādāto vizītes pieprasījuma anketu, šādā kārtībā:

19.1. ja Latvijas Republikas pilsonim vizītei citā valstī tiek pieprasīta vizītes pieprasījuma anketa, institūcija, kuru persona pārstāv, ne vēlāk kā 20 darba dienas pirms vizītes iesniedz Nacionālajai drošības iestādei aizpildītu vizītes pieteikuma anketu, kas to pārbauda, apstiprina un nosūta apmeklējamās valsts kompetentajai institūcijai;

19.2. ja Latvijas Republikas institūcijai nepieciešams pārliecināties par citas valsts pilsonim izsniegtas speciālās atļaujas vai sertifikāta derīgumu, tā ne vēlāk kā 20 darba dienas pirms vizītes lūdz ārvalsts institūcijai, kuru attiecīgā persona pārstāv, aizpildīt vizītes pieprasījuma anketu. Nacionālā drošības iestāde šo anketu saņem aizpildītu no attiecīgās valsts kompetentās iestādes, pārbauda, saskaņo un nosūta Latvijas Republikas institūcijai.

20. Personu ar klasificēto informāciju iepazīstina, ievērojot principu "nepieciešamība zināt".

21. Ja personas rīcībā, kurai nav speciālās atļaujas un sertifikāta vai kura nav parakstījusi saistību rakstu attiecībā uz dienesta vajadzībām klasificēto informāciju, nokļuvusi klasificētā informācija, tās pienākums ir neizpaust klasificēto informāciju. Institūcija, kurai šis fakts kļuvis zināms, par to informē kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija. Attiecīgi kompetentā valsts drošības iestāde vai Nacionālā drošības iestāde rakstveidā brīdina minēto personu par pienākumu neizpaust klasificēto informāciju, kā arī saņem no personas saistību rakstu (6. pielikums) par klasificētās informācijas neizpaušanu.

22. Ja personai, kurai nav atbilstošas kategorijas speciālās atļaujas vai sertifikāta, kļuvusi zināma augstākas slepenības pakāpes klasificētā informācija, tās pienākums ir neizpaust to un informēt institūcijas slepenības režīma nodrošinātāju. Par šo faktu institūcija informē kompetento valsts drošības iestādi vai, ja iesaistīta NATO, ES vai

ārvalstu klasificētā informācija, Nacionālo drošības iestādi.

2.2. Piekļuve konfidenciālai un augstākas slepenības pakāpes klasificētajai informācijai ārkārtējās situācijas, kara vai izņēmuma stāvokļa laikā

23. Institūcijas vadītājs ārkārtējās situācijas, kara vai izņēmuma stāvokļa laikā var sniegt rakstveida atļauju personai, kurai ir izsniegta speciālā atļauja vai sertifikāts, iepazīties ar augstākas slepenības pakāpes klasificēto informāciju. Minētajā atļaujā norāda:

23.1. personas tiešā vadītāja sniegto pamatojumu, ka noteiktā īpašā tiesiskā režīma laikā konkrētā persona ir neaizvietojama;

23.2. informāciju par institūcijā veikto pārbaudi, ka savu līdzšinējo amata vai dienesta pienākumu ietvaros konkrētā persona nav veikusi būtiskus vai atkārtotus ierobežotas pieejamības vai klasificētās informācijas aizsardzības noteikumu pārkāpumus;

23.3. kādai klasificētajai informācijai šā izņēmuma ietvaros konkrētai personai nodrošināta piekļuve saskaņā ar institūcijas darbinieka, amatpersonas vai struktūrvienības, kas organizē sevišķo lietvedību, sagatavoto uzskaiti.

24. Institūcijas vadītājs konkrētai personai atļauj iepazīties ar augstākas slepenības pakāpes klasificēto informāciju, ievērojot principu "nepieciešamība zināt".

25. Institūcijas vadītājs mēneša laikā pēc šo noteikumu 23. punktā minētās atļaujas izsniegšanas rakstveidā informē par to kompetento valsts drošības iestādi, norādot atļaujā iekļauto informāciju.

26. Piekļuves termiņš klasificētajai informācijai saskaņā ar šo noteikumu 23. punktā minēto atļauju nedrīkst pārsniegt trīs mēnešus. Ja nepieciešams ilgāks piekļuves termiņš klasificētajai informācijai, institūcija informē kompetento valsts drošības iestādi par nepieciešamību personai izsniegt augstākas kategorijas speciālo atļauju vai sertifikātu.

27. Institūcijas vadītājs ārkārtējās situācijas, kara vai izņēmuma stāvokļa laikā var sniegt rakstveida atļauju personai, kurai nav izsniegta speciālā atļauja vai sertifikāts, iepazīties ar konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju. Minētajā atļaujā norāda:

27.1. personas tiešā vadītāja sniegto pamatojumu, ka noteiktā īpašā tiesiskā režīma laikā konkrētā persona ir neaizvietojama;

27.2. informāciju par izvērtējumu, ka institūcijai par konkrēto personu nav pieejama būtiska negatīva informācija, kas būtu par pamatu apšaubīt personas lojalitāti un uzticamību;

27.3. institūcijas vadītāja atzinumu, ka noteiktā jautājuma risināšanā vai krīzes pārvarēšanā nav iespējams cits risinājums;

27.4. kādai klasificētajai informācijai šā izņēmuma ietvaros konkrētai personai nodrošināta piekļuve saskaņā ar institūcijas darbinieka, amatpersonas vai struktūrvienības, kas organizē sevišķo lietvedību, sagatavoto uzskaiti.

28. Institūcijas vadītāja atļauja personai, kurai nav izsniegta speciālā atļauja vai sertifikāts, iepazīties ar konfidenciālu vai augstākas slepenības pakāpes klasificēto informāciju pieļaujama tikai tādā gadījumā, ja speciālās atļaujas vai sertifikāta saņemšana nav iespējama ārkārtējās situācijas, kara vai izņēmuma stāvokļa dēļ.

29. Personai, kurai nav izsniegta speciālā atļauja vai sertifikāts, institūcijas vadītājs atļauj iepazīties ar konfidenciālu vai augstākas slepenības pakāpes klasificēto informāciju, ievērojot principu "nepieciešamība zināt".

30. Piešķirot personai, kurai nav izsniegta speciālā atļauja vai sertifikāts, atļauju iepazīties ar konfidenciālu un augstākas slepenības pakāpes informāciju, no personas tiek pieņemts saistību raksts (6. pielikums), ar kuru tā apliecina, ka ir informēta par klasificētās informācijas aizsardzības prasībām, par aizliegumu klasificēto informāciju izpaust vai jebkādā veidā tālāk apstrādāt, kā arī ir brīdināta par Krimināllikumā noteikto atbildību.

31. Institūcijas vadītājs nekavējoties rakstveidā informē kompetento valsts drošības iestādi par šo noteikumu 27. punktā minētās atļaujas izsniegšanu un tajā iekļauto informāciju. Piekļuves termiņš klasificētajai informācijai saskaņā šo noteikumu 27. punktā minēto atļauju nedrīkst pārsniegt trīs mēnešus. Ja nepieciešams ilgāks piekļuves termiņš klasificētajai informācijai, institūcija informē kompetento valsts drošības iestādi par vajadzību personai izsniegt speciālo atļauju vai sertifikātu.

32. Kara stāvokļa laikā institūcijas vadītājs piemēro šo noteikumu 23.2. un 27.2. apakšpunktu un 24. un 29. punktu, savukārt pārējos šīs apakšnodaļas punktus sāk piemērot, tiklīdz iespējams, ņemot vērā faktiskos apstākļus.

2.3. Atbildīgo personu pienākumi

33. Par klasificētās informācijas aizsardzības pasākumu nodrošināšanu institūcijā ir atbildīgs tās vadītājs. Institūcijas vadītājs:

33.1. nodrošina slepenības režīmu vai norīko slepenības režīma nodrošinātāju un par to rakstveidā informē kompetento valsts drošības iestādi;

33.2. organizē sevišķo lietvedību vai norīko atbildīgo personu sevišķās lietvedības organizēšanai un par to rakstveidā informē kompetento valsts drošības iestādi;

33.3. ja institūcijā ir paredzēta konfidenciālas un augstākas slepenības pakāpes NATO un/vai Eiropas Savienības klasificētās informācijas apstrāde, izveido apakšreģistru un, ja nepieciešams, kontrolpunktu un par to rakstveidā informē Nacionālo drošības iestādi;

33.4. norīko institūcijā atbildīgās amatpersonas, darbiniekus vai struktūrvienību, kas nodrošina dienesta vajadzībām klasificētās informācijas lietvedību un fiziskās drošības pasākumu ieviešanu un ievērošanu, un par to rakstveidā informē kompetento valsts drošības iestādi. Šos pienākumus var veikt arī institūcijas struktūrvienība, kas institūcijā atbild par konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas drošību;

33.5. apstiprina institūcijas dienesta vajadzībām klasificētās informācijas sarakstu;

33.6. ja institūcijā lieto akreditētu informācijas sistēmu, norīko personu, kas ir atbildīga par akreditētu informācijas sistēmu;

33.7. apstiprina šo noteikumu 5. punktā minēto institūcijas amatu sarakstu par personām, kurām nepieciešama piekļuve konfidenciālai un augstākas slepenības pakāpes klasificētajai informācijai;

33.8. atbild par šajos noteikumos noteiktajām drošības prasībām atbilstošu telpu izveidi un aprīkošanu klasificētās informācijas apstrādei un glabāšanai;

33.9. nodrošina kārtību, kādā darbinieks vai amatpersona, kuram ir speciālā atļauja vai sertifikāts, bet kurš pārtrauc amata vai dienesta attiecības vai arī kuram uzdod pildīt citus pienākumus institūcijā, nodod visu viņa rīcībā esošo klasificēto informāciju institūcijas sevišķajā lietvedībā, centrālā reģistra birojā, apakšreģistrā vai kontrolpunktā.

34. Par akreditētas informācijas sistēmas darbību ir atbildīgs ar institūcijas vadītāja rakstisku rīkojumu norīkots drošības pārzinis. Par akreditēto informācijas sistēmu atbildīgajai personai ir nepieciešama atbilstošas pakāpes speciālā atļauja, kas atbilst informācijas sistēmā apstrādātā un uzkrātā valsts noslēpuma līmenim ar slepenības pakāpi "konfidenciāli" vai augstākam līmenim. Ja akreditētā informācijas sistēmā apstrādā un glabā NATO un Eiropas Savienības klasificēto informāciju, par informācijas sistēmu atbildīgajām personām ir nepieciešams sertifikāts, kas ir par vienu slepenības pakāpi augstāks par informācijas sistēmā apstrādātās un uzkrātās NATO un Eiropas Savienības

klasificētās informācijas slepenības pakāpi. Ja akreditētā informācijas sistēmā apstrādā un glabā NATO un Eiropas Savienības sevišķi slepeno klasificēto informāciju, par informācijas sistēmu atbildīgajām personām ir nepieciešams sertifikāts, kas apliecina to pieejas tiesības NATO un Eiropas Savienības sevišķi slepenai klasificētajai informācijai.

35. Institūcijā, kur ir paredzēta COSMIC TOP SECRET vai ATOMAL informācijas aprite un glabāšana, slepenības režīma nodrošināšanas struktūrvienībā norīko COSMIC drošības virsnieku un COSMIC drošības virsnieka vietnieku, kas nodrošina COSMIC TOP SECRET un ATOMAL informācijas aprites noteikumu ievērošanu un tās aizsardzību. Centrālā reģistra birojs ne retāk kā reizi gadā apkopo apakšreģistra uzturēto informāciju, un apakšreģistri ne retāk kā reizi gadā apkopo kontrolpunktu COSMIC drošības virsnieku un drošības virsnieku vietnieku sarakstus un to parakstu paraugus.

36. Šo noteikumu 33.1., 33.2., 33.3. un 33.4. apakšpunktā un 35. punktā minētās struktūrvienības vai darbinieki šajos noteikumos paredzēto funkciju izpildē ir tiešā institūcijas vadītāja pakļautībā. Ja slepenības režīmu vai sevišķo lietvedību institūcijā nodrošina viens darbinieks vai amatpersona, uz viņu attiecas visas šajos noteikumos noteiktās slepenības režīma nodrošināšanas vai sevišķās lietvedības struktūrvienības tiesības un pienākumi. Slepenības režīma nodrošināšanas un sevišķās lietvedības organizēšanas funkcijas nav atļauts veikt vienam un tam pašam darbiniekam vai amatpersonai.

37. Slepenības režīma nodrošinātāja pienākumi:

37.1. uzraudzīt konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas aizsardzības prasību ieviešanu un ievērošanu personāla drošības, informācijas drošības, fiziskās drošības, industriālās drošības un informācijas sistēmu drošības jomās;

37.2. kontrolēt, kā darbinieks vai amatpersona, kas veic darbu ar konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju, ievēro un pilda tās aizsardzības noteikumus;

37.3. pieprasīt no darbinieka vai amatpersonas paskaidrojumus par konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas aizsardzības noteikumu neievērošanu un ziņot par konstatētajiem pārkāpumiem institūcijas vadītājam;

37.4. savlaicīgi informēt personu, kurai amata pienākumu izpildei nepieciešama speciālā atļauja un sertifikāts, par speciālo atļauju un sertifikātu saņemšanas kārtību;

37.5. savlaicīgi nosūtīt nepieciešamos dokumentus kompetentajai valsts drošības iestādei personas pārbaudes veikšanai;

37.6. nodrošināt aptaujas lapās sniegtās informācijas izmaiņu apkopošanu institūcijā un savlaicīgu nosūtīšanu kompetentajai valsts drošības iestādei;

37.7. nodrošināt institūcijas kurjera instruēšanu atbilstoši šo noteikumu 132. punktam;

37.8. izstrādāt un iesniegt institūcijas vadītājam apstiprināšanai normatīvo aktu par konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas aprites un aizsardzības pasākumu kopumu institūcijā;

37.9. izstrādāt un iesniegt institūcijas vadītājam apstiprināšanai normatīvo aktu par konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas esības pārbaudes procedūrām institūcijā. Vismaz reizi gadā nodrošināt pārbaudi par papīra formā izsniegtajiem dokumentiem institūcijas darbiniekiem vai amatpersonām. Par veiktajām pārbaudēm sagatavot attiecīgu aktu;

37.10. izstrādāt un iesniegt institūcijas vadītājam apstiprināšanai konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas, kā arī, ja ir, šifrēšanas iekārtu un šifrēšanas materiālu evakuācijas plānu ārkārtējās situācijas vai izņēmuma stāvoklī. Plānā norāda:

37.10.1. konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju, šifrēšanas iekārtas un šifrēšanas materiālus, kurus nogādā evakuācijas vietā vai iznīcina;

37.10.2. darbiniekus vai amatpersonas, kuras atbildīgas par evakuējamo konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas, šifrēšanas iekārtas un šifrēšanas materiālu uzskaiti un glabāšanu, sagatavošanu transportēšanai, transportēšanu, apsardzi vai iznīcināšanu;

37.10.3. kārtību, kādā veicama konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas, šifrēšanas iekārtu un šifrēšanas materiālu apsardze transportēšanas laikā un evakuācijas vietā;

37.11. veikt darbinieku vai amatpersonu, tai skaitā institūcijas vadītāja, instruktāžu par personas atbildību un pienākumu aizsargāt tai zināmo klasificēto informāciju pēc speciālās atļaujas vai sertifikāta anulēšanas, nodošanas un darba tiesisko attiecību izbeigšanas. Darbinieks vai amatpersona ar parakstu apliecina, ka ir informēta par instruktāžā minēto atbildību un pienākumiem.

38. Darbiniekam vai amatpersonai, kura veic darbu ar klasificēto informāciju, ir šādi pienākumi:

38.1. ievērot klasificētās informācijas lietošanas, uzskaites un glabāšanas noteikumus;

38.2. pārtraukt citu personu rīcību, kuru dēļ var notikt klasificētās informācijas izpaušana nepiederošām personām, un nekavējoties ziņot institūcijas slepenības režīma nodrošinātājam;

38.3. pirms amata vai dienesta attiecību pārtraukšanas nodot visu klasificēto informāciju;

38.4. pēc institūcijas atbildīgās struktūrvienības, darbinieka vai amatpersonas pieprasījuma uzrādīt pārbaudei visu tai pieejamo konfidenciālo un augstākas slepenības pakāpes klasificēto informāciju;

38.5. pēc institūcijas atbildīgās struktūrvienības, darbinieka vai amatpersonas pieprasījuma sniegt paskaidrojumus par klasificētās informācijas aizsardzības noteikumu neievērošanu;

38.6. ne vēlāk kā mēneša laikā no dienas, kad personai attiecīgās ziņas kļuvušas zināmas, iesniegt slepenības režīma nodrošinātājam vai kompetentajai valsts drošības iestādei informāciju par izmaiņām aptaujas lapas (2. pielikums) 1., 5., 6.2., 14.1., 16., 17., 18., 20., 21., 22., 23., 24., 26., 27. un 29. punktā.

2.4. Apmācības un instruktāžas

39. Institūcijā nodrošina, ka institūcijas darbinieki vai amatpersonas ne retāk kā reizi gadā tiek informētas par drošības noteikumiem klasificētās informācijas aizsardzības jomā, atbildību par drošības noteikumu neievērošanu, informācijas nesankcionētu izpaušanu vai nozaudēšanu. Pēc nepieciešamības sadarbībā ar kompetento valsts drošības iestādi institūcijas vadītājs organizē instruktāžu par iespējamiem izlūkošanas un pretizlūkošanas apdraudējumiem. Darbinieks vai amatpersona ar parakstu apliecina, ka ir informēta par instruktāžā minēto atbildību un pienākumiem.

40. Militārās izlūkošanas un drošības dienests veic instruktāžu par valsts noslēpuma objektu aizsardzību signālu izlūkošanas jomā (turpmāk – signālu izlūkošanas informācija) personām, kuras saņēmušas speciālo atļauju. Personu instruktāžu par signālu izlūkošanas informācijas aizsardzību Militārās izlūkošanas un drošības dienests veic pirms darba uzsākšanas ar signālu izlūkošanas informāciju (turpmāk – sākotnējā instruktāža), kā arī pēc darba pabeigšanas ar signālu izlūkošanas informāciju (turpmāk – noslēguma instruktāža).

41. Sākotnējās vai noslēguma instruktāžas veikšanu iniciē institūcija, kurā amatpersona vai darbinieks uzsāks vai ir pabeidzis darbu ar signālu izlūkošanas informāciju (turpmāk – instruktāžas iniciators). Instruktāžas iniciators nosūta Militārās izlūkošanas un drošības dienestam pieprasījumu par instruktāžas veikšanu (7. pielikums). Instruktāžas iniciators nodrošina, lai amatpersona vai darbinieks neiepazītos un neveiktu darbu ar signālu izlūkošanas informāciju, pirms nav saņemts Militārās izlūkošanas un drošības dienesta apliecinājums, ka amatpersona vai darbinieks ir instruēts par signālu izlūkošanas informācijas specifiku un apguvis tās aizsardzības prasības.

42. Apliecinājumu par to, ka amatpersona vai darbinieks ir instruēts par signālu izlūkošanas informācijas specifiku un apguvis tās aizsardzības prasības, vai apliecinājumu par noslēguma instruktāžas veikšanu Militārās izlūkošanas un drošības dienests rakstveidā izsniedz instruktāžas iniciatoram. Ja Militārās izlūkošanas un drošības dienests informē instruktāžas iniciatoru, ka amatpersona vai darbinieks sākotnējās instruktāžas laikā nav apguvis signālu izlūkošanas informācijas apstrādes un aizsardzības pamatprincipus, instruktāžas iniciators vienojas ar Militārās izlūkošanas un drošības dienestu par personas atkārtotu instruēšanu vai virza citu personu attiecīgo pienākumu veikšanai.

43. Militārās izlūkošanas un drošības dienests nodrošina informācijas uzskaiti par personām, kurām veikta sākotnējā un noslēguma instruktāža darbam ar signālu izlūkošanas informāciju. Lai nodrošinātu informācijas uzskaiti, Militārās izlūkošanas un drošības dienests apkopo šādu informāciju par minēto personu: vārds, uzvārds, dzimšanas datums, pārstāvētā institūcija, tās struktūrvienība, amats, veiktās instruktāžas datums, speciālās atļaujas numurs un tās derīguma termiņš.

44. Nacionālā drošības iestāde nodrošina personas informēšanu par NATO ATOMAL informācijas specifiku un tās aizsardzības noteikumiem pirms NATO ATOMAL sertifikāta izsniegšanas (8. pielikums). Persona ar parakstu apliecina, ka ir saņēmusi NATO ATOMAL instruktāžu.

3. Klasificētās informācijas fiziskā drošība

3.1. Klasificētās informācijas fiziskās drošības vispārīgie jautājumi

45. Fiziskā drošība ir pasākumu kopums, kuru mērķis ir nodrošināt klasificētās informācijas aizsardzību pret tās neatļautu fizisku iegūšanu, nozaudēšanu, izpaušanu vai kompromitēšanu tās apstrādes, tai skaitā klasificētu informāciju saturošas mutvārdu saziņas (sarunas, diskusijas, rīkojumi, pavēles, telefona sarunas, videokonferences), un glabāšanas laikā.

46. Fiziskās drošības vidi, kurā var tikt apstrādāta klasificētā informācija, iedala šādās zonās:

46.1. 1. drošības zona;

46.2. 2. drošības zona;

46.3. administratīvā drošības zona.

47. Administratīvā drošības zona atbilst šādām prasībām:

47.1. tai ir vizuāli nosakāms, kontrolējams un institūcijas normatīvajā aktā aprakstīts perimetrs;

47.2. tai ir nodrošināta institūcijas vadītāja apstiprināta caurlaižu kārtība, un tās ietvaros tiek nodrošināta nepiederošu personu pavadīšana;

47.3. perimetrā esošie logi un durvis, kas nodrošina iekļūšanu administratīvajā drošības zonā, atbilst vismaz Eiropas Savienības standarta EN 1627 RC2 drošības klasei, un tos pieslēdz pie apsardzes signalizācijas, kas spēj konstatēt to neautorizētu atvēršanu;

47.4. būvkonstrukcijām nodrošina skaņas izolāciju atbilstoši Latvijas būvnormatīvu prasībām, kādas piemēro biroja telpām.

48. Institūcijās, kurās apstrādā un glabā konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju, piekļuvi 1. vai 2. drošības zonai organizē caur administratīvo drošības zonu.

49. Institūcija izstrādā un ar kompetento valsts drošības iestādi vai Nacionālās drošības iestādi, ja tas saistīts ar NATO, Eiropas Savienības vai ārvalstu klasificēto informāciju, saskaņo risku novērtējumu, kurā ir ietvertas minimālās drošības prasības. Kompetentā valsts drošības iestāde vai Nacionālā drošības iestāde, ņemot vērā risku novērtējumu, var pieļaut atkāpes no šajos noteikumos minētajām fiziskās drošības prasībām vai noteikt papildu fiziskās drošības prasības.

3.2. Konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas

50. Telpu var noteikt par 1. drošības zonu, ja, tai piekļūstot, konfidenciāla vai augstākas slepenības pakāpes klasificētā informācija ir atklātā veidā pieejama un ja telpa atbilst šādām prasībām:

50.1. tai patstāvīgi piekļūt var tikai institūcijas vadītāja norīkota persona, kurai ir speciālā atļauja vai sertifikāts, kas atbilst zonā apstrādājamās un glabātās klasificētās informācijas augstākajai slepenības pakāpei;

50.2. nepiederoša persona tajā iekļūt var tikai šo noteikumu 50.1. apakšpunktā minētās personas pavadībā, ja tiek nodrošināta šajā zonā esošās klasificētās informācijas vizuāla nepieejamība;

50.3. šo noteikumu 51. punktā, 52.3. apakšpunktā un 53. punktā minētajām prasībām.

51. 2. drošības zona atbilst šādām prasībām:

51.1. tai ir vizuāli nosakāms, kontrolējams un institūcijas iekšējā normatīvajā aktā aprakstīts perimetrs;

51.2. tajā ir vizuālas norādes par augstāko slepenības pakāpi zonā apstrādājamai un glabātai klasificētajai informācijai;

51.3. tai ir nodrošināta institūcijas vadītāja apstiprināta caurlaižu kārtība, kā arī personu un, ja attiecināms, autotransporta plūsmas kontrole;

51.4. perimetrā esošās durvis, kas nodrošina iekļūšanu paaugstinātas drošības zonā:

51.4.1. atbilst vismaz Eiropas Savienības standarta EN 1627 RC3 drošības klasei, un, ja durvis veidotas ar stiklojumu, tad stiklojums atbilst vismaz Eiropas Savienības standarta EN 356 P6B drošības klasei;

51.4.2. ir nodrošinātas pret to izcelšanu no virām;

51.4.3. ir nostiprinātas sienu konstrukcijā atbilstoši drošības klasei noteiktajām rekomendācijām;

51.5. perimetrā esošie logi atbilst vismaz Eiropas Savienības standarta EN 1627 RC3 drošības klasei, un tiek ievērots viens no šādiem nosacījumiem:

51.5.1. loga stiklojums atbilst vismaz Eiropas Savienības standarta EN 356 P6B drošības klasei;

51.5.2. ailes papildina ar tērauda restēm, kas veidotas no vismaz 17 mm bieziem tērauda stieņiem, kas krustpunktos savstarpēji sametināti ar soli, ne lielāku par 150 x 150 mm, un nostiprinātas logu ailē vismaz sešos punktos ar enkurskrūvēm vismaz 10 mm diametrā un 100 mm dziļumā;

51.5.3. ailes papildina ar Eiropas Savienības standarta EN 1627 RC3 drošības klasei atbilstošām tērauda rullo žalūzijām;

51.6. perimetrā esošiem logiem, caur kuriem ir fiziski iespējama iekļūšana paaugstinātas drošības zonā (piemēram, ēkas pirmais stāvs), piemēro šo noteikumu 51.5.2. apakšpunktā minēto drošības pasākumu vai logu ailes papildina ar Eiropas Savienības standarta EN 1627 RC3 drošības klasei atbilstošām tērauda rullo žalūzijām;

51.7. šo noteikumu 51.5.1. un 51.5.2. apakšpunktā minētajos gadījumos, ja attiecīgajā telpā veic darbu vai glabā klasificēto informāciju, īsteno papildu drošības pasākumus, kas liedz no ārpuses vizuāli novērot telpā notiekošo;

51.8. neveido zonai caurejošas vēdināšanas sistēmas, dūmkanālus vai kabeļu šahtas. Ja tādas ir un to šķērsgriezuma laukums ir lielāks par 1200 cm^2 vai diametrs ir vismaz 35 cm vietā, kur tiek šķērsots zonas perimetrs, tad tās nodrošina pret nepiederošu personu piekļūšanu tām;

51.9. būvkonstrukcijām starp darba telpām, darba telpām un kāpņu telpām, gaiteņiem, hallēm un vestibilu norobežojošām konstrukcijām ar tajās iekļautajām durvju, logu vai to kompleksu konstrukcijām nodrošina skaņas izolāciju R`w(dB)48. Durvju konstrukcijas skaņas izolācijas indekss nav mazāks kā R`w(dB)33;

51.10. ārējā perimetra sienu risinājumus veido no sertificētiem materiāliem, kas spiedē jebkurā konstrukcijas elementā iztur 10 N/mm^2 lineāru spiedienu uz konstrukciju;

51.11. ārējā perimetra pārseguma konstrukcijas veido no sertificētiem materiāliem, kas nodrošina izkliedēto slodzi uz konstrukciju ne mazāku kā 700 kg/m^2.

52. Nepiederoša persona, kura:

52.1. ir attiecīgās institūcijas darbinieks vai amatpersona, var piekļūt 2. drošības zonai un pārvietoties tajā bez pavadības, ja personai ir izsniegta vismaz trešās kategorijas speciālā atļauja;

52.2. nav attiecīgās institūcijas darbinieks, amatpersona vai saimnieciska rakstura darbu veicējs, var piekļūt 2. drošības zonai un pārvietoties tajā autorizētas personas pavadībā, ja personai ir izsniegta vismaz trešās kategorijas speciālā atļauja;

52.3. ir saimnieciska rakstura darbu veicējs, var piekļūt 2. drošības zonai, darbus veicot tikai autorizētas personas fiziskā uzraudzībā. Koplietošanas telpās šo personu uzraudzību var veikt ar tehniskiem līdzekļiem.

53. Šo noteikumu 52.3. apakšpunktā minētajai personai ir nepieciešama vismaz trešās kategorijas speciālā atļauja. Personu bez speciālās atļaujas atļauts piesaistīt gadījumos, ja attiecīgo saimnieciskā rakstura darbu veikšanai nav pieejamas personas, kurām ir izsniegta vismaz trešās kategorijas speciālā atļauja. Šādas personas piesaistīšanu pirms darbu veikšanas saskaņo ar kompetento valsts drošības iestādi.

54. Fiziskās drošības vidi veido tā, lai radītu daudzpakāpju fizisko drošību konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas aizsardzībai. Institūcija izstrādā un ar kompetento valsts drošības iestādi saskaņo drošības procedūras, kurās:

54.1. apraksta drošības zonas un to sadalījumu;

54.2. nosaka klasificētās informācijas augstākās slepenības pakāpi un formu, kādā to atļauts institūcijā apstrādāt un glabāt;

54.3. nosaka caurlaižu īstenošanas kārtību, definējot piekļuves noteikumus un procedūras katrai no drošības zonām, autorizētām un nepiederošām personām, ārpakalpojumu sniedzējiem un apmeklētājiem;

54.4. nosaka telpu uzkopšanas un citu saimniecības darbu veikšanas kārtību katrā no drošības zonām, ja to izpildei piesaista ārpakalpojumu;

54.5. nosaka darbinieku, amatpersonu un apsargu pilnvaras un pienākumus, kā arī kārtību, kādā tiek nodrošināta apsardze.

55. Glabātava ir telpa, kurā konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju var glabāt brīvi pieejamā formā, piemēram, izmantojot plauktu sistēmas vai ekvivalentus risinājumus, kā arī tā atbilst šādām drošības un tehniskām prasībām:

55.1. tā atbilst 1. drošības zonas prasībām;

55.2. telpa ir bez logiem;

55.3. telpas durvis ir sertificētas atbilstoši Eiropas Savienības standarta EN 1143-1 3. drošības klasei vai Eiropas Savienības standarta EN 1627 RC5 drošības klasei, durvju konstrukcija ir nostiprināta sienu konstrukcijā un tiek izmantotas slēdzenes atbilstoši durvju drošības klasei noteiktajām prasībām, kā arī tās ir nodrošinātas pret to izcelšanu no virām;

55.4. telpas konstruktīvie risinājumi (sienas, grīda un griesti) atbilst vienam no šādiem risinājumiem:

55.4.1. izmantota monolītbetona liešanas metode ar sienas minimālo biezumu 150 mm, nodrošinot

minimālo lietderīgo slodzi uz konstrukciju, ne mazāku kā 2000 kg/m^2. Izmanto C30/C37 klases industriālā betona maisījumu vai Eiropas Savienības ietvaros apstiprinātu ekvivalentu;

55.4.2. izmantoti savstarpēji savienojami, noenkurojami, rūpnieciski ražoti sertificēti paneļi, kuri atbilst Eiropas Savienības standarta EN 1143-1 3. drošības klasei vai Eiropas Savienības standarta EN 1627 RC5 drošības klasei un nodrošina šo noteikumu 55.4.1. apakšpunktā minēto lietderīgo slodzi uz konstrukciju.

56. Arhīvs ir telpa, kurā konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju glabā seifos, kas atbilst šo noteikumu 66. punktā minētajām prasībām. Šādu telpu izvieto 2. drošības zonā, un:

56.1. tai piemēro šo noteikumu 51.1., 51.2., 51.3., 51.4., 51.7., 51.8. un 51.9. apakšpunktā minētās prasības;

56.2. tai piemēro šo noteikumu 51.5.2. vai 51.5.3. apakšpunktā minētās prasības;

56.3. telpas konstruktīvo risinājumu veido no sertificētiem materiāliem, kas spiedē jebkurā konstrukcijas elementā iztur 15 N/mm^2 lineāru spiedienu uz konstrukciju un līdz 10 N/mm^2 lineāru spiedienu liecē 1 m augstumā konstrukcijas vertikālās plaknes vidusdaļā, vienlaikus nodrošinot lietderīgo slodzi uz konstrukciju, ne mazāku kā 1800 kg/m^2. Šī prasība netiek attiecināta uz logiem un durvīm.

57. Akreditētas informācijas sistēmas serveru un elektronisko sakaru iekārtu telpa ir telpa, kurā uzstāda konfidenciālas un augstākas slepenības pakāpes akreditētas informācijas sistēmas apstrādes, glabāšanas un sakaru iekārtas, kas nav lietotāju gala iekārtas. Šādu telpu izvieto 2. drošības zonā, un:

57.1. tai piemēro šo noteikumu 51.1., 51.2., 51.3., 51.4., 51.7., 51.8. un 51.9. apakšpunktā minētās prasības;

57.2. tai piemēro šo noteikumu 51.5.2. vai 51.5.3. apakšpunktā minētās prasības;

57.3. telpas konstruktīvo risinājumu veido no sertificētiem materiāliem, kas spiedē jebkurā konstrukcijas elementā iztur 15 N/mm^2 lineāru spiedienu uz konstrukciju un līdz 10 N/mm^2 lineāru spiedienu liecē 1 m augstumā konstrukcijas vertikālās plaknes vidusdaļā, vienlaikus nodrošinot lietderīgo slodzi uz konstrukciju, ne mazāku kā 700 kg/m^2. Šī prasība netiek attiecināta uz logiem un durvīm.

58. Drošā sarunu telpa ir sanāksmju telpa, kurā organizē konfidenciālas un augstākas slepenības pakāpes sanāksmes mutvārdu saziņas formā vai izmantojot audio apskaņošanas aprīkojumu vai videokonferences aprīkojumu. Šādu telpu izvieto 2. drošības zonā vai, ņemot vērā šo noteikumu 49. punktā minētā risku novērtējuma rezultātus, administratīvajā drošības zonā. Drošā sarunu telpa atbilst šādām prasībām:

58.1. telpā nodrošina vismaz 65 dB akustisko vājinājumu uz tuvāko punktu, kurā nav iespējams nodrošināt principa "nepieciešamība zināt" ievērošanu;

58.2. telpai piemēro šo noteikumu 51.1., 51.2. un 51.3. apakšpunktā minētās prasības;

58.3. telpai nav logu;

58.4. telpā drīkst uzstādīt tikai ar kompetento valsts drošības iestādi iepriekš saskaņotus priekšmetus, iekārtas un komunikācijas;

58.5. telpā veikta pārbaude neautorizētu iekārtu klātbūtnes konstatēšanai, par katru pārbaudi saglabājot pārbaudes atskaiti. Pārbaudes veic:

58.5.1. pirms telpu uzsāk izmantot;

58.5.2. vismaz reizi gadā;

58.5.3. ja ir aizdomas par neautorizētu piekļuvi telpai;

58.6. telpai drīkst patstāvīgi piekļūt tikai autorizētas personas, kas nodrošina telpas lietošanas noteikumu ievērošanu;

58.7. telpā ir aizliegts ienest jebkādas neautorizētas, raidošas, ierakstošas iekārtas, piemēram, mobilos tālruņus, planšetdatorus, viedpulksteņus.

59. Telpai, kurā apstrādā konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju elektroniski, papildus šajos noteikumos noteiktajām fiziskās drošības prasībām Nacionālā drošības iestāde nosaka telpas elektromagnētiskā starojuma vājinājuma līmeni, kas ietekmē drošības prasības šajās telpās uzstādāmajām informācijas sistēmas iekārtām. Elektromagnētiskā starojuma vājinājuma līmeņa noteikšanas mērījumu veikšanai institūcija Nacionālajai drošības iestādei iesniedz:

59.1. telpu plānus trijās dimensijās, identificējot telpas, kurām nepieciešams veikt mērījumus, un institūcijas telpu ārējās robežas;

59.2. detalizētu ārējās vides attēlojumu trijās dimensijās, iekļaujot, piemēram, ēkas augstākos vai zemākos stāvus un ēkas vai objektus, kas atrodas institūcijai tiešā tuvumā;

59.3. telpā uzstādāmās informācijas sistēmas aprakstu un paredzētās apstrādājamās klasificētās informācijas slepenības pakāpi.

60. Elektromagnētiskā starojuma vājinājuma līmeņa noteikšanu telpām veic ne retāk kā reizi piecos gados vai pēc būtiskām izmaiņām telpas uzbūvē.

61. Apsardzes signalizācijas komponentes telpās, kurās apstrādā un glabā konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju, atbilst vismaz Eiropas Savienības standarta EN 50133 2. drošības klasei. Šo noteikumu 55., 56., 57. un 58. punktā minētās telpas, kā arī telpas, kas veido drošības zonas perimetru, aprīko ar apsardzes signalizāciju, kuras visas komponentes atbilst vismaz Eiropas Savienības standarta EN 50133 3. drošības klasei. Apsardzes signalizācijas lietotāju nodrošina ar individuālu aktivizācijas kodu, kas pieejams tikai konkrētās telpas lietotājam. Apsardzei nav tiesību deaktivēt telpas apsardzes signalizāciju.

62. Šo noteikumu 55., 56., 57. un 58. punktā minēto telpu durvis un 1. un 2. drošības zonas piekļuves durvis kontrolē ar videonovērošanas sistēmu, kas atbilst šādām prasībām:

62.1. katra videokamera nodrošina vismaz 720 stundas ilgu videosignāla ierakstu, no kura iespējams izgūt attēlu kvalitātē ar vismaz 1280 līniju izšķirtspēju vienā no asīm;

62.2. izvietojot videonovērošanas sistēmas, videokameras nodrošina, ka videoierakstā netiek ierakstīti dažādās drošības sistēmās ievadītie sistēmu aktivizācijas kodi, akreditētu informācijas sistēmu monitori vai vide, kuras ietvaros var tikt tieši eksponēta klasificētā informācija.

63. Šo noteikumu 55., 56., 57. un 58. punktā minēto telpu durvis un 1. un 2. drošības zonas piekļuves durvis, kā arī jebkuru citu telpu, kurā organizē darbu ar konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju, aprīko ar piekļuves kontroles sistēmu, kas nodrošina dažādu lietotāju tiesību piešķiršanas iespēju. Piekļuves kontroles sistēma šo noteikumu 55., 56., 57. un 58. punktā minēto telpu durvīm un 1. un 2. drošības zonas piekļuves durvīm nodrošina vismaz divu līmeņu lietotāju autentifikāciju, piemēram, piekļuves karte un kods, biometrija un piekļuves karte vai biometrija un kods.

64. Šo noteikumu 61., 62. un 63. punktā minētās sistēmas:

64.1. atvienošanas gadījumā no elektrotīkla spēj darboties šo noteikumu 49. punktā minētā risku novērtējuma rezultātos noteikto laiku, līdz iespējams īstenot paredzētos pretpasākumus;

64.2. veidotas kā institūcijas iekšējas, slēgtas sistēmas, kuras kontrolē no telpas, kur pastāvīgi uzturas apsardze. Ārēji starpsavienojumi ir atļauti, ja tie ir izvērtēti šo noteikumu 49. punktā minētā risku novērtējuma ietvaros;

64.3. nodrošina ar sistēmas administratora tiesību profilu un sistēmas inženiera tiesību profilu. Sistēmas administrators piešķir, maina un bloķē lietotāju tiesības, kā arī piešķir sistēmas inženierim, piemēram, uz sistēmas apkopes vai remontdarbu veikšanas laiku, piekļuves tiesības sistēmas datiem un komponentēm. Sistēmas administratora funkcijas pilda autorizēta persona. Sistēmas inženiera funkcijas var veikt autorizēta

persona vai ārpakalpojuma sniedzēja darbinieks, ja ārpakalpojuma sniedzējam ir spēkā esošs vismaz trešās kategorijas industriālās drošības sertifikāts, bet darbiniekam – trešās kategorijas speciālā atļauja;

64.4. darbspējas un kvalitātes kontroli veic ne retāk kā reizi gadā, par to sagatavojot attiecīgu aktu;

64.5. arhīva datiem ir tiesīga piekļūt tikai autorizēta persona;

64.6. piekļuves tiesību drošības kodu maina ne retāk kā reizi gadā vai ja ir aizdomas par tā nonākšanu nepiederošu personu rīcībā, kā arī ja persona pārtrauc amata vai dienesta attiecības.

65. Izņēmuma gadījumā darbs vienas darbdienas ietvaros ar konfidenciālu un slepenu klasificēto informāciju fiziskā formā var tikt organizēts administratīvajā drošības zonā, ja šo noteikumu 37.8. apakšpunktā minētajā iekšējā normatīvajā aktā ir noteikts šā procesa drošības procedūru apraksts. Klasificētās informācijas drošību šā izņēmuma ietvaros nodrošina institūcijas slepenības režīma vai sevišķās lietvedības organizētājs.

66. Konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju glabā seifā, ievērojot, ka:

66.1. sevišķi slepenu klasificēto informāciju glabā atsevišķā Eiropas Savienības standarta EN 1143-1 3. drošības klasei atbilstošā seifā atdalīti, katru klasificētās informācijas veidu ievietojot seifa atsevišķos nodalījumos;

66.2. konfidenciālu un slepenu klasificēto informāciju atļauts glabāt vienā Eiropas Savienības standarta EN 1143-1 2. drošības klasei atbilstošā seifā atdalīti, katru klasificētās informācijas veidu ievietojot seifa atsevišķos nodalījumos;

66.3. uz seifa norāda šādu informāciju:

66.3.1. par seifu atbildīgās personas vārdu, uzvārdu vai citus personas identifikācijas datus un tālruņa numuru, lai nodrošinātu iespēju sazināties ar viņu ārkārtas situācijā vai gadījumā, ja seifs atrasts atvērts;

66.3.2. seifa uzskaites vai identifikācijas numuru;

66.3.3. seifa koda kombinācijas maiņas datumu, ja koda nomaiņas ciklu institūcijā kontrolē katrs darbinieks vai amatpersona;

66.4. seifa koda kombināciju maina:

66.4.1. ja pārtrauc amata vai dienesta attiecības ar personu, kura ir atbildīga par seifu;

66.4.2. ja ir aizdomas, ka seifa koda kombinācija ir kļuvusi zināma nepiederošām personām;

66.4.3. ne retāk kā reizi 24 mēnešos;

66.5. seifa kodu kombinācijas un seifa atslēgu viens eksemplārs kopā ar informāciju par seifa uzskaites numuru, atrašanās vietu un atbildīgo personu identificējošiem datiem (vārds, uzvārds, pārstāvētā institūcija un amats) glabā penālī vai aploksnē slepenības režīma nodrošinātāja vai institūcijas vadītāja seifā, kas atbilst šo noteikumu 66.2. apakšpunktā noteiktajām prasībām. Uz penāļa vai aploksnes aizdares vietas ir par seifu atbildīgās personas zīmoga (spiedoga) nospiedums vai paraksts. Zīmogojumu vai parakstu nosedz ar caurspīdīgu līmlenti vai citu iepakojumam piemērotu materiālu;

66.6. lietotāja seifa atslēgas ikdienas glabāšanas kārtību slepenības režīma nodrošinātājs nosaka šo noteikumu 37.8. apakšpunktā minētā aizsardzības pasākumu kopuma ietvaros.

67. Pēc darba laika beigām, izejot no telpas, kurā veic darbu vai glabā klasificēto informāciju, veic šādas darbības:

67.1. pārbauda, vai klasificētā informācija ir ievietota seifā, aizslēdz seifu, kā arī aizver logus un, ja ir, šo noteikumu 51.5.3. apakšpunktā minētās žalūzijas;

67.2. aizslēdz ieejas durvis;

67.3. pievieno telpai signalizāciju.

68. Sevišķi slepenu klasificēto informāciju atļauts glabāt šo noteikumu 55., 56., 57. un 58. punktā minētajās telpās vai citā speciāli izmantojamā telpā, kas iepriekš saskaņota un sertificēta kompetentajā valsts drošības iestādē vai Nacionālajā drošības iestādē, ja glabā NATO vai Eiropas Savienības atbilstošas kategorijas klasificēto informāciju.

69. Institūcijā apsardzes funkcijas vienlaikus īsteno ne mazāk kā divas personas. Apsardzes funkciju īstenošanā ārpakalpojuma sniedzējam ir jābūt spēkā esošam vismaz trešās kategorijas industriālās drošības sertifikātam un vismaz vienam no maiņā esošajiem apsardzes darbiniekiem – trešās kategorijas speciālajai atļaujai, ja ar līguma nosacījumiem un tehniskiem līdzekļiem apsardzes darbiniekam ir liegta piekļuve 1. un 2. drošības zonai. Ja apsardzes darbinieka funkcijas paredz arī iekļūšanu 1. un 2. drošības zonā, apsardzes ārpakalpojuma sniedzējam ir nepieciešams 1. un 2. drošības zonā apstrādātās klasificētās informācijas augstākajai slepenības pakāpei atbilstošs industriālās drošības sertifikāts, bet darbiniekiem atbilstošas kategorijas speciālās atļaujas.

70. Pamatojoties uz šo noteikumu 49. punktā minētā risku novērtējuma rezultātiem, apsardzes nodrošināšanā var izmantot arī tehniskās apsardzes pakalpojumu, ievērojot šo noteikumu 69. punktā minētās industriālā drošības sertifikāta un speciālās atļaujas esības prasības.

71. Fiziskās drošības vides iedalījumu zonās un zonas un telpu piemērotību konfidenciālu un augstākas slepenības pakāpes valsts noslēpuma objektu apstrādei un glabāšanai atbilstoši kompetencei pārbauda un rakstveida atzinumu sniedz kompetentā valsts drošības iestāde vai Nacionālā drošības iestāde, ja apstrādā vai glabā konfidenciālas un augstākas slepenības pakāpes NATO vai Eiropas Savienības klasificēto informāciju. Kompetentā valsts drošības iestāde vai Nacionālā drošības iestāde var iepazīties ar telpu izbūves darbu pieņemšanas aktiem, lai izvērtētu telpu atbilstību šajos noteikumos minētajām prasībām.

72. Šo noteikumu 71. punktā minētajā atzinumā norāda:

72.1. kompetentās valsts drošības iestādes nosaukumu, kas veica pārbaudi;

72.2. pārbaudāmās institūcijas nosaukumu un adresi;

72.3. apstrādājamās vai uzglabājamās klasificētās informācijas augstāko slepenības pakāpi;

72.4. pārbaudāmo telpu nosaukumus un numurus;

72.5. atļauju konkrētajās telpās glabāt klasificēto informāciju;

72.6. konstatēto fiziskās drošības situāciju;

72.7. konstatētos trūkumus, ja tādi ir;

72.8. norādi par atzinuma derīguma termiņu, kas nedrīkst pārsniegt piecus gadus;

72.9. pārbaudāmās institūcijas pārstāvjus, kas piedalījās pārbaudē.

73. Institūcijai ir pienākums iesniegt kompetentajai valsts drošības iestādei vai Nacionālajai drošības iestādei, ja telpās apstrādā vai glabā NATO vai Eiropas Savienības klasificēto informāciju, pieteikumu atkārtota šo noteikumu 71. punktā minētā atzinuma saņemšanai ne vēlāk kā sešus mēnešus pirms šo noteikumu 72.8. apakšpunktā minētā termiņa beigām.

74. Kompetentās valsts drošības iestādes atbilstoši kompetencei uztur veikto telpu pārbaužu statusu aktuālo sarakstu.

75. Organizējot mācības, konferences, seminārus vai cita tipa pasākumus, kuros ir paredzēta konfidenciālas un

augstākas slepenības pakāpes klasificētās informācijas apstrāde ārpus sertificētām telpām, par pasākumu atbildīgā institūcija:

75.1. vismaz trīs mēnešus pirms pasākuma sākuma informē kompetento valsts drošības iestādi un Nacionālo drošības iestādi, ja paredzēts apstrādāt konfidenciālu un augstākas slepenības pakāpes NATO vai Eiropas Savienības klasificēto informāciju;

75.2. izstrādā un ar kompetento valsts drošības iestādi un Nacionālo drošības iestādi, ja paredzēts apstrādāt konfidenciālu un augstākas slepenības pakāpes NATO vai Eiropas Savienības klasificēto informāciju, saskaņo fiziskās drošības pasākumus un klasificētās informācijas apstrādes un aprites procedūras. Par klasificētās informācijas drošības noteikumu ievērošanu šāda pasākuma laikā atbild institūcija, kas to organizē.

76. Piedaloties militārās operācijās, ievēro militārās operācijas vadošās valsts noteiktās klasificētās informācijas drošības noteikumus un procedūras.

77. Avārijas dienesta darbinieku, ugunsdzēsēju, ātrās medicīniskās palīdzības brigādi, kā arī izmeklēšanas iestādes pārstāvi (ja ir noticis noziedzīgs nodarījums) teritorijā un telpās, kurās veic darbu ar konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju, ielaiž un ļauj tajās uzturēties apsardzes vai par slepenības režīma nodrošināšanu atbildīgā darbinieka vai amatpersonas klātbūtnē, ja tas neapdraud iesaistīto personu veselību un dzīvību.

3.3. Dienesta vajadzībām klasificētās informācijas fiziskā drošība

78. Dienesta vajadzībām klasificēto informāciju ir atļauts apstrādāt un uzglabāt paaugstinātas drošības zonā vai administratīvajā zonā. Administratīvā zona var būt arī atsevišķa telpa. Telpā, kurā apstrādā un uzglabā dienesta vajadzībām klasificēto informāciju, nepiederoša persona uzturas tikai institūcijas darbinieka vai amatpersonas klātbūtnē.

79. Darbu ar dienesta vajadzībām klasificēto informāciju mutvārdu saziņas formā vai izmantojot audio apskaņošanas aprīkojumu vai videokonferences aprīkojumu, nodrošina telpā:

79.1. kurā dienesta vajadzībām klasificētās informācijas apstrādes laikā ir iespējama tikai kontrolēta piekļuve;

79.2. kurā ir ieviesti papildu drošības pasākumi, kas liedz no ārpuses vizuāli novērot telpā notiekošo.

80. Šo noteikumu 79. punktā minētajā gadījumā nodrošina, ka dalībnieki telpā neienes vai izslēdz visas raidošas vai ierakstošas iekārtas, piemēram, mobilos tālruņus, planšetdatorus, viedpulksteņus. Par šo procedūru atbild sanāksmes vadītājs. Sanāksmes laikā atļauts izmantot tikai iekārtas, kas šajos noteikumos noteiktajā kārtībā ir akreditētas dienesta vajadzībām klasificētās informācijas apstrādei.

81. Pēc darba laika beigām, izejot no telpas, kurā veic darbu vai glabā dienesta vajadzībām klasificēto informāciju, veic šādas darbības:

81.1. ja telpā amata vai dienesta pienākumus pilda vairākas personas, dienesta vajadzībām klasificēto informāciju ievieto biroja mēbelēs, metāla skapī vai seifā un to aizslēdz;

81.2. aizver logus un aizslēdz ieejas durvis;

81.3. pievieno telpai signalizāciju.

82. Saimnieciska rakstura darbus vai uzkopšanu telpā, kurā notiek dienesta vajadzībām klasificētās informācijas apstrāde vai glabāšana, veic institūcijas darbinieka vai amatpersonas klātbūtnē, kura attiecīgajā telpā ikdienā strādā. Pirms šādu darbu veikšanas nodrošina, ka dienesta vajadzībām klasificētā informācija nav pieejama saimnieciska rakstura vai uzkopšanas darbu veicējam.

83. Institūcija izstrādā un ar kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja tas saistīts ar NATO, Eiropas Savienības vai ārvalstu dienesta vajadzībām klasificētās informācijas apstrādi, saskaņo procedūras, kā amata vai dienesta pienākumu izpildei dienesta vajadzībām klasificētā informācija var tikt apstrādāta ārpus administratīvai drošības zonai noteiktām drošības prasībām atbilstošām telpām, piemēram, mājās vai viesnīcā, nosakot, ka:

83.1. dienesta vajadzībām klasificēto informāciju pastāvīgi apstrādā, izmantojot akreditētu informācijas sistēmu;

83.2. dienesta vajadzībām klasificēto informāciju papīra formā apstrādā tikai viena pasākuma ietvaros, piemēram, komandējumā vai sanāksmē;

83.3. darbinieks vai amatpersona pārliecinās, ka apstrādes laikā dienesta vajadzībām klasificētā informācija nekļūst pieejama nepiederošai personai.

84. Institūcijai ir pienākums pirmreizējai, kā arī ne retāk kā reizi piecos gados atkārtotai pārbaudei iesniegt kompetentajai valsts drošības iestādei vai Nacionālajai drošības iestādei, ja tas saistīts ar NATO, Eiropas Savienības vai ārvalstu dienesta vajadzībām klasificētās informācijas apstrādi, pieteikumu atzinuma sniegšanai par institūcijā ieviesto dienesta vajadzībām klasificētās informācijas fiziskās drošības prasību un aprites procedūru atbilstību šiem noteikumiem. Konstatējot būtiskas atkāpes no šajos noteikumos noteiktajām drošības prasībām, kas nav pamatotas šo noteikumu 49. punktā minētā risku novērtējuma ietvaros, kompetentā valsts drošības iestāde vai Nacionālā drošības iestāde, ja iesaistīta NATO, Eiropas Savienības vai ārvalstu dienesta vajadzībām klasificētā informācija, var ierosināt dienesta izmeklēšanu atbilstoši šiem noteikumiem.

4. Klasificētās informācijas drošība

4.1. Klasificētās informācijas drošības vispārīgie jautājumi

85. Klasificētās informācijas drošība ir procedūru kopums, kas nosaka klasificētās informācijas reģistrācijas, uzskaites, noformēšanas, saņemšanas, nosūtīšanas, transportēšanas, pavairošanas, tulkošanas, glabāšanas, digitalizācijas, iznīcināšanas, kontroles un deklasificēšanas kārtību.
(MK 09.06.2026. noteikumu Nr. 320 redakcijā)

86. Sevišķo lietvedību darbam ar konfidenciāliem un augstākas slepenības pakāpes valsts noslēpuma objektiem pārbauda kompetentā valsts drošības iestāde. Apakšreģistru un kontrolpunktu darbam ar konfidenciālu un augstākas slepenības pakāpes NATO un Eiropas Savienības klasificēto informāciju pārbauda Nacionālā drošības iestāde.

87. Sevišķās lietvedības, centrālā reģistra biroja, apakšreģistra vai kontrolpunkta atbilstības pārbaude šiem noteikumiem notiek vienlaikus ar šo noteikumu 71. punktā minēto pārbaudi, sagatavojot vienu atzinumu. Atzinumā papildus šo noteikumu 72. punktā minētajai informācijai norāda:

87.1. novērtējumu par institūcijā ieviesto klasificētās informācijas drošības procedūru atbilstību šiem noteikumiem;

87.2. novērtējumu par institūcijā izstrādāto informācijas aizsardzības iekšējo normatīvo aktu atbilstību šiem noteikumiem;

87.3. klasificētās informācijas esības pārbaudes rezultātus (ja veikta atkārtota pārbaude).

88. Valsts drošības iestādes atbilstoši kompetencei uztur sevišķās lietvedības, centrālā reģistra biroja, apakšreģistru un kontrolpunktu pārbaužu statusu aktuālo sarakstu.

89. Darbs ar konfidenciālu un augstākas slepenības pakāpes ārvalstu klasificēto informāciju pieļaujams institūcijā, kurā ir pārbaudīta sevišķā lietvedība darbam ar valsts noslēpumu un ir saņemts saskaņojums no Nacionālās drošības

iestādes. Institūcija, uzsākot darbu ar ārvalstu klasificēto informāciju, informē Nacionālo drošības iestādi.

4.2. Klasificētās informācijas marķēšana un noformēšana

90. Valsts noslēpuma objektu, NATO un Eiropas Savienības klasificēto informāciju marķē un noformē, ievērojot, ka (9. pielikums):

90.1. dokumenta katras lappuses augšējās malas un apakšējās malas vidū izdara atzīmi par konkrētajā lappusē ietvertās informācijas slepenības pakāpi:

90.1.1. "SEVIŠĶI SLEPENI", "SLEPENI", "KONFIDENCIĀLI", "DIENESTA VAJADZĪBĀM";

90.1.2. "COSMIC TOP SECRET", "NATO SECRET", "NATO CONFIDENTIAL", "NATO RESTRICTED";

90.1.3. "TRES SECRET UE/EU TOP SECRET", "SECRET UE/EU SECRET", "CONFIDENTIEL UE/EU CONFIDENTIAL", "RESTREINT UE/EU RESTRICTED";

90.2. atsevišķām dokumenta sastāvdaļām, piemēram, teksta rindkopai, punktam vai apakšpunktam, atbilstoši ietvertajai informācijai var piešķirt dažādas slepenības pakāpes, izmantojot speciālus saīsinātus apzīmējumus:

90.2.1. "SEVIŠĶI SLEPENI" – (SS), "SLEPENI" – (S), "KONFIDENCIĀLI" – (K), "DIENESTA VAJADZĪBĀM" – (DV), bet sastāvdaļām, kuras nesatur valsts noslēpumu, – (N) vai kādu citu normatīvajos aktos noteikto aizsargājamas informācijas marķējumu;

90.2.2. "COSMIC TOP SECRET" – (CTS), "NATO SECRET" – (NS), "NATO CONFIDENTIAL" – (NC), "NATO RESTRICTED" – (NR), bet sastāvdaļām, kuras nesatur NATO klasificēto informāciju, – (NU) vai kādu citu NATO aizsargājamās informācijas marķējumu;

90.2.3. "TRES SECRET UE/EU TOP SECRET" – (TSUE/EUTS), "SECRET UE/EU SECRET" – (SUE/EUS), "CONFIDENTIEL UE/EU CONFIDENTIAL" – (CUE/EUC), "RESTREINT UE/EU RESTRICTED" – (RUE/EUR), bet sastāvdaļām, kuras nesatur Eiropas Savienības klasificēto informāciju, kādu citu Eiropas Savienības aizsargājamās informācijas marķējumu;

90.3. dokumenta lappuses numurē katras lappuses apakšējā malā ar arābu cipariem, norādot lappuses kārtas numuru un aiz domuzīmes – dokumenta kopējo lappušu skaitu;

90.4. papīra dokumenta lappusi, uz kuras nav informācijas, nenumurē un tās vidū izdara norādi: "Šī lappuse nav izmantota." Gadījumā, ja šo dokumentu sagatavo citā valodā, izmanto šīs norādes tulkojumu attiecīgajā valodā;

90.5. konfidenciālam un augstākas slepenības pakāpes valsts noslēpuma objektam atzīmi par klasifikācijas pamatojumu un termiņu norāda dokumenta pirmās lappuses apakšējā labajā pusē;

90.6. nosūtāmo dokumentu var papildināt ar norādi par tā iznīcināšanu, ja pastāv noteikti apstākļi, piemēram, ja ir izstrādāta informatīvā ziņojuma jauna versija, iepriekšējo versiju var iznīcināt, vai pēc noteikta laika, piemēram, pārskats par konkrētu tēmu, kas pēc zināma laika zaudē savu aktualitāti;

90.7. institūcijas organizatorisku dokumentu, rīkojuma dokumentu, privāto un publisko tiesību līgumu vai personāla dokumentu papildina ar norādi, ka attiecīgā dokumenta slepenības pakāpi nepārskata, kamēr tas ir spēkā;

90.8. elektronisku datu nesēju marķē ar klasificētās informācijas augstāko slepenības pakāpi, kādu paredzēts uz tā apstrādāt, elektroniskā datu nesēja reģistrācijas numuru un institūcijas nosaukumu;

90.9. iekārtas, aprīkojumu un ieročus marķē diskrēti, tikai ar slepenības pakāpi, ņemot vērā to pielietojumu;

90.10. šo noteikumu 90.8. un 90.9. apakšpunktā minētos marķējumus veido atbilstoši šo noteikumu 98. punktā noteiktajām krāsām.

91. Sagatavojot valsts noslēpuma objektu, NATO vai Eiropas Savienības klasificēto informāciju saturošu elektronisku dokumentu un papīra dokumentu nestandarta formā, piemēram, fotogrāfiju, topogrāfisko karti, zīmējumu vai plānu, kuru nav iespējams marķēt šo noteikumu 90. punktā noteiktajā kārtībā, elektronisko dokumentu papildina ar atsevišķu datni, bet papīra dokumentu ar šo noteikumu 113. punktā minēto pavadvēstuli, kurā iekļauj šo noteikumu 90.1., 90.5., 90.6. un 90.7. apakšpunktā minēto informāciju. Turpmāka šāda valsts noslēpuma objekta, NATO vai Eiropas Savienības klasificētās informācijas apstrāde nav pieļaujama bez pievienotas atsevišķas datnes vai pavadvēstules.

92. Klasificēta elektroniska dokumenta datnes nosaukumā, izmantojot šo noteikumu 90.2. apakšpunktā minētos speciālos saīsinājumus, iekļauj norādi par klasificētā elektroniskā dokumenta slepenības pakāpi.

93. Konfidenciālam un augstākas slepenības pakāpes valsts noslēpuma objektam un NATO klasificētajai informācijai var noteikt speciālās kategorijas marķējumu:

93.1. ATOMAL – speciālās kategorijas marķējums, kuru piešķir ar atomieročiem saistītai NATO klasificētajai informācijai (piemēram, COSMIC TOP SECRET ATOMAL);

93.2. BOHEMIA – speciālās kategorijas marķējums, kuru piešķir signālu izlūkošanā iegūtai NATO klasificētajai informācijai (piemēram, COSMIC TOP SECRET BOHEMIA);

93.3. SIGNAL – speciālās kategorijas marķējums, kuru piešķir signālu izlūkošanā iegūtai valsts noslēpumu saturošai klasificētajai informācijai (piemēram, SLEPENI SIGNAL).

94. Konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju saturoša dokumenta nosaukumam autors var noteikt slepenības pakāpi. Dokumenta nosaukuma slepenības pakāpi norāda, izmantojot šo noteikumu 90.2. apakšpunktā minētos speciālos saīsinājumus. Dienesta vajadzībām klasificēto informāciju saturoša dokumenta nosaukums ir vispārpieejama informācija.

95. Ja vairākus klasificētus dokumentus ar dažādām slepenības pakāpēm apvieno vienā informācijas kopumā (sējums, lieta u. c.), kopumam:

95.1. piešķir augstāko no apvienotajiem klasificētajiem dokumentiem piešķirtajām slepenības pakāpēm;

95.2. nosaka ilgāko no apvienotajiem klasificētajiem dokumentiem noteiktajiem slepenības pakāpes saglabāšanas termiņiem;

95.3. uz vāka, uz pievienotas atsevišķas lapas vai papildus pievienotā atsevišķā datnē norāda visas iekļautās augstākās slepenības pakāpes, piemēram, "SLEPENI", "NATO SECRET", "CONFIDENTIEL UE/EU CONFIDENTIAL";

95.4. tālāk izplatot, ņem vērā visu iekļauto klasificētās informācijas veidu un to slepenības pakāpju izplatīšanas ierobežojumus.

96. Ja, sagatavojot jaunu klasificētu dokumentu, tajā iekļauj informāciju no cita klasificēta dokumenta, tad ievēro, ka:

96.1. iekļautajai informācijai saglabā slepenības pakāpi, kāda tai noteikta oriģinālajā dokumentā;

96.2. piešķirot slepenības pakāpi klasificētajam dokumentam, par tā kopējo slepenības pakāpi nosaka augstāko no atsevišķajās sastāvdaļās, teksta rindkopās, punktos vai apakšpunktos ietvertajām klasificētās informācijas slepenības pakāpēm;

96.3. pirmās lappuses augšējā labajā stūrī norāda visas klasificētajā dokumentā iekļautās klasificētās informācijas augstākās slepenības pakāpes;

96.4. jaunā klasificētā dokumenta autors nodrošina sasaisti ar oriģinālo dokumentu;

96.5. attiecībā uz ārvalstu klasificēto informāciju ņem vērā arī ar konkrēto valsti noslēgto divpusējo līgumu par

klasificētās informācijas aizsardzību.

97. Klasificētā dokumenta atsevišķās neklasificētās daļas, ja tās ir atbilstoši marķētas, atdalot no attiecīgā dokumenta, var izmantot atklāti.

98. Nodrošinot klasificēto informāciju saturoša dokumenta apriti papīra formā, tam pievieno īpašu norādes lapu atbilstoši tā slepenības pakāpei:

98.1. sevišķi slepenu klasificēto informāciju saturošam dokumentam – violetā krāsā;

98.2. slepenu klasificēto informāciju saturošam dokumentam – sarkanā krāsā;

98.3. konfidenciālu klasificēto informāciju saturošam dokumentam – zilā krāsā;

98.4. dienesta vajadzībām klasificēto informāciju saturošam dokumentam – zaļā krāsā.

99. Norādes lapas augšējās un apakšējās malas vidū norāda valsts noslēpuma objekta, NATO vai Eiropas Savienības klasificētās informācijas kopējo slepenības pakāpi atbilstoši šo noteikumu 90.1. apakšpunktam. Ja ir ārvalstu klasificētā informācija, norāda attiecīgās valsts noteikto slepenības pakāpi un salīdzinošo valsts noslēpuma objekta slepenības pakāpi (10. pielikums).

100. Pamatojoties uz šo noteikumu 49. punktā minētā risku novērtējuma rezultātiem, institūcijas ietvaros klasificētu informāciju saturošu dokumentu apritē norādes lapu var neizmantot.

101. Mācību nolūkam izmantotā informācija, kas imitē klasificēto informāciju, uzskatāma par neklasificētu, izņemot gadījumus, ja mācību scenāriju izveidei par pamatu izmanto klasificēto informāciju. Mācību scenāriju, kas ir balstīts uz klasificēto informāciju, un mācības, kurās izmanto klasificēto informāciju, saskaņo ar kompetento valsts drošības iestādi, nosakot atbilstošus mācībās izmantotās klasificētās informācijas aizsardzības pasākumus. Pēc mācībām dokumentam, kas vairs nav nepieciešams un kas satur klasificētās informācijas imitāciju, nepiemēro šajos noteikumos norādīto iznīcināšanas procedūru.

4.3. Klasificētās informācijas reģistrācija un uzskaite

102. Valsts noslēpuma objektu, NATO, Eiropas Savienības un ārvalstu klasificētās informācijas reģistrāciju un uzskaiti organizē šķirti. Sevišķi slepenu klasificēto informāciju reģistrē un uzskaita atsevišķi no pārējās klasificētās informācijas.

103. Saskaņojot ar kompetento valsts drošības iestādi un Nacionālo drošības iestādi, institūcijā valsts noslēpuma objektu, NATO, Eiropas Savienības un ārvalstu klasificētās informācijas reģistrāciju un apriti var organizēt viena persona vai institūcijas struktūrvienība.

104. Iekšējās aprites, nosūtāmo un saņemto klasificēto informāciju reģistrē klasificētās informācijas reģistrācijas un uzskaites sistēmā.

105. Konfidenciālus un augstākas slepenības pakāpes NATO un Eiropas Savienības klasificētos dokumentus un tos saturošus elektroniskos datu nesējus reģistrē centrālā reģistra biroja izveidotā un uzturētā NATO un Eiropas Savienības dokumentu vai elektroniskās informācijas nesēju reģistrācijas un uzskaites sistēmā Nacionālā slepenā tīkla ietvaros. Institūcijai, kurā nav pieejams Nacionālais slepenais tīkls, bet tiek apstrādāti slepenie un sevišķi slepenie NATO un Eiropas Savienības klasificētie dokumenti vai tiek reģistrēti šādu informāciju saturoši elektronisko datu nesēji, no centrālā reģistra biroja triju darbdienu laikā ir jāsaņem vienotais reģistrācijas numurs katrai institūcijas reģistrācijas un uzskaites sistēmā reģistrētai vienībai. Vienotais reģistrācijas numurs no centrālā reģistra biroja ir jāsaņem visām ATOMAL informācijas vienībām.

106. Reģistrējot klasificēto informāciju, fiksē vismaz šādu informāciju:

106.1. par konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju saturošu nosūtāmo dokumentu – šo noteikumu 11. pielikumā minēto informāciju, bet par saņemto dokumentu – šo noteikumu 12. pielikumā minēto informāciju;

106.2. par dienesta vajadzībām klasificēto informāciju saturošu dokumentu norāda autoru, datumu, nosaukumu, reģistrācijas numuru;

106.3. par elektronisko datu nesēju, kuru izmanto atkārtotai klasificēto dokumentu transportēšanai vai apstrādei, norāda reģistrācijas datumu, reģistrācijas numuru, klasificētās informācijas veidus un to augstākās slepenības pakāpes, piederību akreditētai informācijas sistēmai, elektroniskā informācijas nesēja veidu un sērijas numuru (ja tāds ir). Elektronisko datu nesēju, kas paredzēts dažādu klasificētās informācijas veidu apstrādei un uzglabāšanai, reģistrē vienā klasificētās informācijas reģistrācijas un uzskaites sistēmā;

106.4. par iekārtām, aprīkojumu un ieročiem norāda reģistrācijas datumu, reģistrācijas numuru, slepenības pakāpi, ražotāju, aprakstu un sērijas numuru, ja tāds ir.

107. Šo noteikumu 91. punktā minētajā gadījumā uz katra institūcijā saņemtā klasificētā papīra formas dokumenta pirmās lappuses vai pavadvēstules brīvā vietā izdara atzīmi par minētā dokumenta saņemšanu un reģistrāciju, norāda saņēmējas institūcijas nosaukumu, saņemšanas datumu, reģistrācijas numuru un lappušu skaitu.

108. Konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju saturošu dokumentu apritē institūcijā nodrošina piekļuves fakta uzskaiti, ko var veikt fiziski ar personas parakstu vai elektroniski reģistrācijas un uzskaites sistēmā, kas nodrošina elektronisku dokumentu apriti tikai autorizētiem institūcijas lietotājiem.

109. Reģistrācijas un uzskaites sistēmā nodrošina tajā veikto darbību izsekojamību, darbību nenoliegšanu, datu integritāti un autentiskumu.

110. No privāto tiesību subjekta saņemtai informācijai valsts noslēpuma statusu piešķir, ja tā satur valsts noslēpuma objektu. Valsts noslēpuma statusu informācijai var piešķirt un reģistrēt institūcija, kurai ir tiesības apstrādāt valsts noslēpumu un kurai privāto tiesību subjekts to ir adresējis. Saņemto informāciju marķē un reģistrē šajos noteikumos noteiktajā kārtībā, kā arī informē privāto tiesību subjektu par saņemtajai informācijai piešķirto valsts noslēpuma statusu un no tā izrietošajām drošības prasībām.

4.4. Klasificētās informācijas saņemšana un nosūtīšana

111. Institūcija klasificēto informāciju saņem un nosūta tikai ar sevišķās lietvedības, centrālā reģistra biroja, apakšreģistra, kontrolpunkta vai šo noteikumu 33.4. apakšpunktā noteiktā darbinieka vai struktūrvienības starpniecību. Klasificētos dokumentus var saņemt un nosūtīt papīra formā, izmantojot elektronisku datu nesēju vai akreditētu informācijas sistēmu.

112. Organizējot konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju saturoša elektroniska dokumenta apriti akreditētā informācijas sistēmā, nodrošina šo noteikumu 107. punktā minētā saņemšanas apstiprinājuma ekvivalentu.

113. Klasificēto informāciju var pārsūtīt citam adresātam bez pavadvēstules. Ja, pārsūtot informāciju, ir nepieciešams sniegt saņēmējam klasificēto informāciju nesaturošas norādes, izmanto atbilstoši noformētu pavadvēstuli:

113.1. kurai nosaka dienesta vajadzībām klasificētās informācijas slepenības pakāpi un lapas augšējā labajā stūrī norāda visas iekļautās klasificētās informācijas augstākās slepenības pakāpes, piemēram, "NATO SECRET", "CONFIDENTIEL UE/EU CONFIDENTIAL", kas veido sūtījuma kopējo slepenības pakāpi;

113.2. kurā norāda, vai ir iespējama tālāka pavadvēstulei pievienotās klasificētās informācijas apstrāde bez pavadvēstules, vienlaikus norādot:

113.2.1. pavadvēstules slepenības pakāpi bez pielikumiem;

113.2.2. iespējamību pavadvēstuli iznīcināt atbilstoši šo noteikumu 90.6. apakšpunktam.

114. Pārsūtot klasificēto informāciju saturošu dokumentu elektroniskā formā, izmanto portatīvā dokumenta formātu (PDF). Šo noteikumu 91. punktā minēto atsevišķo datni pārvērš PDF datnē un apvieno ar pārsūtāmo elektronisko dokumentu vienā datnē. Ja tālākai nodošanai elektroniskā formā paredzēto informācijas kopumu nav iespējams vai nav lietderīgi pārvērst PDF datnē, pirms informācijas sūtīšanas sūtītājam un saņēmējam ir rakstveidā jāvienojas par veidu, kā šādu informāciju ir paredzēts nodot.

115. Ja valsts noslēpuma objektu saturošu dokumentu paredzēts nodot ārvalstij vai starptautiskai organizācijai, tā pirmās lappuses augšā, pirmsteksta zonā, tekstam atbilstošā valodā norāda, ka dokumentā iekļautā informācija ir Latvijas Republikas īpašums, kas nodots citu valstu vai starptautisku organizāciju pārstāvju rīcībā saskaņā ar noslēgtu līgumu, un dokumentu aizliegts nodot trešajai pusei, izmantot tiesvedības procesā vai mainīt tā klasifikācijas pakāpi bez dokumenta autora rakstveida apstiprinājuma (piemēram, "*This information is the property of the originator and is supplied in accordance with the concluded bilateral agreement on protection of classified information. It must not be passed on to third parties, used in any judicial proceedings or reclassified without the prior written approval of originator. Original classification of the document must be preserved at all times. The originator reserves the right to inquire as to how this information has been used.*").

116. Ja valsts noslēpuma objektu saturošu dokumentu rada svešvalodā vai tulko nodošanai ārvalstij vai starptautiskai organizācijai, katra dokumenta lappuses augšējās un apakšējās malas vidū, aiz dokumenta lappusē ietvertās informācijas slepenības pakāpes, aiz šķērssvītras iekļauj informācijas valstiskās piederības starptautiskā saīsinājuma atzīmi "LV" un atzīmi par dokumenta lappusē ietvertās informācijas slepenības pakāpi atbilstoši objekta teksta valodai (piemēram, uz dokumenta angļu valodā "SLEPENI / LV SECRET" vai "NAV KLASIFICĒTS / LV NOT CLASSIFIED").

117. Ja valsts noslēpuma objektu saturošu dokumentu rada vai tulko nodošanai ārvalstīm vai valstu grupām starptautisko organizāciju vai valstu daudzpusējās sadarbības ietvaros, šo noteikumu 116. punktā minēto atzīmi papildina ar norādi par dokumenta izplatīšanas ierobežojumiem (piemēram, "SLEPENI / LV SECRET releasable to NATO" vai "SLEPENI / LV SECRET releasable to Joint Expeditionary Force"). Dokumenta izplatīšanas ierobežojumu norādi "Releasable to" var pievienot arī Latvijā radītai NATO un Eiropas Savienības klasificētās informācijas slepenības pakāpei.

118. Ar NATO dalībvalsti, ar kuru nav noslēgts divpusējais līgums par klasificētās informācijas aizsardzību, var apmainīties ar nacionālo klasificēto informāciju, atbalstot NATO programmu, projektu vai līgumu, pamatojoties uz Vienošanās starp Ziemeļatlantijas līguma pusēm par informācijas drošību 1. pantā noteikto apņemšanos.

119. Ar Eiropas Savienības dalībvalsti, ar kuru nav noslēgts divpusējais līgums par klasificētās informācijas aizsardzību, var apmainīties ar nacionālo klasificēto informāciju, atbalstot Eiropas Savienības programmu, projektu vai līgumu, pamatojoties uz nolīgumā "Par Padomē sanākušo Eiropas Savienības dalībvalstu nolīgumu par tādas klasificētās informācijas aizsardzību, ar kuru apmainās Eiropas Savienības interesēs" noteikto apņemšanos.

120. Saņemot ārvalstu klasificēto informāciju no valsts, ar kuru Latvijai nav noslēgts divpusējs līgums par klasificētās informācijas aizsardzību:

120.1. nepieciešams sazināties ar informācijas autoru, lai noskaidrotu pielīdzināmo valsts noslēpuma objekta slepenības pakāpi vai informācijas pieejamības ierobežojumus un nepieciešamos drošības pasākumus;

120.2. pirms saņemtās informācijas tālākas apstrādes to papildina ar šo noteikumu 120.1. apakšpunktā minēto darbību laikā noskaidroto informāciju;

120.3. par notikušo informē Nacionālo drošības iestādi.

121. Nacionālā drošības iestāde nodrošina divpusēju līgumu projektu izstrādi par klasificētās informācijas aizsardzību un aktuāla noslēgto līgumu saraksta uzturēšanu un publisku pieejamību.

122. Klasificēto informāciju saturošu elektronisku dokumentu, kas ir marķēts ar slepenības pakāpes marķējumu un izplatīšanas ierobežojuma norādi "Releasable to", var apstrādāt gan slepenības pakāpei, gan izplatīšanas ierobežojuma norādei atbilstošā akreditētā informācijas sistēmā.

123. Katram sūtījumam fiziskā formā pievieno sūtījuma pavadrakstu (13. pielikums), kurā norāda visas sūtījumā iekļautās klasificētās informācijas vienības.

124. Saņemot institūcijai adresētu klasificētās informācijas sūtījumu, pārbauda sūtījuma adreses atbilstību, pārliecinās par sūtījuma iepakojuma stāvokli (plombas un drošības uzlīmes), salīdzina sūtījuma pavadraksta reģistrācijas numuru ar kurjera pavadrakstā norādīto numuru un parakstās tajā par sūtījuma saņemšanu. Konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas sūtījuma kurjera pavadrakstu glabā vismaz piecus gadus. Visu slepenības pakāpju ATOMAL informācijas kurjera pavadrakstus glabā vismaz 10 gadus. Kurjera pavadrakstu var digitalizēt.

125. COSMIC TOP SECRET un ATOMAL informāciju saņem un šo noteikumu 124. punktā minētās darbības veic institūcijas COSMIC drošības virsnieks vai viņa vietnieks.

126. Ja tiek transportēta konfidenciāla klasificētā informācija un transportēšanu veic šo noteikumu 129.4. apakšpunktā minētais komersants, kas sniedz pasta pakalpojumus, par minētās klasificētās informācijas transportēšanas faktu tiek sastādīts kurjera pavadraksts. Kurjera pavadraksts satur vismaz šādu informāciju:

126.1. saņēmēja nosaukums;

126.2. saņēmēja adrese;

126.3. sūtījuma pavadraksta reģistrācijas numurs/-i, ja ir vairāki sūtījumi;

126.4. sūtījuma drošības uzlīmes vai plombas numurs, ja tādu izmanto;

126.5. kurjera vārds, uzvārds un/vai identifikators un kurjera pakalpojuma sniedzēja juridiskās personas dati (ja piegādi veic komercpakalpojuma sniedzējs);

126.6. sūtījuma izsūtīšanas datums un laiks;

126.7. sūtījuma saņemšanas datums un laiks;

126.8. datums un laiks, kad sūtījuma atdots atpakaļ;

126.9. kurjera paraksts un tā atšifrējums par sūtījuma pieņemšanu;

126.10. adresāta paraksts un tā atšifrējums par sūtījuma saņemšanu;

126.11. atzīme, ka sūtījums ir vai nav bojāts, un iespēja norādīt īsu sūtījuma bojājuma aprakstu, kuru ar parakstu apstiprina kurjers un sūtījuma saņēmējs.

127. Ja konstatēts sūtījuma bojājums, tad:

127.1. kurjera pavadrakstā izdara atzīmi par notikušo un pievieno īsu bojājumu aprakstu;

127.2. pēc kurjera pavadraksta aizpildīšanas izveido tā kopiju, un to paraksta saņēmējs un kurjers;

127.3. ja bojājumi ir tādi, kas liecina par to, ka varētu būt atklāts sūtījuma saturs, par to rakstveidā informē:

127.3.1. sūtījuma sagatavotāju;

127.3.2. institūcijas slepenības režīma nodrošinātāju;

127.3.3. kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija.

128. Ja tiek konstatēts, ka saņemtajā sūtījumā trūkst sūtījuma pavadrakstā norādītās klasificētās informācijas vai ir tāda klasificētā informācija, kas nav norādīta sūtījuma pavadrakstā, tad konstatēto faktu fiksē sūtījuma pavadrakstā, informē klasificētās informācijas sūtītāju un vienojas par tālākajām darbībām.

4.5. Klasificētās informācijas transportēšana

129. Klasificētās informācijas nosūtīšanu veic elektroniski, izmantojot akreditētu informācijas sistēmu. Ja tas nav iespējams, tad klasificēto informāciju transportēt ir atļauts:

129.1. Militārā kurjerdienesta vai diplomātiskajam kurjeram – klasificēto informāciju līdz slepenības pakāpei "SEVIŠĶI SLEPENI" (ieskaitot) un ATOMAL informāciju;

129.2. institūcijas norīkotam kurjeram:

129.2.1. informāciju ar slepenības pakāpi no "konfidenciāli" līdz "sevišķi slepeni" (ieskaitot) un ATOMAL informāciju tikai Šengenas zonas robežās. Šajā apakšpunktā noteiktais teritoriālais ierobežojums neattiecas uz Ārlietu ministrijas vai Latvijas Republikas diplomātisko un konsulāro pārstāvniecību norīkotajiem *ad hoc* diplomātiskajiem kurjeriem, kuri ārpus Šengenas zonas robežām var transportēt klasificēto informāciju ar slepenības pakāpi "konfidenciāli";

129.2.2. dienesta vajadzībām klasificēto informāciju;

129.3. institūcijas darbiniekam vai amatpersonai:

129.3.1. klasificēto informāciju ar slepenības pakāpi no "konfidenciāli" līdz "slepeni" (ieskaitot) tikai attiecīgās valsts robežās un tikai savu amata vai dienesta pienākumu vajadzībām;

129.3.2. klasificēto informāciju ar slepenības pakāpi "konfidenciāli" NATO un Eiropas Savienības dalībvalstu ietvaros un tikai savu amata vai dienesta pienākumu vajadzībām;

129.3.3. dienesta vajadzībām klasificēto informāciju;

129.4. komersantam, kas sniedz pasta pakalpojumus:

129.4.1. konfidenciālu klasificēto informāciju, ja ir saņemts 3. kategorijas industriālās drošības sertifikāts un kurjeram, kas veic transportēšanu ir izsniegta 3. kategorijas speciālā atļauja;

129.4.2. dienesta vajadzībām klasificēto informāciju ierakstīta sūtījuma formā ar paziņojumu sūtītājam par sūtījuma saņemšanu.

130. Komersants šo noteikumu 129.4.1. apakšpunktā minētajā gadījumā nodrošina:

130.1. sūtījuma transportēšanu tikai Latvijas Republikas robežās;

130.2. sūtījuma pieņemšanas un nodošanas atskaites funkcionalitāti;

130.3. sūtījuma tiešu transportēšanu līdz galamērķim;

130.4. kurjera pavadraksta atdošanu sūtītājam.

131. Šo noteikumu 129.1., 129.2. un 129.3. apakšpunktā minētajai personai:

131.1. nepieciešama atbilstošas slepenības pakāpes speciālā atļauja vai sertifikāts;

131.2. nepieciešams iepazīties ar šajos noteikumos minētajām drošības prasībām klasificētās informācijas transportēšanai;

131.3. ir aizliegts atstāt konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju bez uzraudzības, nogādājot to tieši līdz galamērķim bez pārtraukumiem, bet dienesta vajadzībām klasificēto informāciju var īslaicīgi uzglabāt personas rīcībā nodotā glabātavā, kas ir aizsargāta pret nepiederošu personu piekļūšanu, piemēram, viesnīcas seifā;

131.4. ir aizliegts iepazīties ar transportējamās informācijas saturu, izņemot šo noteikumu 129.3. apakšpunktā minētajai personai;

131.5. informācija jātransportē tā, lai nepiederoša persona nevar konstatēt, ka transportē klasificēto informāciju, un nav iespējams iepazīties ar tās saturu.

132. Attiecībā uz konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju šo noteikumu 129.2. un 129.3. apakšpunktā minētajai personai reizi gadā vai transportējot klasificēto informāciju neregulāri, pirms katra sūtījuma ar parakstu jāapliecina iepazīšanās ar kurjera instruktāžu (14. pielikums). Apliecinājumu glabā vismaz piecus gadus, un tas ir pieejams sevišķās lietvedības, centrālā reģistra biroja, apakšreģistra vai kontrolpunkta sertifikācijas procesā.

133. Šo noteikumu 129.2. un 129.3. apakšpunktā minētās personas klasificēto informāciju transportē, izmantojot amata vai dienesta pienākumu veikšanai pieejamo autotransportu vai gaisa, jūras, dzelzceļa, autobusu satiksmes transportu, izmantojot rokas bagāžas iespējas. Pārvietojoties kājām, nogādāt klasificēto informāciju līdz galamērķim atļauts tikai līdz slepenības pakāpei "konfidenciāli" (ieskaitot). Pilsētas sabiedriskajā transportā atļauts transportēt tikai dienesta vajadzībām klasificēto informāciju.

134. Konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju saturošu dokumentu transportē necaurredzamā dubultiepakojumā kopā ar kurjera pavadrakstu. Sūtījuma:

134.1. ārējo iepakojumu nodrošina ar aizsardzību pret neautorizētu tā atvēršanu un uz tā norāda tikai saņēmējas institūcijas nosaukumu un adresi, kā arī sūtījuma pavadraksta numuru;

134.2. iekšējā iepakojuma aizdares vietas paraksta un nosedz ar caurspīdīgu līmlenti vai citu iepakojuma veidam piemērotu materiālu vai izmanto specializētas drošības uzlīmes, kuras nav iespējams noņemt tās nesabojājot, un uz tā norāda attiecīgo slepenības pakāpi, saņēmēja institūciju un darbinieku, nosūtītāju un tā adresi, kā arī sūtījuma iesaiņotāja vārdu, uzvārdu un nosūtāmā dokumenta reģistrācijas numuru;

134.3. pavadrakstu ievieto iekšējā iepakojumā.

135. Dienesta vajadzībām klasificēto informāciju saturošu dokumentu transportē kopā ar kurjera pavadrakstu. Pirms transportēšanas sūtījumu iepako necaurredzamā iepakojumā, kuru nodrošina ar aizsardzību pret neautorizētu tā atvēršanu, un uz tā norāda tikai saņēmējas institūcijas nosaukumu un adresi, kā arī sūtījuma pavadraksta numuru.

136. Institūcijas darbinieks vai amatpersona amata vai dienesta pienākumu ietvaros var dienesta vajadzībām klasificēto informāciju saturošu dokumentu iznest ārpus institūcijas telpām, piemēram, uz sanāksmi, ievērojot šo noteikumu 131.5. apakšpunktā minētos nosacījumus. Uz minēto gadījumu nav attiecināmi šo noteikumu 135. punktā minētie nosacījumi.

137. Nestandarta formas klasificētās informācijas transportēšanai izmanto bandroles, ruļļveida pakas, maisus, kastes vai konteinerus, kurus aizdara ar atbilstoša pielietojuma un izmēra plombu, kas nav atverama bez tās sabojāšanas.

138. Ja vienā iepakojumā transportē klasificētos dokumentus ar dažādām slepenības pakāpēm, uz iekšējā iepakojuma norāda tajā ievietoto dokumentu augstākās slepenības pakāpes.

139. Ja klasificētās informācijas transportēšanai izmanto ar Nacionālās drošības iestādes atzītu šifrēšanas sistēmu šifrētu elektronisko datu nesēju, to transportē atbilstoši izvēlētās šifrēšanas sistēmas nodrošinātajam aizsardzības līmenim.

140. Ja klasificētās informācijas starptautiskas transportēšanas procesā ir iesaistīts komersants, izstrādā transportēšanas plānu. Transportēšanas plānu iepriekš rakstveidā saskaņo ar kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja pārved NATO vai Eiropas Savienības klasificēto informāciju vai sūtījumu sūta ārpus Latvijas teritorijas. Transportēšanas plānā norāda:

140.1. pilnu maršrutu;

140.2. visas maršrutā iekļautās pieturvietas un iesaistītās institūcijas;

140.3. par pārvešanu atbildīgo personu (vārds, uzvārds, pārstāvētā institūcija);

140.4. par sūtījuma saņemšanu atbildīgo personu (vārds, uzvārds, pārstāvētā institūcija).

141. Ja transportēšanas plānā pēc šo noteikumu 140. punktā noteiktās saskaņošanas rodas izmaiņas, par to informē kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja pārved NATO vai Eiropas Savienības klasificēto informāciju, vai sūtījumu sūta ārpus Latvijas teritorijas.

4.6. Klasificētās informācijas pavairošana

142. Dienesta vajadzībām klasificēto informāciju saturošu dokumentu var pavairot dokumenta turētājs, ja tas nepieciešams amata vai dienesta vajadzībām un izgatavotā kopija netiek nosūtīta vai nodota ārpus institūcijas. Šādu kopiju nereģistrē, un, kad kopija vairs nav nepieciešama, tās turētājs to iznīcina, iznīcināšanas procesu nedokumentējot.

143. Konfidenciālu un slepenu klasificēto informāciju saturošu dokumentu var pavairot ar institūcijas sevišķās lietvedības, centrālā reģistra biroja, apakšreģistra vai kontrolpunkta starpniecību:

143.1. ja nepieciešama dokumenta reģistrēta kopija nosūtīšanai citai institūcijai;

143.2. ja nepieciešama papīra formas dokumenta darba kopija izmantošanai vienas darbdienas ietvaros institūcijā organizētā pasākumā.

144. Šo noteikumu 143.1. apakšpunktā minēto kopiju institūcijas darbinieks, amatpersona vai struktūrvienība, kas organizē sevišķo lietvedību, centrālā reģistra birojs, apakšreģistrs vai kontrolpunkts reģistrē šo noteikumu 106. punktā noteiktajā kārtībā.

145. Šo noteikumu 143.2. apakšpunktā minētajā gadījumā:

145.1. izveidotās kopijas marķē ar marķējumu "DARBA KOPIJA";

145.2. izveidotās kopijas nereģistrē;

145.3. reģistrācijas un uzskaites sistēmā pie dokumenta oriģināla norāda datumu, kad izveidota darba kopija, un tās apjomu;

145.4. pēc organizētā pasākuma nekavējoties iznīcina darba kopijas šo noteikumu 15. pielikumā noteiktajos veidos un reģistrācijas un uzskaites sistēmā pie dokumenta oriģināla norāda atzīmi, ka izveidotais darba kopiju apjoms ir iznīcināts.

146. Sevišķi slepena valsts noslēpuma objekta, NATO vai Eiropas Savienības sevišķi slepena dokumenta kopiju

izgatavo informācijas autors vai ar informācijas autora rakstveida atļauju dokumenta saņēmējs.

147. Izņēmuma gadījumos, ja nav iespējams laikus iegūt autora atļauju sevišķi slepena valsts noslēpuma objekta, NATO vai Eiropas Savienības sevišķi slepena dokumenta pavairošanai vai saņemt kopiju, to var izgatavot informācijas saņēmējs. Par veikto sevišķi slepena valsts noslēpuma objekta, NATO vai Eiropas Savienības sevišķi slepena dokumenta pavairošanu, izgatavoto kopiju skaitu un to aktuālo statusu nekavējoties paziņo valsts noslēpuma objekta autoram vai Nacionālajai drošības iestādei, ja pavairota NATO un Eiropas Savienības klasificētā informācija.

148. Bez autora atļaujas aizliegts pārsūtīt citai institūcijai sevišķi slepenu klasificēto informāciju saturoša dokumenta kopiju.

149. Sevišķi slepena ārvalstu klasificēto informāciju saturoša dokumenta pavairošanai ievēro prasības, kas noteiktas ar konkrēto valsti noslēgtajā divpusējā līgumā par klasificētās informācijas aizsardzību.

150. Institūcijai, kurā tiek apstrādāta ATOMAL informācija, ir aizliegts to pavairot. Ja ir nepieciešams pavairot ATOMAL informāciju, ir jāsazinās ar Nacionālo drošības iestādi.

151. Institūcijas darbinieks vai amatpersona konfidenciālu vai slepenu klasificēto informāciju saturoša dokumenta projekta papīra formas izdruku var saņemt institūcijas sevišķajā lietvedībā, centrālā reģistra birojā, apakšreģistrā vai kontrolpunktā. Dokumenta projekts ir dokuments, kas vēl atrodas izstrādes stadijā, nav institūcijas vadītāja apstiprināts vai parakstīts. Šādu dokumenta projektu atzīmē ar marķējumu "PROJEKTS" un līdz piecām darbdienām to var nereģistrēt. Darbinieks, kuram tiek izsniegts dokumenta projekts, ir atbildīgs par atbilstošu tā aizsardzību, izmantošanu un atdošanu sevišķajā lietvedībā, centrālā reģistra birojā, apakšreģistrā vai kontrolpunktā iznīcināšanai. Dokumenta projektu ir aizliegts nodot tālāk citai personai.

4.7. Klasificētās informācijas tulkošana

152. Tulkojot klasificēto informāciju saturošus dokumentus, ievēro, ka:

152.1. tos tulko institūcijas darbinieks vai persona, ar kuru ir noslēgts līgums par tulkošanas pakalpojumu sniegšanu, ietverot informācijas konfidencialitātes prasības. Personai, kura tulko konfidenciālu un augstākas slepenības pakāpes klasificēto dokumentu, ir nepieciešams saņemt attiecīgas slepenības pakāpes speciālo atļauju un/vai sertifikātu;

152.2. tos tulko atbilstošā fiziskās drošības vidē akreditētā informācijas sistēmā;

152.3. tulkojumam saglabā oriģinālajam dokumentam noteikto slepenības pakāpi;

152.4. tulkojumu reģistrē kā oriģinālā dokumenta eksemplāru un tā tālāko apriti organizē kopā ar oriģinālo dokumentu, izņemot gadījumus, ja dokumenta oriģināls ir latviešu valodā un tulkojums ir sagatavots nosūtīšanai ārvalstīm.

153. Klasificētā dokumenta tulkojumam pirmās lappuses augšējā kreisajā stūrī:

153.1. raksta vārdu "Tulkojums" vai šo vārdu attiecīgajā valodā, kādā ir veikts tulkojums;

153.2. norāda valsti vai starptautisko organizāciju, no kuras šis dokuments saņemts;

153.3. norāda oriģinālam piešķirto reģistrācijas numuru;

153.4. norāda oriģināla slepenības pakāpi.

154. Ārvalstu sevišķi slepenu klasificēto informāciju saturošu dokumentu tulkošanā ievēro prasības, kas noteiktas ar konkrēto valsti noslēgtajā divpusējā līgumā par klasificētās informācijas aizsardzību.

4.8. Konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas esības pārbaude

155. Ne retāk kā reizi 12 mēnešos institūcijas darbinieks, amatpersona vai struktūrvienība, kas organizē sevišķo lietvedību, centrālā reģistra birojs, apakšreģistrs un kontrolpunkts atbilstoši kompetencei veic iepriekšējā kalendāra gadā institūcijā reģistrētās fiziskās formas konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas esības pārbaudi. Ne retāk kā reizi 12 mēnešos tiek veikta visu ATOMAL fiziskas formas informācijas vienību esības pārbaude.

156. Esības pārbaudes aktam nosaka dienesta vajadzībām klasificētās informācijas slepenības pakāpi, izņemot gadījumu, ja aktā atbilstoši šo noteikumu 96.2. apakšpunktam ir augstākas slepenības pakāpes informācija. Esības pārbaudes aktu reģistrē un uzglabā atbilstoši tā slepenības pakāpei.

157. Konfidenciālu un augstākas slepenības pakāpes NATO un Eiropas Savienības klasificēto dokumentu un to saturošu elektronisko datu nesēju esības pārbaudes aktu var izveidot automātiski centrālā reģistra biroja izveidotā un uzturētā NATO un Eiropas Savienības dokumentu vai elektroniskās informācijas nesēju reģistrācijas un uzskaites sistēmā Nacionālā slepenā tīkla ietvaros. Institūcijai, kurā nav pieejams Nacionālais slepenais tīkls, bet kurā tiek apstrādāti konfidenciālas un augstākas slepenības pakāpes NATO un Eiropas Savienības klasificētie dokumenti un tos saturoši elektronisko datu nesēji, esības pārbaudes aktu reģistrē institūcijas reģistrācijas un uzskaites sistēmā un vienu eksemplāru nosūta centrālā reģistra birojam.

158. Kompetentā valsts drošības iestāde ir tiesīga noteikt papildu esības pārbaudes nepieciešamību konfidenciālai un augstākas slepenības pakāpes klasificētajai informācijai.

159. Pēc esības pārbaudes akta apstiprināšanas un reģistrēšanas tas vairs nav labojams. Sevišķi slepenas un ATOMAL informācijas esības pārbaudes aktu glabā 10 gadus, bet konfidenciālas un slepenas klasificētās informācijas esības pārbaudes aktu glabā piecus gadus. Papīra formā sagatavotu esības pārbaudes aktu var digitalizēt.

160. Kompetentajai valsts drošības iestādei ir tiesības bez brīdinājuma veikt pārbaudes par valsts noslēpuma objektu esību institūcijā un šajos noteikumos noteikto aizsardzības prasību ievērošanu. Nacionālajai drošības iestādei ir tiesības bez brīdinājuma veikt pārbaudes par NATO, Eiropas Savienības un ārvalstu klasificētās informācijas esību institūcijā un aizsardzības prasību ievērošanu. Šo noteikumu 37.9. apakšpunktā minētais pārbaudes akts ir pieejams šajā punktā minēto pārbaužu ietvaros.

4.9. Klasificētās informācijas slepenības pakāpes noteikšana, grozīšana un atcelšana

161. Valsts noslēpuma objektam, Latvijā radītiem NATO vai Eiropas Savienības klasificētajiem dokumentiem slepenības pakāpi nosaka institūcija, kuras darbinieks vai amatpersona to izstrādā. Nosakot slepenības pakāpi valsts noslēpuma objektam, norāda termiņu, uz kādu dokumentam ir piešķirta slepenības pakāpe. Slepenības pakāpi pārskata institūcija, kuras darbinieks vai amatpersona izstrādāja vai pēc kuras pasūtījuma komersants izstrādāja valsts noslēpuma objektu, NATO vai Eiropas Savienības klasificēto informāciju saturošu dokumentu.

162. Institūcijai ir pienākums veikt tās radītā vai tās vajadzībām komersanta radītā valsts noslēpuma objekta, NATO vai Eiropas Savienības klasificētā dokumenta slepenības pakāpes regulāru pārskatīšanu, izņemot tiem dokumentiem, kas minēti šo noteikumu 90.7. apakšpunktā un ir atbilstoši marķēti.

163. Ja ir pieņemts lēmums saglabāt vai grozīt valsts noslēpuma objektam, Latvijā radītai NATO vai Eiropas Savienības klasificētajai informācijai sākotnēji noteikto slepenības pakāpi vai veikt tās deklasificēšanu, par to rakstveidā informē visas institūcijas, kas ir attiecīgā valsts noslēpuma objekta, NATO vai Eiropas Savienības

klasificētās informācijas turētāji. Pēc šādas informācijas saņemšanas institūcija piecu darbdienu laikā izdara grozījumus attiecīgās informācijas apzīmējumos un reģistrācijas un uzskaites sistēmā par slepenības pakāpes saglabāšanu, grozīšanu vai atcelšanu. Ja klasificētais dokuments ir papīra formā:

163.1. uz dokumenta pirmās lappuses norāda slepenības pakāpes saglabāšanas, grozīšanas vai atcelšanas pamatojumu un datumu, veiktos labojumus apstiprinot ar parakstu;

163.2. uz dokumenta katras lappuses slepenības pakāpes grozīšanas vai atcelšanas gadījumā ar vienu svītru pārsvītro oriģinālo slepenības pakāpes marķējumu un blakus norāda jauno informācijas aizsardzības marķējumu.

164. Elektroniskas formas dokumentam šo noteikumu 163. punktā minēto informāciju norāda atsevišķā datnē, kuru paraksta kopā ar elektronisko dokumentu.

165. Par šo noteikumu 163. punktā minēto lēmumu institūcija informē visus darbiniekus vai amatpersonas, kuri ir attiecīgās klasificētās informācijas turētāji.

166. Klasificētās informācijas turētājs groza vai atceļ no citas institūcijas, starptautiskas organizācijas vai ārvalsts saņemtas klasificētās informācijas slepenības pakāpi tikai tādā gadījumā, ja ir saņemts minētās institūcijas, starptautiskās organizācijas vai ārvalsts rakstveida paziņojums par slepenības pakāpes grozīšanu vai atcelšanu.

167. Ja tiek likvidēta vai reorganizēta iestāde, kurā tika apstrādāta un glabāta klasificētā informācija, klasificēto informāciju nodod iestādes tiesību un saistību pārņēmējai vai augstākai iestādei. Ja tiek nodota konfidenciāla un augstākas slepenības pakāpes klasificētā informācija, iestādē, kas pārņem saistības, vai augstākā iestādē ir jābūt pārbaudītai sevišķai lietvedībai, apakšreģistram vai kontrolpunktam atbilstoši šo noteikumu 71. un 87. punktam. Privāto tiesību juridiskās personas likvidācijas, reorganizācijas vai maksātnespējas procesa ierosināšanas gadījumā klasificēto informāciju nodod kompetentajai valsts drošības iestādei vai iestādei, kuras organizēta iepirkuma ietvaros attiecīgā informācija ir saņemta.

4.10. Klasificētās informācijas glabāšana, digitalizācija un iznīcināšana

(Apakšnodaļas nosaukums MK 09.06.2026. noteikumu Nr. 320 redakcijā)

168. Institūcija izvērtē klasificētu informāciju saturošus dokumentus, lai noteiktu pastāvīgi glabājamos dokumentus un uz laiku glabājamo dokumentu glabāšanas termiņus.
(MK 09.06.2026. noteikumu Nr. 320 redakcijā)

169. Institūcija, kuras rīcībā ir digitalizācijai nepieciešamie līdzekļi un aprīkojums:

169.1. digitalizē fiziskā formā radītu klasificēto informāciju, izņemot gadījumus, kad to ir aizliedzis informācijas autors;

169.2. iznīcina fiziskas formas klasificēto informāciju vai dzēš elektroniskas formas klasificēto informāciju, ja tā nav nepieciešama darbam, ja uz laiku glabājamiem klasificētajiem dokumentiem ir beidzies to glabāšanas laiks vai to pieprasa attiecīgās klasificētās informācijas autors.
(MK 09.06.2026. noteikumu Nr. 320 redakcijā)

170. Lēmumu par klasificēto dokumentu digitalizāciju vai iznīcināšanu pieņem institūcijas vadītājs, bet lēmuma izpildi nodrošina institūcijas darbinieks, amatpersona vai struktūrvienība, kas organizē sevišķo lietvedību, centrālā reģistra birojs, apakšreģistrs, kontrolpunkts vai par dienesta vajadzībām klasificēto informāciju atbildīgā struktūrvienība, darbinieks vai amatpersona, ievērojot, ka:

170.1. sevišķi slepenu klasificēto informāciju saturoša dokumenta digitalizācijas un iznīcināšanas procesā piedalās liecinieks – kompetentās valsts drošības iestādes darbinieks vai amatpersona vai Nacionālās drošības iestādes darbinieks vai amatpersona, ja digitalizē vai iznīcina NATO, Eiropas Savienības vai ārvalstu klasificēto informāciju saturošu dokumentu;

170.2. slepenu un konfidenciālu klasificēto informāciju saturoša dokumenta digitalizācijas un iznīcināšanas procesā piedalās liecinieks – autorizēta persona, kas nav saistīta ar institūcijas sevišķo lietvedību, centrālā reģistra biroju, apakšreģistru vai kontrolpunktu;

170.3. dienesta vajadzībām klasificēto informāciju saturoša dokumenta digitalizāciju un iznīcināšanu veic šo noteikumu 33.4. apakšpunktā minētais darbinieks, amatpersona vai struktūrvienība;

170.4. visu slepenības pakāpju ATOMAL informācijas iznīcināšanas procesā piedalās liecinieks – Nacionālās drošības iestādes amatpersona;

170.5. sevišķi slepenu un slepenu, kā arī visu slepenības pakāpju ATOMAL klasificēto informāciju saturošu dokumentu iznīcināšanas procesā pirms to iznīcināšanas kopā ar liecinieku salīdzina iznīcināmo dokumentu reģistrācijas datus un lappušu skaitu ar iznīcināšanas aktā norādīto. Iznīcinot konfidenciālu klasificēto informāciju saturošus dokumentus, šo salīdzināšanu veic vismaz desmit procentiem iznīcināmo dokumentu, to atzīmējot iznīcināšanas aktā;

170.6. personas, kas piedalās klasificētu informāciju saturošu dokumentu iznīcināšanas procesā, ar parakstu iznīcināšanas aktā apliecina klasificētās informācijas iznīcināšanu. Digitalizācijas un iznīcināšanas process uzskatāms par pabeigtu ar iznīcināšanas akta parakstīšanas brīdi. COSMIC TOP SECRET un ATOMAL informācijas iznīcināšanas aktus paraksta arī COSMIC drošības virsnieks vai viņa vietnieks. Papīra formā sagatavotu iznīcināšanas aktu pēc parakstīšanas var digitalizēt;

170.7. iznīcināšanas aktam nosaka dienesta vajadzībām klasificētās informācijas slepenības pakāpi, izņemot gadījumu, ja aktā atbilstoši šo noteikumu 96.2. apakšpunktam ir iekļauta augstākas slepenības pakāpes informācija. Iznīcināšanas aktu reģistrē un glabā atbilstoši tā slepenības pakāpei. Institūcija var izveidot un glabāt konfidenciālu un augstākas slepenības pakāpes NATO un Eiropas Savienības dokumentu iznīcināšanas aktu centrālā reģistra biroja izveidotā un uzturētā NATO un Eiropas Savienības dokumentu vai elektroniskās informācijas nesēju reģistrācijas un uzskaites sistēmā Nacionālā slepenā tīkla ietvaros. Institūcija, kurā nav pieejams Nacionālais slepenais tīkls, bet tiek apstrādāti konfidenciālas un augstākas slepenības pakāpes NATO un Eiropas Savienības dokumenti, iznīcināšanas akta vienu eksemplāru nosūta centrālā reģistra birojam;

170.8. pēc konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju saturoša dokumenta digitalizācijas vai iznīcināšanas atbilstošajā klasificētās informācijas reģistrācijas un uzskaites sistēmā iekļauj informāciju par veikto digitalizāciju vai iznīcināšanu, norādot digitalizācijas datumu vai iznīcināšanas akta numuru un datumu. Šos ierakstus apliecina ar parakstu vai apstiprina ar citiem informācijas sistēmā nodrošinātajiem līdzekļiem;

170.9. pēc dienesta vajadzībām klasificētās informācijas saturoša dokumenta digitalizācijas vai iznīcināšanas atbilstošajā klasificētās informācijas reģistrācijas un uzskaites sistēmā iekļauj informāciju par veikto digitalizāciju vai iznīcināšanu, norādot attiecīgās darbības datumu.

(Grozīts ar MK 09.06.2026. noteikumiem Nr. 320)

170.[1] Institūcijai ir tiesības veikt papīra formā sagatavoto un reģistrēto valsts noslēpumu saturošo dokumentu digitalizāciju, ievērojot šādus noteikumus:

170.[1]1. dokumentu digitizē formātā, kas ir piemērots elektroniska dokumenta ilglaicīgai glabāšanai (piemēram, PDF/A, JPEG2000, TIFF), ja iespējams, nodrošinot teksta atpazīšanas funkcionalitāti. Digitalizācijas procesā nodrošina digitalizētā dokumenta integritāti un atbilstību oriģinālam, veicot dokumenta pārbaudi un digitalizācijas procesa kontroli;

170.[1]2. digitalizētā dokumenta datni institūcija paraksta ar likuma "Par valsts noslēpumu" 7. panta 7.[1] daļā minēto elektronisko parakstu vai apliecina ar kvalificētu elektronisko zīmogu Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK, 3. panta 27. punkta izpratnē;

170.[1]3. nodrošina digitalizētā dokumenta satura attēlojumu un atbilstību normatīvajos aktos noteiktajā dokumentu glabāšanas laikā;

170.[1]4. nodrošina satura lasīšanu elektroniski un, ja nepieciešams, atvasinājuma veidošanu papīra un elektroniskā formā;

170.[1]5. visu normatīvajos aktos paredzamo glabāšanas termiņu nodrošina digitalizēto dokumentu autentiskumu, aizsardzību no neatļautas piekļūšanas, pazušanas vai iznīcināšanas.

(MK 09.06.2026. noteikumu Nr. 320 redakcijā)

171. Piedalīties klasificētās informācijas iznīcināšanā kā liecinieku var norīkot institūcijas darbinieku vai amatpersonu, kuram ir speciālā atļauja vai sertifikāts, kas ir atbilstošs iznīcināmās informācijas slepenības pakāpei.

172. Klasificēto informāciju saturošus dokumentus iznīcina šo noteikumu 15. pielikumā norādītajos veidos. Ja šo noteikumu 15. pielikumā norādītie dokumentu iznīcināšanas veidi nav piemēroti, institūcija attiecīgu klasificēto informāciju saturošu dokumentu iznīcināšanas veidu rakstveidā saskaņo ar kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija.

173. Lēmumu par klasificētās tehnikas, aprīkojuma un ieroču iznīcināšanu pieņem institūcijas vadītājs un norīko atbildīgo institūcijas darbinieku, amatpersonu vai struktūrvienību lēmuma izpildei. Lēmuma izpildes pārraudzību nodrošina institūcijas darbinieks, amatpersona vai struktūrvienība, kas organizē sevišķo lietvedību, centrālā reģistra birojs, apakšreģistrs, kontrolpunkts vai atbildīgā persona par dienesta vajadzībām klasificētās informācijas lietvedības un fiziskās drošības pasākumu ieviešanu un ievērošanu. Institūcija rakstveidā saskaņo ar kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija, klasificētas tehnikas, aprīkojuma un ieroču iznīcināšanas procedūras, piemērojot šajā apakšnodaļā noteikto, ciktāl tas attiecināms.

174. Pēc konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas iznīcināšanas informāciju par piekļuves faktu konfidenciālai un slepenai klasificētajai informācijai glabā piecus gadus, informāciju par piekļuves faktu sevišķi slepenai un ATOMAL informācijai – 10 gadus.

175. Konfidenciālas un slepenas klasificētās informācijas iznīcināšanas aktu glabā piecus gadus, sevišķi slepenas klasificētās informācijas un ATOMAL informācijas iznīcināšanas aktu – 10 gadus.

176. Institūcijas klasificētās informācijas iznīcināšanas procedūras ārkārtējā, izņēmuma vai kara stāvokļa gadījumiem izstrādā institūcijas klasificētās informācijas evakuācijas plāna ietvaros un saskaņo ar kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija.

4.11. Klasificētās informācijas izsniegšanas pieprasījumu apstrāde

177. Ja privāto tiesību subjekta informācijas pieprasījums institūcijai ir saistīts ar institūcijas radīto klasificēto informāciju, institūcija izsniedz tikai tādu informāciju, kuru var deklasificēt. Institūcija:

177.1. izvērtē, vai pieprasījumā ir noteikts un pamatots mērķis pieprasītās informācijas tālākai izmantošanai;

177.2. izvērtē pieprasītās informācijas deklasificēšanas pieļaujamību;

177.3. ja pieprasīto informāciju nav iespējams deklasificēt, sniedz pieprasītājam atbildi saskaņā ar normatīvajiem aktiem.

178. Institūcija atbildi uz šo noteikumu 177. punktā minēto informācijas pieprasījumu sniedz 30 dienu laikā, bet ne vēlāk kā triju mēnešu laikā no pieprasījuma saņemšanas dienas. Ja pieprasītās informācijas apkopošanai un deklasificēšanai ir nepieciešams ilgāks laiks par 30 dienām, par to informē informācijas pieprasītāju, norādot iemeslu.

179. Institūcija nav tiesīga lemt par citas institūcijas radītās klasificētās informācijas izsniegšanu.

5. Klasificētās informācijas aizsardzība iepirkumos

180. Iepirkumā, kas saistīts ar konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas izmantošanu, ir tiesīgs piedalīties komersants, kuram ir derīgs atbilstošas kategorijas industriālās drošības sertifikāts.

181. Iepirkumā, kas saistīts ar dienesta vajadzībām klasificētās informācijas izmantošanu, nepiemēro industriālās drošības sertifikāta prasību.

182. Iepirkumā, kas saistīts ar valsts noslēpuma objektu vai ārvalstu klasificētās informācijas izmantošanu, ir tiesīgs piedalīties Latvijas Republikā vai ārvalstī, ar kuru Latvijas Republikai noslēgts divpusējs līgums par savstarpēju klasificētās informācijas aizsardzību, reģistrēts saimnieciskās darbības veicējs.

183. Iepirkumā, kas saistīts ar NATO vai Eiropas Savienības klasificētās informācijas izmantošanu, ir tiesīgs piedalīties NATO, Eiropas Savienības vai valstī, ar kuru NATO vai Eiropas Savienība ir noslēgusi divpusēju līgumu par savstarpēju klasificētās informācijas aizsardzību, reģistrēts saimnieciskās darbības veicējs.

184. Iepirkumā, kas saistīts ar konfidenciālas vai augstākas slepenības pakāpes klasificētās informācijas izmantošanu, ir tiesīgs piedalīties komersanta darbinieks, kuram ir derīga atbilstošas kategorijas speciālā atļauja vai sertifikāts.

185. Ārvalstī reģistrēta komersanta industriālās drošības sertifikāta un ārvalstī reģistrēta komersanta darbinieka speciālās atļaujas vai sertifikāta derīguma pārbaudi veic Nacionālā drošības iestāde pēc institūcijas rakstveida pieprasījuma.

186. Pasūtītāja vai klasificētās informācijas valdītāja pienākums ir noteikt minimālās drošības prasības klasificētās informācijas aizsardzībai iepirkuma norises posmam un iepirkuma līguma izpildes posmam. Informācijas aizsardzības pārkāpums jebkurā no šiem posmiem var būt par pamatu, lai pārtrauktu iepirkumu vai iepirkuma līgumu. Noteikto drošības prasību neievērošana iepirkuma līguma izpildes posmā var būt par pamatu, lai noteiktu kompensāciju par zaudējumiem, kas tā dēļ ir radušies.

187. Pirms iepirkuma uzsākšanas pasūtītājs un klasificētās informācijas valdītājs nosaka iepirkuma priekšmeta vai gala rezultāta valsts noslēpuma objekta, NATO vai Eiropas Savienības klasificētās informācijas slepenības pakāpi un pretendentam izvirzāmās klasificētās informācijas aizsardzības prasības, norādot:

187.1. pamatojumu klasificētās informācijas izmantošanai iepirkuma izpildē;

187.2. katras iepirkuma daļas klasifikācijas pakāpi;

187.3. vai pretendentam nepieciešams industriālās drošības sertifikāts, nosakot tā kategoriju;

187.4. vai pretendentam ir nepieciešams industriālās drošības sertifikāts, kas dod tiesības glabāt klasificēto informāciju savās telpās;

187.5. vai pretendentam ir nepieciešama akreditēta informācijas sistēma;

187.6. personāla, fiziskās un informācijas drošības prasības;

187.7. pretendenta apakšuzņēmējam vai tā nolīgtam apakšuzņēmējam izvirzāmās drošības prasības, ņemot vērā apakšuzņēmējam izpildē nododamās daļas klasifikācijas pakāpes;

187.8. pretendenta darbiniekam izvirzāmās drošības prasības, ievērojot šo noteikumu 184. punktu.

188. Ja iepirkumā, kas saistīts ar konfidenciālas un augstākas slepenības pakāpes klasificētās informācijas izmantošanu un kurā piedalās ārvalstu institūcija, vienas līgumslēdzējpuses pārstāvim iepirkuma izpildei nepieciešama piekļuve otras līgumslēdzējpuses telpām, kurām ir noteikta prasība pēc derīgas speciālās atļaujas vai

sertifikāta, šādu piekļuvi atļauj tikai ar iepriekšēju apmeklējamās valsts kompetentās valsts institūcijas atļauju šo noteikumu 19. punktā noteiktajā kārtībā.

189. Ja pretendentam iepirkuma piedāvājuma sagatavošanai izsniedz klasificēto informāciju, pasūtītājs iepirkuma dokumentācijā nosaka prasību iepirkumā neuzvarējušajam pretendentam:

189.1. nodot atpakaļ pasūtītājam no tā saņemto un pretendenta radīto konfidenciālu un augstākas slepenības pakāpes klasificēto informāciju;

189.2. iznīcināt no pasūtītāja saņemto un pretendenta radīto dienesta vajadzībām klasificēto informāciju atbilstoši šo noteikumu 15. pielikumā norādītajiem veidiem, sniedzot rakstveida apliecinājumu pasūtītājam par veikto iznīcināšanu.

6. Valsts noslēpuma objektu nodošana ārvalstu pārstāvjiem Latvijas Republikas un ārvalstu sadarbības ietvaros

190. Valsts noslēpuma objektu nodod ārvalsts institūcijai Latvijas Republikas un ārvalsts sadarbības ietvaros saskaņā ar starptautisko līgumu noteikumiem.

191. Par valsts noslēpuma objekta nodošanu ārvalsts institūcijai ir tiesīgs lemt informācijas autors, ievērojot starptautisko līgumu noteikumus.

192. Pirms valsts noslēpuma objekta, kas satur izrakstu no NATO, Eiropas Savienības vai ārvalsts klasificētās informācijas, nodošanas ārvalstu institūcijām, tā nodošanu saskaņo ar Nacionālo drošības iestādi.

7. Informācijas sistēmu aizsardzība, kurās tiek apstrādāta klasificētā informācija

193. Informācijas sistēmas akreditācijas procesa ietvaros institūcijai izsniedz atzinumu par informācijas sistēmas atbilstību drošības prasībām. Atzinumā norāda:

193.1. pārbaudāmās institūcijas vai institūcijas struktūrvienības nosaukumu;

193.2. augstāko klasificētās informācijas slepenības pakāpi, kuru ļauts apstrādāt pārbaudāmajā informācijas sistēmā;

193.3. pārbaudāmās informācijas sistēmas īsu aprakstu;

193.4. norādi par atļauju vai aizliegumu informācijas sistēmā uzsākt klasificētās informācijas apstrādi;

193.5. konstatētos trūkumus;

193.6. norādi par šo noteikumu 193.4. apakšpunktā minētās atļaujas derīguma termiņu;

193.7. pārbaudāmās institūcijas pārstāvjus, kas piedalījās pārbaudē (vārds, uzvārds, amats).

194. Nacionālā drošības iestāde nosaka šifrēšanas sistēmas, kuras drīkst izmantot klasificētās informācijas aizsardzībai, kā arī veic šo šifrēšanas iekārtu un šifrēšanas materiālu uzskaiti un administrēšanu. Šifrēšanas materiālu iepirkumus veic Nacionālā drošības iestāde, izņemot gadījumus, ja institūcija saņēmusi Nacionālās drošības iestādes saskaņojumu patstāvīgai šādu iepirkumu organizēšanai. Nacionālā drošības iestāde veic tās personas instruktāžu, kas institūcijā atbildīga par šifru materiāliem, un izsniedz šifrēšanas atļauju pieejai šifrēšanas materiāliem. Institūcijā par šifru materiāliem atbildīgā persona nodrošina tālāku šifru materiālu lietotāju instruktāžu institūcijas ietvaros.

195. Satversmes aizsardzības birojs izstrādā un Ministru kabinets izdod instrukciju par šifrēšanas atļauju izsniegšanu, šifrēšanas iekārtu un šifrēšanas materiālu uzskaiti, izplatīšanu, glabāšanu un iznīcināšanu.

196. Satversmes aizsardzības birojs izstrādā un Ministru kabinets izdod instrukciju par kārtību, kādā veicama informācijas sistēmu drošības pārbaude, reģistrācija un akreditācija, kā arī par drošības prasībām, kādas tiek izvirzītas informācijas sistēmām, lai nodrošinātu klasificētās informācijas elektronisku apstrādi, glabāšanu un pārsūtīšanu.

8. Klasificētās informācijas drošības prasību pārkāpumi, izpaušana vai nozaudēšana

197. Ja ir pamats uzskatīt, ka notikusi klasificētās informācijas izpaušana, nozaudēšana vai normatīvajos aktos, kas regulē klasificētās informācijas drošības prasību jomu, noteikto drošības prasību pārkāpums, institūcijas vadītājs:

197.1. nekavējoties informē kompetento valsts drošības iestādi, bet, ja ir iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija, – Nacionālo drošības iestādi;

197.2. sadarbojoties ar kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja ir iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija, un nodrošinot klasificētās informācijas aizsardzību atbilstoši šiem noteikumiem, atbilstoši iespējām pārtrauc personas rīcību, kuras dēļ noticis vai notiek klasificētās informācijas drošības prasību pārkāpums vai klasificētās informācijas izpaušana vai nozaudēšana, kā arī apkopo visu iespējamo informāciju par notikušo;

197.3. ne vēlāk kā triju darbdienu laikā izveido sev tieši pakļautu dienesta izmeklēšanas komisiju vismaz triju cilvēku sastāvā, to rakstveidā saskaņojot ar kompetento valsts drošības iestādi vai Nacionālo drošības iestādi, ja iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija. Kompetentā valsts drošības iestāde vai Nacionālā drošības iestāde ir tiesīga iekļaut pārstāvi dienesta izmeklēšanas komisijā.

198. Kompetentajai valsts drošības iestādei vai Nacionālajai drošības iestādei, ja iesaistīta NATO, Eiropas Savienības vai ārvalstu klasificētā informācija, ir tiesības uzdot institūcijai veikt dienesta izmeklēšanu šajā nodaļā noteiktajā kārtībā.

199. Dienesta izmeklēšanas komisijas sastāvā norīko personas, kurām izsniegto speciālo atļauju un sertifikātu kategorijas atbilst pārkāpumā identificētās klasificētās informācijas kategorijai.

200. Dienesta izmeklēšanas komisijai ir šādi pienākumi:

200.1. noskaidrot klasificētās informācijas izpaušanas vai nozaudēšanas apstākļus (piemēram, laiks, vieta) un drošības prasību pārkāpuma būtību un iemeslus;

200.2. noskaidrot iesaistītās personas un to lomu pārkāpumā;

200.3. noskaidrot cēloņus un apstākļus, kas veicinājuši pārkāpuma izdarīšanu un sagatavot priekšlikumus šādu pārkāpumu turpmākai mazināšanai vai novēršanai;

200.4. noteikt kaitējumu, kas radies vai varēja rasties klasificētās informācijas izpaušanas, nozaudēšanas un/vai drošības prasību pārkāpuma gadījumā;

200.5. meklēt, pieprasīt un saglabāt dienesta izmeklēšanas ietvaros gūtos pierādījumus.

201. Dienesta izmeklēšanas komisijas locekļiem ir šādas tiesības:

201.1. veikt attiecīgās institūcijas telpu, teritorijas, seifu, galdu, skapju un cita inventāra apskati;

201.2. pārbaudīt informācijas sistēmas, elektroniskās informācijas nesējus, reģistrācijas un uzskaites

sistēmas un citus dokumentus;

201.3. pieprasīt paskaidrojumus ar pārkāpumu saistītām institūciju amatpersonām un darbiniekiem, tai skaitā ārpakalpojumu sniedzējiem, piemēram, apsardzes darbiniekiem, uzkopšanas darbu veicējiem.

202. Dienesta izmeklēšanu veic un gala atzinumu sagatavo 20 darbdienu laikā no dienesta izmeklēšanas komisijas izveidošanas dienas. Institūcijas vadītājs objektīvu iemeslu dēļ var pagarināt dienesta izmeklēšanas komisijas darbu par 20 darbdienām. Dienesta izmeklēšanas un gala ziņojuma sagatavošanas termiņā neieskaita laiku, kurā amatpersonai ir bijusi pārejoša darbnespēja vai viņa ir bijusi atvaļinājumā vai komandējumā.

203. Dienesta izmeklēšanas komisija gala atzinumā norāda:

203.1. detalizētu pārkāpuma aprakstu;

203.2. dienesta izmeklēšanas komisijas veiktās darbības;

203.3. pārkāpumā iesaistītās personas un to atbildību;

203.4. klasificētās informācijas izpaušanas, nozaudēšanas vai drošības prasību pārkāpuma radītās sekas vai potenciālās sekas nākotnē;

203.5. priekšlikumus, lai nākotnē novērstu vai maksimāli ierobežotu šāda veida pārkāpumu atkārtotu iestāšanos;

203.6. priekšlikumus pārkāpumā iesaistīto personu sodīšanai atbilstoši normatīvajiem aktiem.

204. Dienesta izmeklēšanas materiālu kopijas pēc gala atzinuma apstiprināšanas nekavējoties nosūta kompetentajai valsts drošības iestādei un Nacionālajai drošības iestādei, ja tas saistīts ar NATO, Eiropas Savienības vai ārvalstu klasificētās informācijas apstrādi.

205. Dienesta izmeklēšanas materiālus, kas saistīti ar dienesta vajadzībām klasificēto informāciju, konfidenciālas un slepenas klasificētās informācijas izpaušanu, nozaudēšanu vai drošības pasākumu pārkāpumu, glabā piecus gadus, bet dienesta izmeklēšanas materiālus, kas saistīti ar sevišķi slepenas un ATOMAL klasificētās informācijas izpaušanu, nozaudēšanu vai drošības pasākumu pārkāpumu, – 10 gadus.

206. Nacionālā drošības iestāde NATO, Eiropas Savienības vai ārvalstu klasificētās informācijas izpaušanas, nozaudēšanas vai drošības pasākumu pārkāpuma gadījumā informē atbildīgās institūcijas saskaņā ar starptautiskajiem līgumiem.

9. Noslēguma jautājumi

207. Valsts drošības iestādes personu pārbaudes speciālās atļaujas saņemšanai, kas uzsāktas pirms šo noteikumu stāšanās spēkā, pabeidz atbilstoši regulējumam, kāds bija spēkā līdz šo noteikumu spēkā stāšanās dienai.

208. Speciālās atļaujas, kas ir spēkā šo noteikumu spēkā stāšanās dienā, ir derīgas līdz to anulēšanai vai derīguma termiņa beigām.

209. Institūcijas veic šajos noteikumos minēto institūcijas iekšējo normatīvo aktu aktualizēšanu vai izstrādi līdz 2025. gada 1. janvārim.

210. Institūcijas šajos noteikumos noteiktās fiziskās drošības procedūras, kas nav saistītas ar fiziskās drošības vides infrastruktūras izmaiņām, ievieš līdz 2025. gada 1. janvārim, bet fiziskās drošības vides infrastruktūras

prasības īsteno piecu gadu laikā pēc šo noteikumu stāšanās spēkā.

211. Valsts drošības iestādes telpu atbilstības pārbaudes, kas uzsāktas pirms šo noteikumu stāšanās spēkā, veic atbilstoši regulējumam, kāds bija spēkā līdz šo noteikumu spēkā stāšanās dienai.

212. Šo noteikumu 5. nodaļas prasības nav attiecināmas uz iepirkumiem, kas uzsākti pirms šo noteikumu stāšanās spēkā.

213. Institūcija, kura veic darbu ar ārvalstu klasificēto informāciju, par to informē Nacionālo drošības iestādi sešu mēnešu laikā pēc šo noteikumu stāšanās spēkā.

214. Satversmes aizsardzības birojs izstrādā šo noteikumu 195. un 196. punktā minētās Ministru kabineta instrukcijas līdz 2025. gada 1. janvārim. No 2024. gada 1. janvāra līdz šo noteikumu 195. un 196. punktā minēto instrukciju spēkā stāšanās dienai ir piemērojamas saskaņā ar Ministru kabineta 2004. gada 6. janvāra noteikumiem Nr. 21 "Valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu klasificētās informācijas aizsardzības noteikumi" un Ministru kabineta 2005. gada 26. aprīļa noteikumiem Nr. 280 "Kārtība, kādā aizsargājama informācija dienesta vajadzībām" izdotās Ministru kabineta instrukcijas.

215. Šo noteikumu 8. nodaļas prasības nav attiecināmas uz dienesta izmeklēšanām, kas uzsāktas pirms šo noteikumu spēkā stāšanās.

216. Noteikumi stājas spēkā 2024. gada 1. janvārī.

217. Atzīt par spēku zaudējušiem Ministru kabineta 2004. gada 6. janvāra noteikumus Nr. 21 "Valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu klasificētās informācijas aizsardzības noteikumi" (Latvijas Vēstnesis, 2004, 17. nr.).

Ministru prezidente *E. Siliņa*

Tieslietu ministre *I. Lībiņa-Egnere*

1. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Apliecinājums

Es, _____
(vārds, uzvārds)
_____, apņemos
(personas kods, dzimšanas datums (ārvalstniekiem))

1) neizpaust informāciju dienesta vajadzībām, kas man tiks uzticēta vai kļūs zināma, pildot amata vai dienesta pienākumus vai konkrētu darba vai dienesta uzdevumu;

2) bez iebildumiem un precīzi izpildīt ar informācijas dienesta vajadzībām aizsardzību saistīto rīkojumu (pavēļu), noteikumu un instrukciju prasības, ar kurām esmu iepazīstināts;

3) ziņot par prettiesiskiem mēģinājumiem iegūt no manis informāciju dienesta vajadzībām, kā arī par man zināmiem informācijas dienesta vajadzībām aizsardzības pasākumu pārkāpumiem.

Esmu brīdināts(-a), ka par informācijas dienesta vajadzībām izpaušanu, nozaudēšanu un citiem šīs informācijas aizsardzības pasākumu pārkāpumiem tikšu saukts(-a) pie disciplināratbildības un/vai kriminālatbildības.

Kontaktinformācija: _____
(mob. tel.) (e-pasts)

20____. gada ____. _____ _____
(paraksts)

Apliecinājumu pieņēma _____
(atbildīgās personas amats, vārds, uzvārds un paraksts)

2. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Aptaujas lapa

Aizpildot šo aptaujas lapu, Jūs sniedzat ziņas, kuras valsts drošības iestādei nepieciešamas, lai uzsāktu pārbaudi par Jūsu atbilstību pieejai valsts noslēpumam atbilstoši likumam "Par valsts noslēpumu". Aptaujas lapu aizpilda personīgi, tajā sniedzot skaidri salasāmu, patiesu un sev zināmu informāciju. Apzināta nepatiesu vai maldinošu ziņu sniegšana aptaujas lapā var būt par pamatu, lai atteiktu izsniegt vai pagarināt Jums speciālo atļauju darbam ar valsts noslēpumu.

Aptaujas lapā aizpilda visas tās ailes. Ja nav sniedzamas informācijas, tad raksta "Nav informācijas", savukārt, ja sniedzamajā informācijā nav izmaiņu kopš pēdējās aizpildītās aptaujas lapas, tad raksta "Nav izmaiņu". Ja informācijas apjoma dēļ nepieciešams, atbildes turpina sniegt aptaujas lapas pielikumā. Aptaujas lapā var nesniegt atbildi pēc būtības, norādot "Informāciju sniegšu pārrunās".

1. Vārds un uzvārds (drukātiem burtiem)		
Ja Jums ir mainīts vārds vai uzvārds, tad		
Iepriekšējais vārds vai uzvārds	Mainīšanas iemesls	Mainīšanas datums

2. Personas kods ___ ___ ___ ___ ___ ___ - ___ ___ ___ ___ ___ Iepriekšējais personas kods, ja mainīts ___ ___ ___ ___ ___ ___ - ___ ___ ___ ___ ___

3. Dzimšanas datums (dd/mm/gggg) _____/_____/_____	**4. Dzimšanas vieta**	
	Valsts	Pilsēta

5. Visas pilsonības, kādas Jums ir vai ir bijušas		
Pilsonība	Kad un kā iegūta/atteikta/atņemta	Pieņemšanas/atteikšanās iemesls

6. Kontaktinformācija		
6.1. Visi Jūsu izmantotie tālruņu numuri		6.2. Tālruņa numuri un e-pasta adreses, kuras izmantojot ar Jums var sazināties
Tālruņa numurs	Tālruņa numura lietotāja vārds un uzvārds (ja reģistrēts uz citas personas vārda)	

7. Vai iepriekš esat saņēmis(-usi) atļauju darbam ar vai strādājis(-usi) ar valsts noslēpumu saturošu informāciju, tai skaitā Ziemeļatlantijas līguma organizācijas, Eiropas Savienības vai citas valsts klasificēto informāciju?	
Informācijas veids un slepenības pakāpe	

(piemēram, valsts noslēpuma objekts ar slepenības pakāpi "slepeni", "Nato Secret", citas valsts "Confidential")	Atļaujas izsniedzējs

8. Vai Jums ir bijusi atteikta pieeja valsts noslēpumu saturošai informācijai, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības vai citas valsts klasificētai informācijai?
Ja ir liegta, lūdzu, norādiet informācijas veidu, slepenības pakāpi, laiku, lieguma iemeslus un apstākļus, kā arī iestādi, kas to liegusi.

9. Norādiet visas savas dzīvesvietas, kurās dzīvots ilgāk par trim mēnešiem, tai skaitā arī ārvalstīs
- Sniegt informāciju par pēdējiem 15 gadiem, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

No (gads)	Līdz (gads)	Adrese

10. Darba un dienesta vietas, tai skaitā arī ārvalstīs
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

No (gads)	Līdz (gads)	Darba vai dienesta vieta	Valsts

11. Ienākumi, kas gūti ārpus darba vai dienesta vietas un kuru summa gada laikā pārsniedz divas Ministru kabineta noteiktās minimālās mēnešalgas
- Sniegt informāciju pār pēdējiem desmit gadiem, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

No (gads)	Līdz (gads)	Ienākumu veids (autoratlīdzība, dividendes u. tml.)	Valsts

12. Militārā pieredze, kas nav militārais dienests, dalība militāros veidojumos (tai skaitā neformālos veidojumos, militāri taktisko spēļu dalībnieks u. c.) vai dalība militāros konfliktos, tai skaitā arī ārvalstīs (ja nav ienākumu gūšanas vieta, kas norādīta aptaujas lapas 11. punktā)

13. Izglītība, tai skaitā arī nepabeigtā
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

No (gads)	Līdz (gads)	Mācību iestāde	Apgūtā specialitāte	Iegūtais grāds

14. Ziņas par ģimenes locekļiem, tai skaitā arī par personu, ar kuru faktiski dzīvo kopā, pusbrāļiem un pusmāsām
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

	Vārds, uzvārds (iepriekšējie uzvārdi)	Dzimšanas datums	Pilsonība (visas)	Dzīvesvieta (valsts, pilsēta)	Nodarbošanās (darbavieta, amats, ja ir zināms)
14.1. Laulātais/ faktiskās kopdzīves partneris (pasvītrot atbilstošo)					
14.2. Tēvs					
14.3. Māte					
14.4. Brāļi, pusbrāļi (pilngadīgi)					
14.5. Māsas, pusmāsas (pilngadīgas)					
14.6. Bērni, tai skaitā arī faktiskās kopdzīves partnera (pilngadīgi)					
14.7. Laulātā/ faktiskās kopdzīves partnera tēvs					
14.8. Laulātā/ faktiskās kopdzīves partnera māte					
14.9. Laulātā/ faktiskās kopdzīves partnera brāļi, pusbrāļi (pilngadīgi)					
14.10. Laulātā/ faktiskās kopdzīves partnera māsas, pusmāsas (pilngadīgi)					

15. Ziņas par personām, kuras netiek norādītas aptaujas lapas 14. punktā, bet ar kurām ir kopīga dzīvesvieta vai mājsaimniecība, piemēram, citi radinieki, faktiskā kopdzīves partnera radinieki, citas personas, ar kurām dzīvo kopā
- Sniegt tikai sev zināmo informāciju.

Vārds un uzvārds	Dzimšanas datums un nodarbošanās (darbavieta, amats)	Radniecība vai cits kopīgas mājsaimniecības raksturojums

16. Jūsu un aptaujas lapas 14.1. punktā minētās personas ārpus Ziemeļatlantijas līguma organizācijas vai Eiropas Savienības esošu valstu apmeklējumi
- Sniegt tikai sev zināmo informāciju par pēdējiem pieciem gadiem.

Vieta, valsts	Iemesls (privāti vai profesionālā darbība)	No (mēnesis, gads)	Līdz (mēnesis, gads)

17. Vai Jūs vai aptaujas lapas 14.1. punktā minētā persona esat tikuši izraidīti no kādas valsts vai arī ir tikusi liegta iebraukšana kādā valstī?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai;
- Sniegt tikai sev zināmo informāciju.

Valsts	Datums/laikposms	Iemesls

18. Vai Jums ir kontakti ar personām, kas nav Ziemeļatlantijas līguma organizācijas vai Eiropas Savienības dalībvalstu pilsoņi vai kas dzīvo ārpus Ziemeļatlantijas līguma organizācijas vai Eiropas Savienības dalībvalstīm?

Vārds un uzvārds	Dzīvesvieta (valsts, pilsēta)	Radniecība vai kontaktu raksturs	Kontaktēšanās iemesli	Kontaktu veids, raksturs un biežums (klātienē, telefons, e-pasts u. c.)

19. Vai Jūs esat sodīts(-a) disciplināri? Lūdzu norādiet pārkāpuma apstākļus un soda piemērošanas laiku. Vai Jums ir šobrīd spēkā esoši disciplinārsodi?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

20. Vai Jums Latvijas Republikas teritorijā vai ārvalstīs ir piemērots administratīvais sods, izņemot tādus administratīvos sodus, par kuriem lēmumi pieņemti bez Jūsu klātbūtnes?
- Jānorāda gada laikā piemērotie administratīvie sodi;
- Nav jānorāda administratīvie sodi, kas piemēroti par apstāšanās vai stāvēšanas noteikumu pārkāpumu, kad neatradāties pārkāpuma izdarīšanas vietā, vai ja pārkāpums fiksēts ar tehniskajiem līdzekļiem, neapturot transportlīdzekli (piemēram, fotoradara fiksētie pārkāpumi).

Pārkāpums	Pārkāpuma izdarīšanas laiks un vieta	Sods

21. Norādiet visus kriminālprocesus, kuros esat bijis(-usi) iesaistīts(-a), tai skaitā ārvalstīs. Nav jānorāda kriminālprocesi, kuros piedalīties bija amata vai dienesta pienākums.
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai;
- Nesniegt informāciju par kriminālprocesiem, kuros piedalīties bija amata vai dienesta pienākums.

22. Vai Jums vai aptaujas lapas 14. punktā minētajām personām ir bijuši kontakti ar ārvalstu vēstniecību darbiniekiem, diplomātiem, ārvalstu drošības iestādēm, speciālajiem dienestiem, izlūkošanas vai pretizlūkošanas iestādēm?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai;
- Neattiecas uz amata vai dienesta pienākumu ietvaros notikušo;
- Sniegt tikai sev zināmo informāciju.

23. Vai Jums ir piedāvāts slepeni sadarboties?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

24. Vai esat šantažēts, saņēmis draudus vai izjutis cita veida apdraudējumu sev vai aptaujas lapas 14. punktā minētajām personām? Lūdzu norādiet apdraudējumu, draudu avotu, laikposmu.
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai;
- Sniegt tikai sev zināmo informāciju.

25. Vai Jūsu rīcībā ir fakti, informācija vai pieņēmumi, kas varētu tikt izmantoti pret Jums vai aptaujas lapas 14. punktā minētajām personām šantāžas vai diskreditācijas nolūkā?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai;
- Sniegt tikai sev zināmo informāciju.

26. Vai lietojat vai esat lietojis(-usi) narkotiskās vielas, tai skaitā medikamentus, kas satur narkotiskas vielas, vai psihotropos medikamentus (miega līdzekļus, trankvilizatorus, antidepresantus, antipsihotiskos līdzekļus u. c.)?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

Nosaukums	Lietošanas periods, biežums	Lietošanas iemesls

27. Vai Jūs esat konsultējies(-usies) ar ārstniecības personu (psihiatru, narkologu, psihoterapeitu, ģimenes ārstu vai citu ārstu), psihologu, psihoterapijas speciālistu vai atkarību speciālistu sakarā ar alkohola, narkotisko, psihotropo vai toksisko vielu lietošanu, azartspēļu vai citām atkarībām?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

Konsultāciju iemesls (uzstādītā diagnoze)	Konsultāciju laikposms	Ārstniecības persona (vārds, uzvārds) un tās kontaktinformācija, prakses vieta

28. Vai spēlējat vai esat spēlējis(-usi) azartspēles, tai skaitā totalizatori, interaktīvās spēles ar naudas likmēm un loterijas biļešu iegāde, apmeklējis spēļu zāles, kazino u. c.?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

Nosaukums, spēļu vieta	Spēlēšanas periods, biežums	Spēlēšanas iemesls

29. Vai esat vai esat bijis(-usi) reģistrēts(-a) no azartspēlēm un interaktīvajām izlozēm pašatteikušos personu reģistrā? Ja jā, tad kādos laikposmos (no–līdz)?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

30. Kādus sociālos tīklus Jūs lietojat un kādas viedokļu apmaiņas vai diskusiju platformas, tīmekļvietnes, blogus u. tml. Jūs pārvaldāt?

31. Norādiet visas profesionālās, sabiedriskās, politiskās, reliģiskās vai labdarības organizācijas, tai skaitā nereģistrētas interešu grupas, nodibinājumus un biedrības, kuru biedrs vai loceklis esat vai esat bijis(-usi), kurās darbojaties, strādājat vai esat darbojies(-usies), strādājis (-usi).
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

Nosaukums	No (gads)	Līdz (gads)	Organizācijas darbības mērķis un Jūsu loma/funkcijas

32. Vai Jūs vai aptaujas lapas 14. punktā minētās personas kādreiz ir darbojušās Padomju Savienības komunistiskajā partijā (PSKP), Latvijas komunistiskajā partijā (LKP), Latvijas PSR Darbaļaužu internacionālajā frontē, Darba kolektīvu apvienotajā padomē, Kara un darba veterānu organizācijā vai Vislatvijas sabiedrības glābšanas komitejā?
- Sniegt tikai sev zināmo informāciju.

Vārds, uzvārds	Nosaukums	Laikposms un iesaistes statuss

33. Vai Jums šobrīd ir aktuālas kredītsaistības, parādi, tai skaitā mikrokredīti, nebanku kreditētāju vai privātpersonu aizdevumi?

Veids (hipotēka, līzings, patēriņa, mikrokredīts u. c.)	Aizdevējs (firma/vārds, uzvārds/reģistrācijas Nr./personas kods)	Aizņēmuma mērķis	Saistību atlikušais termiņš

34. Vai šobrīd esat aizdevis līdzekļus vai īpašumus (nodevis lietošanā) citām fiziskām vai juridiskām personām, kuru summa pārsniedz divas Ministru kabineta noteiktās minimālās mēnešalgas?

Juridiskas personas nosaukums/ fiziskas personas vārds, uzvārds (kam aizdots)	Reģistrācijas numurs/ personas kods	Kas aizdots un tā vērtība (līdzekļi – summa, īpašums – vērtība)

35. Vai Jums ir īpašumi (kustama/nekustama manta, vērtspapīri, kapitāldaļas u. tml.) ārvalstīs?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

Īpašuma veids	Reģistrācijas numurs vai adrese	Dalība % vai skaits un vērtība	Īpašumā kopš

36. Vai Jums ir kredītiestāžu konti, glabātavas ārvalstīs?
- Sniegt visu informāciju, ja pirmo reizi pretendējat speciālās atļaujas saņemšanai;
- Sniegt informāciju par laikposmu no iepriekšējās aptaujas lapas aizpildīšanas brīža, ja atkārtoti pretendējat speciālās atļaujas saņemšanai.

Valsts	Kredītiestādes nosaukums	Kredītiestādes reģistrācijas numurs	Kontu, glabātavu skaits

Aptaujas lapai pievienoju pielikumu uz ____ lapām, kurās sniegtas ziņas par aptaujas lapas punktiem Nr. _____.

Es, _____, ar parakstu apliecinu, ka:

1) esmu iepazinies(-usies) ar normatīvajiem aktiem, kas reglamentē darbu ar valsts noslēpumu;

2) piekrītu, ka normatīvajos aktos noteiktajā kārtībā tiks veikta manis sniegtās informācijas pārbaude un apkopošana;

3) aizpildīju šo dokumentu, norādot visu informāciju, kas ir manā rīcībā, apzinoties, ka jebkurš tīši (apzināti) nepareizs apgalvojums vai faktu grozījums var būt par pamatu, lai liegtu man pieeju valsts noslēpumam.

Pēc speciālās atļaujas saņemšanas neatkarīgi no tās anulēšanas vai derīguma termiņa izbeigšanās apņemos:

1) neizpaust informāciju, kas satur valsts noslēpumu un man tiks uzticēta vai kļūs zināma;

2) bez iebildumiem un precīzi izpildīt ar slepenības režīma ievērošanu saistīto noteikumu, instrukciju, rīkojumu (pavēļu) prasības;

3) ziņot par mēģinājumiem iegūt no manis valsts noslēpumu, kā arī par man zināmiem slepenības režīma pārkāpumiem.

Esmu brīdināts (brīdināta), ka par valsts noslēpuma izpaušanu, kā arī par valsts noslēpuma objekta nozaudēšanu un citiem slepenības režīma pārkāpumiem tikšu saukts (saukta) pie krimināltiesiskās vai disciplinārās atbildības likumā noteiktajā kārtībā.

Apņemos valsts drošības iestādē pēc pieprasījuma iesniegt bankas un citu kredītiestāžu vai maksājumu platformu informāciju par maniem naudas uzkrājumiem un finanšu darījumiem, kā arī citu nepieciešamo informāciju, kurai pēc valsts drošības iestādes ieskatiem var būt būtiska nozīme, vērtējot manu atbilstību pieejai valsts noslēpumam, atbilstoši likuma "Par valsts noslēpumu" 10. panta desmitajai daļai.

Apņemos mēneša laikā rakstiski ziņot un nosūtīt kompetentajai valsts drošības iestādei informāciju par izmaiņām aptaujas lapas 1., 5., 6.2., 14.1., 16., 17., 18., 20., 21., 22., 23., 24., 26., 27. un 29. punktā norādītajos datos.

Sniegto ziņu pareizību apliecinu ar parakstu

_____ / _____/
(vārds, uzvārds/paraksts)

20____. gada ____._____

3. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Speciālās atļaujas paraugs

Nr.: _____

[...] KATEGORIJAS SPECIĀLĀ ATĻAUJA
PIEEJAI VALSTS NOSLĒPUMAM

Vārds, uzvārds: _____

Personas kods: _____

ir pārbaudīts(-a) atbilstoši normatīvajos aktos noteiktajām drošības prasībām un tam(tai) ir tiesības piekļūt

_____ valsts noslēpuma objektiem.

Speciālās atļaujas izsniegšanas datums: _____

Speciālās atļaujas derīguma termiņš: _____

Paraksts:

Izsniedzējs:

_____

_____

Zīmogs:

_____

(iestādes nosaukums, parakstītājs)

Kontaktinformācija: _____

(izsniedzēja kontaktinformācija)

4. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Sertifikāta paraugs pieejai konfidenciālas un augstākas slepenības pakāpes NATO klasificētajai informācijai

Nr.: _____

NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE

Certificate is hereby issued to:

Name, surname:

_____

Date and place of birth: _____

Place of employment; Title/military rank: _____

on the grounds of a personnel security clearance carried out by the

Republic of Latvia

_____

in accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, a person is to be declared suitable to be entrusted with information classified up to and including:

_____

The validity of this certificate will expire not later than:

_____

Signed:

Title: **Constitution Protection Bureau**
Republic of Latvia (NSA)

_____

_____

_____ **Stamp:**

Date of issue: _____

Contact details of the issuing authority: **ndi@sab.gov.lv**

Nr.: _____

NATO PERSONĀLA DROŠĪBAS PĀRBAUDES SERTIFIKĀTS

Sertifikāts ir izsniegts:

Vārds, uzvārds:

Dzimšanas datums un vieta: _____

Darba vieta, amats/dienesta pakāpe: _____

Pamatojoties uz personāla drošības pārbaudi, ko veikusi

Latvijas Republika

---

saskaņā ar šobrīd spēkā esošajām NATO drošības prasībām, ieskaitot Drošības pielikumu C-M(64)39 saistībā ar ATOMAL informāciju, persona ir atzīstama par piemērotu, lai tai uzticētu klasificētu informāciju līdz slepenības pakāpei (ieskaitot):

Serifikāta derīguma termiņš:

Paraksts:

Iestāde: **Latvijas Republikas Satversmes Aizsardzības birojs (NDI)**

_____

_____

Zīmogs:

_____

Dokumenta izdošanas datums: _____

Dokumenta izdevējiestādes kontaktinformācija: **ndi@sab.gov.lv**

5. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Sertifikāta paraugs pieejai konfidenciālas un augstākas slepenības pakāpes Eiropas Savienības klasificētajai informācijai

Nr.: _____

EU PERSONNEL SECURITY CLEARANCE CERTIFICATE

Certificate is hereby issued to:

Name, surname:

_____

Date and place of birth: _____

Place of employment; Title/military rank: _____

on the grounds of a personnel security clearance carried out by the

Republic of Latvia

_____

in accordance with current European Union security requirements, a person is to be declared suitable to be entrusted with information classified up to and including:

_____

The validity of this certificate will expire not later than:

_____

Signed:

Title: **Constitution Protection Bureau**
Republic of Latvia (NSA)

_____

_____

Stamp:

_____

Date of issue: _____

Contact details of the issuing authority: **ndi@sab.gov.lv**

Nr.: _____

EIROPAS SAVIENĪBAS PERSONĀLA DROŠĪBAS PĀRBAUDES SERTIFIKĀTS

Sertifikāts ir izsniegts:

Vārds, uzvārds:

Dzimšanas datums un vieta: _____

Darba vieta; Amats/Dienesta pakāpe: _____

Pamatojoties uz personāla drošības pārbaudi, ko veikusi

Latvijas Republika

---

saskaņā ar šobrīd spēkā esošajām Eiropas Savienības drošībām prasībām, persona ir atzīstama par piemērotu, lai tai uzticētu informāciju, kas ir klasificēta līdz slepenības pakāpei (ieskaitot):

Sertifikāta termiņš:

Paraksts:

Iestāde: **Latvijas Republikas Satversmes aizsardzības birojs (NDI)**

_____

_____

_____ **Zīmogs:**

Dokumenta izdošanas datums: _____

Dokumenta izdevējiestādes kontaktinformācija: **ndi@sab.gov.lv**

6. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Saistību raksts

Es, _____,
(vārds, uzvārds, personas kods)

esmu informēts(-a), ka

1) manā rīcībā ir nonākusi valsts noslēpumu saturoša informācija;

2) manā rīcībā ir nonākusi NATO, Eiropas Savienības vai ārvalstu klasificētā informācija;

3) ir aizliegts tālāk izpaust vai jebkādā veidā apstrādāt manā rīcībā nonākušo minēto klasificēto informāciju.

Esmu brīdināts(-a), ka:

saskaņā ar Krimināllikumā noteikto persona var tikt saukta pie krimināltatbildības par ziņu izpaušanu, kuras ir valsts noslēpums un kuras izpaudusi persona, kurai tās uzticētas vai kļuvušas zināmas sakarā ar dienesta vai darba pienākumu pildīšanu.

202____. gada _____ _____
(paraksts)

Pieņēma:

__VDI_____ darbinieks, VDI apliecības Nr. _____

202____. gada
____._____ / _____ /
(paraksts)

7. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Instruktāžas pieprasījums darbam ar signālu izlūkošanas informāciju

Aizpildīšanas datums _____

1. Veikt (SĀKOTNĒJO/NOSLĒGUMA) instruktāžu.
(nevajadzīgo nosvītrot)

2. Instruktāža darbam ar signālu izlūkošanas (COMINT/ELINT) informāciju.
(nevajadzīgo nosvītrot)

3. Vārds, uzvārds _____

4. Darba vai dienesta vieta _____

5. Amats _____

6. Dzimšanas datums _____

7. Darba vai dienesta tālruņa numurs _____

8. E-pasta adrese _____

9. Speciālā atļauja (kategorija/termiņš) _____ / _____

10. Nepieciešams darbam ar _____ signālu
(valsts vai starptautiskās organizācijas nosaukums)
izlūkošanas informāciju*

11. Sertifikāts darbam ar NATO klasificēto informāciju (informācijas līmenis, ar kuru atļauts strādāt/termiņš)
_____/_____**

Piezīmes.
1. * Aizpilda, ja nepieciešamas tiesības strādāt ar ārvalstu vai starptautiskās organizācijas signālu izlūkošanas informāciju.
2. ** Aizpilda, ja nepieciešamas tiesības strādāt ar NATO signālu izlūkošanas informāciju.

Pieprasītāja vārds, uzvārds, paraksts _____

8. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Instruktāžas anketa un apliecinājums par ATOMAL informācijas aizsardzību

1. Jūsu ieņemamais amats ir iekļauts Jūsu iestādes to amatu sarakstā, kuriem nepieciešama piekļuve ATOMAL informācijai. Šī instruktāža sniedz pamatinformāciju par to, kas ir ATOMAL informācija, kam ar to ir tiesības iepazīties, par tās speciālas aizsardzības nepieciešamību, atbildību un kaitējumu, ko var radīt šīs informācijas atklāšana neautorizētām personām.

2. ATOMAL ir speciālās kategorijas marķējums, kuru piešķir ar atomieročiem saistītai NATO klasificētajai informācijai, ko ar NATO starpniecību Latvijas Republikai ir nodevusi Amerikas Savienoto Valstu valdība vai Apvienotās Karalistes valdība un kas var būt jebkādā tehniski iespējamā tās fiksēšanas veidā, tai skaitā tie var būt materiāli, objekti, priekšmeti, vielas vai elektromagnētiskais lauks, kas ietver, uzglabā, uzkrāj vai atspoguļo šādu informāciju.

3. Saskaņā ar likuma "Par valsts noslēpumu" 2. panta ceturto daļu valsts noslēpuma statuss ir pilnībā attiecināms uz NATO klasificēto informāciju, ieskaitot ATOMAL informāciju, un šīs informācijas aizsardzība nodrošināma atbilstoši tās klasifikācijas pakāpei, ja citos normatīvajos aktos nav noteikts citādi.

4. ATOMAL informācijas nozaudēšana vai nelikumīga tās izpaušana var izraisīt likuma "Par valsts noslēpumu" 3. pantā paredzētās sekas attiecībā pret NATO.

5. Sertifikātu pieejai ATOMAL informācijai izsniedz tikai tām personām, kuras iepriekš ir saņēmušas atbilstošas kategorijas NATO sertifikātu un kuras apliecina iepazīšanos ar ATOMAL informācijas aizsardzības prasībām.

6. Saņemot sertifikātu darbam ar ATOMAL informāciju, Jums ir tiesības iepazīties ar ATOMAL informāciju tādā apjomā, kāds ir nepieciešams tiešo amata vai dienesta pienākumu pildīšanai vai konkrētu uzdevumu veikšanai.

7. ATOMAL informāciju marķē ar klasifikācijas pakāpei atbilstošu speciālās kategorijas marķējumu "ATOMAL", piemēram, COSMIC TOP SECRET ATOMAL, NATO SECRET ATOMAL, NATO CONFIDENTIAL ATOMAL.

8. Persona, kurai ir nodota ATOMAL informācija, ir atbildīga par tās aizsardzību. ATOMAL informācija atbilstoši tās klasifikācijas pakāpei jāaizsargā visu laiku no tās saņemšanas brīža. Šādu informāciju aizliegts atklāt personām, kas nav autorizētas to saņemt, neatkarīgi no personas amata vai tai izsniegtās speciālās atļaujas un sertifikāta līmeņa.

9. Persona, kuras pārvaldījumā ir ATOMAL informācija, atbild par drošības noteikumu ievērošanu un ziņo iestādes COSMIC drošības virsniekam vai tā vietniekam par jebkuriem apstākļiem, gadījumiem, tīšām vai netīšām darbībām, kuru dēļ var tikt apdraudēta ATOMAL informācijas drošība.

10. ATOMAL informāciju ir aizliegts pavairot.

11. ATOMAL informāciju drīkst apstrādāt tikai Nacionālās drošības iestādes sertificētās telpās.

12. ATOMAL informācijas aizsardzības prasības ir noteiktas Ministru kabineta 2023. gada 19. decembra noteikumos Nr. 822 "Valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu institūciju klasificētās informācijas aizsardzības noteikumi" un saistošajās NATO direktīvās, ar kurām iepazīties var pie iestādes COSMIC drošības virsnieka vai tā vietnieka.

13. Ar parakstu apliecinu, ka esmu saņēmis(-usi) instruktāžu par ATOMAL informācijas aizsardzības jautājumiem, kas jāievēro darbā ar ATOMAL informāciju. Esmu instruēts(-a) par ATOMAL informācijas aizsardzības nozīmību, draudiem un kaitējumu, ko Latvijas Republikas un Ziemeļatlantijas līguma organizācijas drošībai var radīt ATOMAL informācijas pazaudēšana vai izpaušana. Es apzinos, ka esmu pilnībā atbildīgs(-a) par man nodotās ATOMAL informācijas aizsardzību un varu tikt saukts(-a) pie krimināltatbildības pēc Latvijas Krimināllikuma 94. vai 95. panta par tīšu vai netīšu šīs informācijas izpaušanu.

Instruktāžu saņēma:

(paraksts un atšifrējums (vārds un uzvārds, personas kods vai cits identifikators))

Instruktāžu sniedza COSMIC drošības virsnieks vai vietnieks:

(paraksts un atšifrējums (vārds un uzvārds vai cits identifikators))

Datums:

Vārds, uzvārds un paraksts: _____

Datums: _____

9. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Valsts noslēpuma objekta (dokumenta) pirmās lapas noformējuma paraugs

Lappuses slepenības pakāpe un izplatīšanas ierobežojums (ja ir)

Dokumenta autora veidlapas rekvizīti

Tulkojums

Dokumenta kopējā slepenības pakāpe:

Saņemts no:
(atzīme par valsti vai starptautisko organizāciju)

Eksemplāra numurs:
(nepiemēro informācijai dienesta vajadzībām)

Reģistrācijas numurs:
(atzīme par oriģinālam piešķirto reģistrācijas numuru)

Dokumentā iekļautās klasificētās informācijas veidi un slepenības pakāpes:

Slepenības pakāpe:
(atzīme par oriģināla slepenības pakāpi)

Reģistrācijas numurs:

Adresāts:

Reģistrācijas datums:

Uz (atbildes gadījumā) (datums)

This information is the property of the originator and is supplied in accordance with the concluded bilateral agreement on the protection of classified information. It must not be passed on to third parties, used in any judicial proceedings or reclassified without the prior written approval of the originator. Original classification of the document must be preserved at all times. The originator reserves the right to inquire as to how this information has been used.

(gadījumā, ja valsts noslēpuma objekts tiek nodots ārvalstij vai starptautiskajai organizācijai)

Satura izklāsts

Dokumenta teksts

(N)
<teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts>
<teksts>
<teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts>
<teksts><teksts>
(K)
<teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts>
<teksts>
<teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts>
<teksts><teksts>
(DV)
<teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts><teksts>

(piemērs slepenības pakāpju speciālo saīsināto apzīmējumu lietojumam)

Pielikumi:

(norāde par iespēju apstrādāt pielikumu bez šī dokumenta un dokumenta slepenības pakāpi bez pielikuma)

Parakstītāja amata nosaukums | Amatpersonas paraksts | Vārds un uzvārds

(nosūtāmam dokumentam norāde par tā iznīcināšanas iespējamību pie noteiktiem apstākļiem vai pēc konkrēta laika)

Norādes par slepenības pakāpes maiņu vai par deklasificēšanu	Klasifikācijas pamatojums: (Tikai konfidenciāli un augstākas klasifikācijas dokumentiem un norāda tikai Ministru kabineta 2004. gada 26. oktobra noteikumu Nr. 887 "Valsts noslēpuma objektu saraksts" punktu)
	Slepenības statusa termiņš:
	Slepenības statusa pārskatīšanas laiks:
	(Attiecībā uz institūcijas organizatorisko dokumentu, rīkojumu, privāto un publisko tiesību līgumu un personāla dokumentu ir norāde, ka dokumenta slepenības pakāpe nav jāpārskata, kamēr tas ir spēkā)

Atzīme par dokumenta saņemšanu:

datums un laiks

reģistrācijas numurs

lappušu skaits

Lappuses slepenības pakāpe un izplatīšanas ierobežojums (ja ir)	Lappuses numurs – kopējais lappušu skaits

10. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Atsevišķu ārvalstu vai starptautisku organizāciju klasificēto dokumentu apzīmējumi

Valsts	Nato Restricted	Nato Confidential	Nato Secret	Cosmic Top Secret
Albānija	I KUFIZUAR	KONFIDENCIAL	SEKRET	TEPËR SEKRET
Beļģija	Nav nacionālā ekvivalenta[1]	CONFIDENTIEL VERTROUWELIJK	SECRET GEHEIM	TRÈS SECRET ZEER GEHEIM
Bulgārija	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	ПОВЕРИТЕЛНО	СЕКРЕТНО	СТРОГО СЕКРЕТНО
Kanāda	Nav nacionālā ekvivalenta[1]	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET
Horvātija	OGRANIČENO	POVJERLJIVO	TAJNO	VRLO TAJNO
Čehija	VYHRAZENÉ	DŮVĚRNÉ	TAJNÉ	PŘÍSNĚ TAJNÉ
Dānija	TIL TJENESTEBRUG	FORTROLIGT	HEMMELIGT	YDERST HEMMELIG
Igaunija	PIIRATUD	KONFIDENTSIAALNE	SALAJANE	TÄIESTI SALAJANE
Francija	Nav nacionālā ekvivalenta[1]	Nav nacionālā ekvivalenta[1]	SECRET [4]	TRÈS SECRET [5]
Vācija	VS-NUR FÜR DEN DIENSTGEBRAUCH	VS-VERTRAULICH	GEHEIM	STRENG GEHEIM
Grieķija	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ (Greek) PERIORISMENIS CHRISIS (Latin)	ΕΜΠΙΣΤΕΥΤΙΚΟ (Greek) EMPISTEYTIKO (Latin)	ΑΠΟΡΡΗΤΟ (Greek) APORRITO (Latin)	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ (Greek) AKROS APORRITO (Latin)
Ungārija	KORLÁTOZOTT TERJESZTÉSÜ	BIZALMAS	TITKOS	SZIGORÚAN TITKOS
Islande	TAKMARKAÐUR AÐGANGUR	TRÚNAÐARMÁL	LEYNDARMÁL	ALGJÖRT LEYNDARMÁL
Itālija	RISERVATO	RISERVATISSIMO	SEGRETO	SEGRETISSIMO
Latvija	DIENESTA VAJADZĪBĀM	KONFIDENCIĀLI	SLEPENI	SEVIŠĶI SLEPENI I
Lietuva	RIBOTO NAUDOJIMO	KONFIDENCIALIAI	SLAPTAI	VISIŠKAI SLAPTAI
Luksemburga	RESTREINT LUX	CONFIDENTIEL LUX	SECRET LUX	TRES SECRET LUX
Melnkalne	INTERNO	POVJERLJIVO	TAJNO	STROGO TAJNO
Nīderlande	Departementaal VERTROUWELIJK	Staatsgeheim CONFIDENTIEEL Stg. CONFIDENTIEEL	Staatsgeheim GEHEIM Stg. GEHEIM	Staatsgeheim ZEER GEHEIM Stg. ZEER GEHEIM
Ziemeļmaķedonija	ИНТЕРНО	ДОВЕРЛИВО	СТРОГО ДОВЕРЛИВО	ДРЖАВНА ТАЈНА
Norvēģija	BEGRENSET	KONFIDENSIELT	HEMMELIG	STRENGT HEMMELIG
Polija	ZASTRZEŻONE	POUFNE	TAJNE	ŚCIŚLE TAJNE
Portugāle	RESERVADO	CONFIDENCIAL	SECRETO	MUITO SECRETO
Rumānija	SECRET DE SERVICIU	SECRET	STRICT SECRET	STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ
Slovākija	VYHRADENÉ	DÔVERNÉ	TAJNÉ	PRÍSNE TAJNÉ

Slovēnija	INTERNO	ZAUPNO	TAJNO	STROGO TAJNO
Spānija	DIFUSIÓN LIMITADA	CONFIDENCIAL	RESERVADO	SECRETO
Turcija	HİZMETE ÖZEL	ÖZEL	GİZLİ	ÇOK GİZLİ
Lielbritānija	UK OFFICIAL - SENSITIVE	Nav nacionālā ekvivalenta[1]	UK SECRET	UK TOP SECRET
ASV	Nav nacionālā ekvivalenta[1]	CONFIDENTIAL	SECRET	TOP SECRET

Piezīme Nr. 1: Beļģija, Kanāda, Francija un ASV nacionālajās sistēmās nelieto klasificētās informācijas slepenības pakāpi RESTRICTED. Beļģija, Kanāda, Francija un ASV apstrādā un aizsargā NATO RESTRICTED klasificēto informāciju tādā veidā, kas nodrošina līdzvērtīgu klasificētās informācijas aizsardzību atbilstoši C-M(2002)49-REV1 paredzētajām prasībām.

Piezīme Nr. 2: Kopš 2021. gada 1. jūlija Francija savā nacionālajā sistēmā neizmanto klasificētās informācijas slepenības pakāpi CONFIDENTIEL DÉFENSE. Klasificēto informāciju, kas marķēta ar NATO CONFIDENTIAL, Francija apstrādā un aizsargā atbilstoši prasībām, kas attiecināmas uz klasificētās informācijas slepenības pakāpi SLEPENS. Klasificēto informāciju ar slepenības pakāpi CONFIDENTIEL DÉFENSE, kas radīta Francijā līdz 2021. gada 1. jūlijam, NATO apstrādā un aizsargā atbilstoši prasībām, kas attiecināmas uz klasificētās informācijas slepenības pakāpi NATO CONFIDENTIAL.

Piezīme Nr. 3: Lielbritānija savā nacionālajā sistēmā neizmanto klasificētās informācijas slepenības pakāpi CONFIDENTIAL. Ja nepastāv atsevišķas vienošanās starp Lielbritāniju un NATO, Lielbritānijai klasificēto informāciju ar slepenības pakāpi NATO CONFIDENTIAL jāapstrādā un jāaizsargā atbilstoši prasībām, kas attiecināmas uz klasificētās informācijas ar slepenības pakāpi UK SECRET.

Piezīme Nr. 4: Kopš 2022. gada 1. jūlija Francija savā nacionālajā sistēmā neizmanto klasificētās informācijas slepenības pakāpi SECRET DÉFENSE. Klasificēto informāciju ar slepenības pakāpi SECRET DÉFENSE, kas radīta Francijā līdz 2021. gada 1. jūlijam, NATO apstrādā un aizsargā atbilstoši prasībām, kas attiecināmas uz klasificētās informācijas slepenības pakāpi NATO SECRET.

Piezīme Nr. 5: Kopš 2022. gada 1. jūlija Francija savā nacionālajā sistēmā neizmanto klasificētās informācijas slepenības pakāpi TRÈS SECRET DÉFENSE. Klasificēto informāciju ar slepenības pakāpi TRÈS SECRET DÉFENSE, kas radīta Francijā līdz 2021. gada 1. jūlijam, NATO apstrādā un aizsargā atbilstoši prasībām, kas attiecināmas uz klasificētās informācijas slepenības pakāpi COSMIC TOP SECRET.

11. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Sevišķās lietvedības reģistrācijas un uzskaites žurnālos un/vai elektroniskajās informatīvajās sistēmās iekļaujamā informācija par nosūtīto valsts noslēpuma objektu, par nosūtīto NATO klasificēto informāciju un par nosūtīto Eiropas Savienības klasificēto informāciju

1. Dokumenta reģistrācijas datums.

2. Dokumenta reģistrācijas numurs.

3. Dokumenta autors un dokumenta nosaukums (īss saturs).

4. Dokumenta izstrādātāja struktūrvienība, atbildīgā darbinieka vārds un uzvārds.

5. Lapu skaits dokumentā un pielikumā.

6. Adresāts.

7. Eksemplāra numurs.

8. Informācija par dokumenta nosūtīšanu vai nodošanu:

8.1. dokumenta saņēmēja amats, vārds, uzvārds un paraksts par saņemšanu, dokumenta saņemšanas laiks;

8.2. dokumenta saņemšanu apliecinoša dokumenta numurs un datums.

9. Darbinieka vārds, uzvārds un paraksts par dokumenta atdošanu atpakaļ, dokumenta atdošanas datums un laiks.

10. Informācija par dokumenta pavairošanu:

10.1. dokumenta pavairošanas laiks un datums, kopijas numurs;

10.2. persona, kurai kopija nodota vai nosūtīta (amats, vārds un uzvārds);

10.3. dokumenta saņemšanas laiks, persona, kura saņēmusi kopiju (vārds, uzvārds un paraksts);

10.4. kopijas iznīcināšanas pamatojums, personas, kura iznīcināja kopiju, amats, vārds, uzvārds un paraksts;

10.5. piezīmes par kopijas iznīcināšanu.

11. Informācija par dokumenta iznīcināšanu:

11.1. dokumenta iznīcināšanas pamatojums, iznīcināšanas laiks, persona, kura iznīcināja dokumentu (amats, vārds, uzvārds un paraksts);

11.2. dokumenta iznīcināšanas akta numurs un datums.

12. Vispārīgas piezīmes.

12. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Sevišķās lietvedības reģistrācijas un uzskaites žurnālos un/vai elektroniskajās informatīvajās sistēmās iekļaujamā informācija par saņemto valsts noslēpuma objektu, par saņemto NATO klasificēto informāciju un par saņemto Eiropas Savienības klasificēto informāciju

1. Dokumenta saņemšanas datums.

2. Dokumenta saņemšanas reģistrācijas numurs.

3. Nacionālās drošības iestādes vai nosūtītāja piešķirtais dokumenta reģistrācijas numurs un datums.

4. Dokumenta nosūtītājs.

5. Dokumenta adresāts.

6. Dokumenta autors un dokumenta nosaukums (īss saturs).

7. Eksemplāra numurs.

8. Lapu skaits dokumentā un pielikumā.

9. Informācija par dokumenta nodošanu vai iepazīstināšanu ar tā saturu:

9.1. dokumenta saņēmēja amats, vārds, uzvārds, paraksts par saņemšanu un saņemšanas laiks;

9.2. darbinieka vārds, uzvārds un paraksts par dokumenta nodošanu atpakaļ.

10. Informācija par dokumenta nosūtīšanu:

10.1. institūcija, saņēmēja amats, vārds un uzvārds;

10.2. dokumenta saņemšanas laiks un datums, saņēmēja paraksts;

10.3. piezīmes par nosūtīšanu.

11. Informācija par dokumenta pavairošanu:

11.1. dokumenta pavairošanas laiks un datums, kopijas numurs;

11.2. persona, kam nodota vai nosūtīta kopija (amats, vārds un uzvārds);

11.3. dokumenta saņemšanas laiks, saņēmēja vārds, uzvārds un paraksts;

11.4. kopijas iznīcināšanas pamatojums, persona, kura iznīcinājusi kopiju (amats, vārds, uzvārds un paraksts);

11.5. piezīmes par kopijas iznīcināšanu.

12. Informācija par dokumenta iznīcināšanu:

12.1. dokumenta iznīcināšanas pamatojums, laiks, persona, kura iznīcinājusi dokumentu (amats, vārds, uzvārds un paraksts);

12.2. iznīcināšanas akta numurs un datums.

13. Vispārīgas piezīmes.

13. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Sūtījuma pavadraksts

Nosūtītājs

Adresāts

Sūtījuma Nr. _____ pavadraksts

Sūtījuma kopējā slepenības pakāpe: _____

Datums	Klasificētās informācijas slepenības pakāpe	Reģistrācijas numurs	Lappušu skaits, pielikumi (vai cits apjoma parametrs)	Saņēmēja paraksts un tā atšifrējums, saņemšanas datums, laiks un spiedogs

Sūtījuma iepakojuma drošības uzlīmes vai plombas numurs (ja tāda tiek izmantota): _____

Nosūtītāja vārds, uzvārds un paraksts: _____

Datums: _____

14. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Kurjera instruktāža un apliecinājums klasificētās informācijas transportēšanai

1. Jūsu ieņemamais amats ir iekļauts Jūsu iestādes amatu sarakstā, kas pilnvaro Jūs transportēt klasificēto informāciju. Pirms klasificētās informācijas transportēšanas uzsākšanas Jūs tiekat informēts par šīs informācijas speciālajiem aizsardzības pasākumiem un Jūsu kā kurjera pienākumiem un atbildību.

2. Transportējot klasificēto informāciju:

2.1. Jūs esat pilnībā atbildīgs par transportējamās informācijas drošību un aizsardzību no tās saņemšanas brīža līdz piegādes brīdim;

2.2. izmanto amata vai dienesta pienākumu veikšanai pieejamo autotransportu vai gaisa, jūras, dzelzceļa, autobusu satiksmes transportu, izmantojot rokas bagāžas iespējas. Transportēt līdz galamērķim pārnēsājot, atļauts tikai klasificētu informāciju līdz slepenības pakāpei "konfidenciāli" (ieskaitot). Pilsētas sabiedriskajā transportā atļauts transportēt tikai dienesta vajadzībām klasificēto informāciju;

2.3. sūtījumu nogādā tieši adresātam un par sūtījuma piegādi atbilstošajos dokumentos saņem adresāta parakstu;

2.4. ir aizliegts atstāt konfidenciālo un augstākas slepenības pakāpes klasificēto informāciju bez uzraudzības, to nogādā tieši līdz galamērķim bez pārtraukumiem; dienesta vajadzībām klasificēto informāciju var īslaicīgi uzglabāt personas rīcībā nodotā glabātavā, kas ir aizsargāta pret nepiederošu personu piekļūšanu, piemēram, viesnīcas seifs;

2.5. ir aizliegts iepazīties ar transportējamās informācijas saturu, izņemot gadījumus, ja transportēta tiek klasificētā informācija, kas ir nepieciešama Jums amata vai dienesta pienākumu veikšanai;

2.6. nodrošina to, lai nepiederoša persona nevarētu konstatēt, ka transportē klasificēto informāciju, un nav iespējams iepazīties ar tās saturu.

3. Jums personīgi nepieciešams sekot līdzi ceļošanas dokumentu (pase, ID karte) derīguma termiņiem.

4. Ja muitas, policijas un/vai imigrācijas dienesta amatpersona robežas šķērsošanas punktā pieprasa uzrādīt sūtījuma saturu:

4.1. Jums tā ir jāinformē, ka tiek transportēta klasificētā informācija un sūtījuma atvēršanu nav pieļaujams veikt publiskā vietā, un tā ir pieļaujama tikai muitas, policijas un/vai imigrācijas dienesta amatpersonas klātbūtnē;

4.2. Jums ir nepieciešams veikt piesardzības pasākumus, lai minētā amatpersona redzētu tikai tik daudz, cik tai nepieciešams savu tiešo pienākumu izpildei;

4.3. pēc pārbaudes Jums ir nepieciešams sūtījumu nekavējoties iepakot no jauna un saņemt muitas, policijas un/vai imigrācijas dienesta amatpersonas parakstu un zīmogu, kas apliecina, ka sūtījums ticis atvērts pārbaudei robežas šķērsošanas punktā.

5. Problēmsituācijās ir jāsazinās ar iestādi, kuras uzdevumā Jūs pildāt kurjera pienākumus, un jāinformē par radušos situāciju. Pirms informācijas nogādāšanas pārliecinieties, ka Jums ir vajadzīgie kontakti.

6. Ar parakstu apliecinu, ka esmu informēts par saviem pienākumiem un apzinos, ka esmu pilnībā atbildīgs par man uzticētās klasificētās informācijas aizsardzību tās transportēšanas laikā:

(paraksts un atšifrējums (vārds un uzvārds, personas kods vai cits identifikators))

Datums:

15. pielikums
Ministru kabineta
2023. gada 19. decembra
noteikumiem Nr. 822

Klasificētu informāciju saturošu dokumentu iznīcināšanas prasības

	Slepenības pakāpe	Minimālās iznīcināšanas metodes
Papīra dokuments un magnētiskās lentes[A]	Dienesta vajadzībām	• iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 30 mm^2; • dedzināt, līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
	Konfidenciāli	• iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 10 mm^2; • dedzināt, līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
	Slepeni	• iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 10 mm^2; • dedzināt, līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
	Sevišķi slepeni un visu pakāpju speciālās kategorijas	• iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 5 mm^2; • dedzināt, līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
Elektronisks dokuments (datne)	Visas	• dzēš, bet elektronisku dokumentu par iznīcinātu var uzskatīt tikai brīdī, kad ir iznīcināti visi tās akreditētās informācijas sistēmas elektroniskie datu nesēji, kurā elektroniskais dokuments izstrādāts vai uzglabāts
Cietie diski (HDD[B])	Dienesta vajadzībām	• ja elektroniskais datu nesējs ir droši dzēsts[C], to iznīcina sasmalcinot, un daļiņu lielums nedrīkst būt lielāks par 320 mm^2, bet, ja nav droši dzēsts, tad pēc sasmalcināšanas daļiņu lielums nedrīkst būt lielāks par 30 mm^2; • kausējot (t>800°C), līdz ārējais apvalks pārvērties pelnos un iekšējie mehānismi karstuma ietekmē ir viegli deformējušies
	Konfidenciāli	• ja elektroniskais datu nesējs ir droši dzēsts[C], to iznīcina sasmalcinot, un daļiņu lielums nedrīkst būt lielāks par 30 mm^2, bet, ja nav droši dzēsts, tad pēc sasmalcināšanas daļiņu lielums nedrīkst būt lielāks par 10 mm^2; • kausējot (t>800°C), līdz ārējais apvalks pārvērties pelnos un iekšējie mehānismi karstuma ietekmē ir viegli deformējušies
	Slepeni	• ja elektroniskais datu nesējs ir droši dzēsts[C], to iznīcina sasmalcinot, un daļiņu lielums nedrīkst būt lielāks par 20 mm^2, bet, ja nav droši dzēsts, tad pēc sasmalcināšanas daļiņu lielums nedrīkst būt lielāks par 10 mm^2; • kausējot, līdz ārējais apvalks pārvērties pelnos un iekšējie mehānismi karstuma ietekmē ir pilnīgi izkususi
	Sevišķi slepeni un visu pakāpju speciālās kategorijas	• ja elektroniskais datu nesējs ir droši dzēsts[C], to iznīcina sasmalcinot, un daļiņu lielums nedrīkst būt lielāks par 10 mm^2, bet, ja nav droši dzēsts, tad pēc sasmalcināšanas daļiņu lielums nedrīkst būt lielāks par 5 mm^2; • kausējot, līdz ārējais apvalks pārvērties pelnos un iekšējie mehānismi karstuma ietekmē ir pilnīgi izkususi
Optiskie diski, piemēram, kompaktdiski (CD), ciparu videodiski (DVD), augsta blīvuma optiskie diski (*Blu-Ray*)	Dienesta vajadzībām	• iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 30 mm^2; • dedzināt (t>300°C), līdz viss iznīcināmais objekts ir viegli deformēts
	Konfidenciāli	• iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 10 mm^2; • dedzināt (t>300°C), līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
	Slepeni	• iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 5 mm^2; • dedzināt (t>300°C), līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
	Sevišķi slepeni un visu pakāpju speciālās kategorijas	• iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 5 mm^2; • dedzināt (t>300°C), līdz iznīcināmais objekts pārvēršas pelnos vai sadeg

Pusvadītāju datu nesēji[D] un viedkartes	Dienesta vajadzībām	• veic elektroniskā datu nesēja drošu dzēšanu[C], iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 10 mm^2; • kausējot, dedzinot, līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
	Konfidenciāli	• veic elektroniskā datu nesēja drošu dzēšanu[C], iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 1 mm^2; • kausējot, dedzinot, līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
	Slepeni	• veic elektroniskā datu nesēja drošu dzēšanu[C], iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 1 mm^2; • kausējot, dedzinot, līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
	Sevišķi slepeni un visu pakāpju speciālās kategorijas	• veic elektroniskā datu nesēja drošu dzēšanu[C], iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 0,5 mm^2; • kausējot, dedzinot, līdz iznīcināmais objekts pārvēršas pelnos vai sadeg
Toneru kasetņu foto elementa rullis	Dienesta vajadzībām	• slīpējot/skrāpējot virsmu; • deformējot
	Konfidenciāli	• slīpējot virsmu, līdz zaļais/zilais slānis uz ruļļa ir noslīpēts; • iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 320 mm^2; • dedzinot 300°C vismaz 10 min
	Slepeni	• slīpējot virsmu, līdz zaļais/zilais slānis uz ruļļa ir noslīpēts; • iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 320 mm^2 • dedzinot 300 °C vismaz 10 min.
	Sevišķi slepeni un visu pakāpju speciālās kategorijas	• slīpējot virsmu, līdz zaļais/zilais slānis uz ruļļa ir noslīpēts; • iznīcina sasmalcinot, daļiņu lielums nedrīkst būt lielāks par 10 mm^2; • dedzinot 400°C vismaz 10 min
Mikročipa atmiņas moduļi īslaicīgai atmiņas glabāšanai (RAM[E])	Visas	Sistēmu operatīvās atmiņas moduļi (*Random Access Memory*) nav fiziski jāiznīcina, bet ir jāatvieno no sistēmas un jātur bez elektrības 24 h, pēc tam šos moduļus drīkst izmantot citiem mērķiem
Klasificēto informācijas sistēmu tīkla iekārtas (komutatori, maršrutētāji, ugunsmūri u. c.)	Visas	Tīkla iekārtām, kuras pārstāj lietot akreditētā informācijas sistēmā, atjauno to rūpnīcas iestatījumus. Ja tīkla iekārtas satur elektroniskus datu nesējus, tos izņem no iekārtas un atbilstoši iznīcina

Piezīmes.

1. **A** – magnētisko lenšu ietvarus vai kasetes salauž, atdalot pašu lenti no ietvara, iznīcina tikai pašu magnētisko lenti.

2. **B** – HDD (*Hard Disk Drive*) – cietais disks ir ilgtermiņa magnētiskā datu glabāšanas iekārta, kas sastāv no viena vai vairākiem magnētiskajiem diskiem, to piedziņas iekārtas (diskdziņa), lasīšanas un rakstīšanas galviņu komplekta un elektroniskas saskarnes, kas nodrošina šīs iekārtas sadarbību ar citām iekārtām.

3. **C** – elektroniska datu nesēja drošа dzēšana ir tā visu sektoru pārrakstīšana ar nullēm, vieniniekiem vai gadījuma skaitļu virknēm. Izmanto jebkuru programmatūru, kas nodrošina dzēšanas verifikāciju un kādu no sekojošiem dzēšanas standartiem – DoD 5220.22-M (3 pārrakstīšanas), DoD 5220.22-M (ECE) (7 pārrakstīšanas), DoD 5200.28-STD (7 pārrakstīšanas), NIST 800-88 *Purge*, VSITR (7 pārrakstīšanas), NATO *Standarts* (7 pārrakstīšanas) vai *Peter Gutmann* (35 pārrakstīšanas). Pēc drošas dzēšanas ir jāveic sasniegto rezultātu verifikācija.

4. **D** – SSD (*Solid-State Drive*) – pusvadītāju jeb cietvielu disks, kas izmanto integrālās shēmas pastāvīgai atmiņai, USB *Flash* – zibatmiņas, EPROM – pusvadītāja lasāmatmiņa, kuras saturu lietotājs var dzēst, apstarojot to ar ultravioleto gaismu un pēc tam ierakstīt jaunus datus, SD *card* – atmiņas kartes, RAID (*Redundant Array of Independent Disks*) kontrolieri – divu vai vairāku diskdziņu izmantošana vienu un to pašu datu glabāšanai dažādās vietās uz vairākiem cietajiem diskiem.

5. **E** – RAM (*Random-Access Memory*) – ir īslaicīgas atmiņas glabātava datora primārās (operatīvās) atmiņas daļā, kurā uzglabātajām programmu instrukcijām un datiem ir iespējama tieša pieeja no centrālā procesora, izmantojot ātrdarbīgo ārējo kopni. Brīvās pieejas atmiņa parasti ir energoatkarīga atmiņa.

© Oficiālais izdevējs "Latvijas Vēstnesis"