



HOTĂRÎRE
pentru aprobarea Regulamentului cu privire la asigurarea regimului
secret în cadrul autorităților publice și al altor persoane juridice

nr. 1176 din 22.12.2010

Monitorul Oficial nr.139-145/686 din 26.08.2011

* * *

În temeiul [Legii nr.245-XVI din 27 noiembrie 2008](#) cu privire la secretul de stat (Monitorul Oficial al Republicii Moldova, 2009, nr.45-46, art.123), cu modificările ulterioare, Guvernul

HOTĂRĂȘTE:

1. Se aprobă Regulamentul cu privire la asigurarea regimului secret în cadrul autorităților publice și al altor persoane juridice (se anexează).

2. În vederea implementării regulamentului nominalizat, autoritățile publice și alte persoane juridice, care utilizează informații atribuite secret de stat, în termen de 3 luni din la data intrării în vigoare a acestuia, vor elabora și vor aproba normele proprii cu privire la asigurarea regimului secret și vor întreprinde măsurile necesare pentru realizarea prezentei hotărâri.

3. Cetățenilor care, la momentul intrării în vigoare a prezentei hotărâri, dispun de dreptul de acces la secretul de stat și al căror acces a fost coordonat cu Serviciul de Informații și Securitate al Republicii Moldova, li se va menține acest drept pînă la expirarea termenelor stabilite de art.24 alin.(2) lit.b) și alin.(3) din [Legea nr.245-XVI din 27 noiembrie 2008](#) cu privire la secretul de stat, pentru forma 1 și, respectiv, forma 2 de acces la secret de stat.

4. Cetățenii care, la momentul intrării în vigoare a prezentei hotărâri, dispun de dreptul de acces la secret de stat, însă accesul acestora nu a fost coordonat cu Serviciul de Informații și Securitate al Republicii Moldova, vor fi supuși măsurilor de verificare în termen de 5 ani din data intrării în vigoare a prezentei hotărâri.

5. Autoritățile publice și alte persoane juridice vor asigura verificarea persoanelor prevăzute în pct.4 din prezenta hotărâre, conform unui plan coordonat cu Serviciul de Informații și Securitate al Republicii Moldova.

6. Se abrogă Hotărârea Guvernului nr.638 din 18 septembrie 1995 “Pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în organele puterii legislative, executive, juridice, organele administrației publice locale, întreprinderile, instituțiile și organizațiile Republicii Moldova”.

PRIM-MINISTRU

Vladimir FILAT

Contrasemnează:

Ministrul de stat

Victor Bodi

Chișinău, 22 decembrie 2010.

Nr.1176.

Aprobat
prin Hotărârea Guvernului
nr.1176 din 22 decembrie 2010

REGULAMENT
cu privire la asigurarea regimului secret în cadrul
autorităților publice și al altor persoane juridice

Capitolul I
DISPOZIȚII GENERALE PRIVIND ASIGURAREA
REGIMULUI SECRET

Secțiunea 1
Considerații generale

1. Prezentul Regulament stabilește modalitatea de asigurare a regimului secret în cadrul autorităților publice și al altor persoane juridice.

2. Regimul secret reprezintă ansamblul de măsuri organizatorico-juridice, care fac parte din sistemul național de protecție a secretului de stat, privind metodele și mijloacele utilizate de protejare a informațiilor și a purtătorilor materiali de informații atribuite la secret de stat, precum și acțiunile întreprinse în acest domeniu, care se referă inclusiv la:

- 1) secretizarea și desecretizarea informațiilor;
- 2) cerințele înaintate față de autoritățile publice, alte persoane juridice și personalul acestora cu privire la protecția secretului de stat;
- 3) modul de acces la secretul de stat;
- 4) întocmirea, evidența, păstrarea, procesarea, multiplicarea, utilizarea, transmiterea, distrugerea informațiilor atribuite la secret de stat;
- 5) protecția secretului de stat prin măsuri de ordin juridic și de ordin procedural, măsuri de protecție fizică, de protecție a sistemelor informaționale, de telecomunicații, precum și a personalului;
- 6) exercitarea controlului asupra măsurilor referitoare la protecția secretului de stat.

3. În sensul prezentului Regulament se definesc următoarele noțiuni:

autorizație de acces la secret de stat – document prin care se confirmă că persoana fizică, titular al acesteia, poate avea acces la secret de stat de un anumit grad de secretizare;

articole secrete – complexe, sistemele și articolele de înarmare și tehnică militară, precum și anumite instalații, agregate, blocuri, rețele, dispozitive, materiale, produse chimice, aparataj, utilaj, machete de produse și altele asemenea, care fac parte din categoria informațiilor atribuite la secret de stat;

secretizarea informației – încadrarea informației la un anumit grad de secretizare;

desecretizarea informației – scoaterea informației secretizate de sub incidența reglementărilor privind secretul de stat și suprimarea parafei de secretizare aplicată pe purtătorul material de asemenea informație;

certificat de securitate – document prin care se confirmă dreptul persoanelor juridice, cu excepția autorităților publice, de a desfășura o activitate ce ține de utilizarea informațiilor atribuite la secret de stat, crearea mijloacelor de protejare a informației, realizarea măsurilor și/sau prestarea serviciilor de protecție a secretului de stat;

zonă de securitate – perimetru delimitat și special amenajat unde sînt gestionate informațiile atribuite la secret de stat.

4. Măsurile de protecție a informațiilor atribuite la secret de stat trebuie stabilite în raport cu:

- 1) gradul de secretizare a informațiilor;
- 2) volumul și purtătorii materiali ai informațiilor;
- 3) modul de acordare a dreptului de acces la secret de stat;
- 4) calitatea, funcția și numărul persoanelor care au sau pot avea acces la secret de stat;
- 5) amenințările, riscurile și vulnerabilitățile ce pot avea consecințe asupra informațiilor atribuite la secret de stat.

Secțiunea a 2-a

Reguli generale privind secretizarea și desecretizarea informațiilor

5. Informațiile din domeniul apărării naționale, economiei, științei și tehnicii, relațiilor externe, securității statului, asigurării ordinii de drept și activității autorităților publice sînt secretizate, ținînd cont de importanța pe care o au pentru interesele și/sau securitatea Republicii Moldova și de consecințele ce s-ar produce ca urmare a pierderii sau divulgării lor neautorizate.

6. În funcție de gravitatea prejudiciilor ce pot fi cauzate intereselor și/sau securității Republicii Moldova în cazul divulgării sau pierderii acestor informații, [Legea nr.245-XVI din 27 noiembrie 2008](#) cu privire la secretul de stat (în continuare – Legea) stabilește 4 grade de secretizare a informațiilor atribuite la secret de stat și, respectiv, parafele de secretizare pentru purtătorii materiali de asemenea informații:

1) “Strict secret” – grad de secretizare atribuit informațiilor a căror divulgare neautorizată poate aduce prejudicii deosebit de grave intereselor și/sau securității Republicii Moldova;

2) “Secret” – grad de secretizare atribuit informațiilor a căror divulgare neautorizată poate dăuna grav intereselor și/sau securității Republicii Moldova;

3) “Confidențial” – grad de secretizare atribuit informațiilor a căror divulgare neautorizată poate dăuna intereselor și/sau securității Republicii Moldova;

4) “Restricționat” – grad de secretizare atribuit informațiilor a căror divulgare neautorizată poate fi în dezavantajul intereselor și/sau securității Republicii Moldova sau poate conduce la divulgarea unei informații secretizate cu parafa “Strict secret”, “Secret” sau “Confidențial”.

7. În corespundere cu gradele de secretizare a informațiilor atribuite la secret de stat, sînt stabilite următoarele termene de secretizare a informațiilor, care încep din ziua în care pe purtătorul material de informații atribuite la secret de stat a fost aplicată parafa de secretizare:

1) “Strict secret” – pînă la 25 de ani;

2) “Secret” – pînă la 15 ani;

3) “Confidențial” – pînă la 10 ani;

4) “Restricționat” – pînă la 5 ani.

8. Termenul de secretizare a informațiilor despre persoanele care colaborează sau au colaborat confidențial cu organele ce desfășoară activitate de informații, de contrainformații și operativă de investigații este nelimitat, indiferent de gradul de secretizare.

9. Termenul de secretizare a datelor despre identitatea și calitatea ofițerului de informații este de 50 de ani din data eliberării din serviciu a ofițerului, dar nu mai puțin de 25 de ani din data decesului acestuia. Termenul poate fi prelungit pe perioade consecutive a cîte 10 ani, la decizia directorului Serviciului de Informații și Securitate, în cazul în care desecretizarea datelor contravine intereselor asigurării securității naționale și/sau a drepturilor și intereselor legitime ale urmașilor ofițerului de informații.

10. Termenele de secretizare pot fi prelungite în anumite situații excepționale de către Comisia interdepartamentală pentru protecția secretului de stat, în baza unei motivații temeinice, la solicitarea conducătorilor autorităților publice învestite cu împuterniciri de dispoziție asupra informațiilor atribuite la secret de stat sau, după caz, din oficiu.

11. Drept temei pentru secretizarea informațiilor, elaborate/primate în cadrul activității de administrare, de producție, științifice și de altă natură a autorităților publice și altor persoane juridice și aplicarea parafei de secretizare pe purtătorii lor materiali, este corespunderea cu:

1) prevederile articolelor 7 și 8 din [Lege](#);

2) Nomenclatorul informațiilor atribuite la secret de stat;

3) nomenclatoarele departamentale de informații care urmează a fi secretizate.

12. Categoriile informațiilor atribuite la secret de stat se stabilesc conform Nomenclatorului informațiilor atribuite la secret de stat.

13. În scopul concretizării și sistematizării informațiilor în domeniile lor de activitate, autoritățile publice învestite cu împuterniciri de dispoziție asupra acestor informații, elaborează, în baza și în limitele Nomenclatorului informațiilor atribuite la secret de stat, nomenclatoare departamentale detaliate de informații, care urmează a fi secretizate. După caz, pot fi elaborate și nomenclatoare interdepartamentale

detaliate de informații, care urmează a fi secretizate și care trebuie să corespundă Nomenclatorului informațiilor atribuite la secret de stat.

14. Pentru elaborarea nomenclatoarelor departamentale detaliate de informații care urmează a fi secretizate, în cadrul autorităților publice învestite cu împuterniciri de dispoziție asupra acestora se instituie comisii în componența cărora se includ, în mod obligatoriu, și reprezentanți ai subdiviziunilor interioare de protecție a informațiilor atribuite la secret de stat. În vederea elaborării nomenclatoarelor interdepartamentale detaliate de informații care urmează a fi secretizate, se instituie comisii interdepartamentale, în componența cărora se includ, în mod obligatoriu, și reprezentanți ai subdiviziunilor interioare de protecție a informațiilor atribuite la secret de stat din cadrul fiecărei autorități publice implicate.

15. În nomenclatorul departamental detaliat de informații, care urmează a fi secretizate, trebuie să fie prevăzute categoriile informațiilor, iar, în caz de necesitate, și informațiile aparte privind aspectele de activitate ale autorității publice. Gradul de secretizare a acestor informații se stabilește în mod diferențiat, ținându-se cont de gravitatea prejudiciilor ce pot fi cauzate intereselor și/sau securității Republicii Moldova în cazul divulgării sau pierderii acestor informații.

16. Nomenclatoarele departamentale/interdepartamentale detaliate de informații, care urmează a fi secretizate, se aprobă de conducătorul autorității/conducătorii autorităților publice respective și conțin informații cu împuternicirile de dispoziție asupra cărora sînt învestite autoritățile publice în cauză, stabilesc gradele și termenele lor de secretizare.

17. Conținutul nomenclatoarelor departamentale/interdepartamentale detaliate de informații, care urmează a fi secretizate, nu sînt date publicității. Ele urmează să fie aduse la cunoștința structurilor de subordonare departamentală, precum și a persoanelor juridice care efectuează lucrări cu utilizarea informațiilor atribuite la secret de stat, în partea ce se referă la activitatea acestora, pentru a putea fi utilizate la secretizarea informațiilor. De asemenea, persoanele juridice care efectuează lucrări cu utilizarea informațiilor atribuite la secret de stat, în coordonare cu beneficiarul acestor lucrări, pot elabora nomenclatoare detaliate separate de informații care urmează a fi secretizate.

18. Secretizarea informației se efectuează prin încadrarea acesteia la un anumit grad de secretizare, potrivit nomenclatorului departamental/ interdepartamental detaliat de informații, care urmează a fi secretizate, și, respectiv, asigurarea aplicării parafei de secretizare, conform gradului de secretizare.

19. Decizia cu privire la secretizarea informației se adoptă de către persoana cu funcții de răspundere care semnează documentul, la propunerea executantului, și se manifestă prin aplicarea semnăturii pe suportul material de informații.

20. Secretizarea documentelor care se semnează de către conducătorul autorității publice sau al altei persoane juridice se efectuează la propunerea șefilor subdiviziunilor interioare care au întocmit documentul.

21. Secretizarea documentelor care se semnează de către șefii subdiviziunilor interioare se efectuează la propunerea executanților.

22. Aplicarea parafei de secretizare pe document se asigură de către persoana care-l întocmește.

23. Gradul de secretizare a informației se determină în conformitate cu Nomenclatorul informațiilor atribuite la secret de stat și nomenclatoarele departamentale/interdepartamentale detaliate de informații care urmează a fi secretizate, iar în cazuri aparte – conform părții care se referă la lucrările ce urmează a fi efectuate în baza acestor nomenclatoare.

24. Gradul de secretizare a informațiilor ce se conțin în document se determină de executant și persoana care semnează sau aprobă documentul.

25. Gradul de secretizare a informațiilor privind efectuarea unor lucrări în comun și a altor lucrări se determină de către beneficiarul acestor lucrări în comun cu executantul lucrărilor.

26. Gradul de secretizare a informațiilor ce se conțin în tezele de licență, masterat, doctorat, alte lucrări cu tematică secretă, se determină de către executant și conducătorul lui științific.

27. Gradul de secretizare a informațiilor ce se conțin în cererea de înregistrare a dreptului de proprietate intelectuală se determină de către autor (coautori) și conducătorul autorității publice învestite

cu împuterniciri de dispoziție asupra informațiilor atribuite la secret de stat, care prezintă cererea.

28. Documentul elaborat pe baza prelucrării informațiilor cu grade de secretizare diferite va fi secretizat conform noului conținut, care poate fi superior originalelor.

29. Documentul rezultat din cumularea neprelucrată a unor extrase provenite din informații secretizate va primi gradul de secretizare corespunzător conținutului extrasului cu cel mai înalt nivel de secretizare.

30. Rezumatele, traducerile și extrasele din documentele secretizate primesc gradul de secretizare corespunzător conținutului.

31. Dacă unele părți ale unui document (spre exemplu, pagini, paragrafe, secțiuni, anexe) conțin informații ce se atribuie la diferite grade de secretizare, pe acestea se vor aplica parafele corespunzătoare gradului de secretizare respectiv. În acest caz, gradul de secretizare atribuit documentului integral va fi cel al părții cu cel mai înalt grad de secretizare.

32. Scrisorile sau notele care însoțesc documentele anexate poartă nivelul de secretizare cel mai înalt care a fost atribuit acestora din urmă. Autoritatea emitentă indică în mod clar gradul de secretizare în cazul în care sînt separate de anexele lor.

33. Parafa de secretizare reflectă gradul superior de secretizare a informațiilor ce se conțin în lucrări, documente, articole și se marchează prin una din inscripțiile: "Strict secret", "Secret", "Confidențial" sau "Restricționat".

34. Parafa de secretizare a lucrării, etapelor și părților ei componente se indică de către beneficiarul acestora în sarcina (planul) de executare a lucrării.

35. Cînd se aplică parafa "Strict secret", se indică, sub linie, punctul din nomenclatorul departamental/interdepartamental detaliat de informații care urmează a fi secretizate, în baza căruia se determină parafa.

36. Parafa de secretizare a articolului și a fiecărei părți componente a acestuia se indică, de către cel care elaborează sau fabrică, în documentația cu privire la articol (spre exemplu, condițiile tehnice, instrucțiunile privind exploatarea, pașaportul tehnic).

37. Secretizarea informațiilor care nu corespund criteriilor stabilite în punctul 11 din prezentul Regulament și, respectiv, aplicarea parafei de secretizare cu privire la aceste informații nu se admite.

38. În cazul în care persoanele cu funcții de răspundere din cadrul autorităților publice și altor persoane juridice consideră că divulgarea anumitor informații este de natură să aducă atingere intereselor și/sau securității Republicii Moldova, dar nu pot fi identificate cu cele incluse în nomenclatorul respectiv, vor asigura secretizarea preliminară a acestora, prin aplicarea parafei, conform gradului de secretizare apreciat.

39. Dacă informația care nu este prevăzută în nomenclatorul departamental/interdepartamental detaliat de informații care urmează a fi secretizate dezvăluie informațiile ce se conțin în acest nomenclator, atunci acestea trebuie să aibă același grad de secretizare, care este menționat în punctele respective ale nomenclatorului.

40. Persoanele responsabile, în termen de o lună de la secretizarea preliminară a informațiilor, sînt obligate să prezinte persoanei cu funcție de răspundere, care a aprobat nomenclatorul respectiv, propuneri de completare/modificare a acestuia, însoțite de o motivație temeinică. Pînă la adoptarea unei decizii definitive, caracterul secret al acestor informații va fi asigurat în conformitate cu cerințele prezentului Regulament.

41. După aprecierea informațiilor secretizate preliminar în conformitate cu prevederile articolului 12 alineatul (3) din [Lege](#), conducătorii autorităților publice și ai altor persoane juridice, care au aprobat nomenclatorul respectiv, vor lua o decizie argumentată, în formă scrisă, cu privire la completarea/modificarea nomenclatorului în vigoare sau scoaterea parafei de secretizare atribuite preliminar.

42. Propunerile de modificare și/sau completare a Nomenclatorului informațiilor atribuite la secret de stat, însoțite de motivația temeinică, se înaintează Guvernului.

43. Conducătorii autorităților publice, învestite cu împuterniciri de dispoziție asupra informațiilor atribuite la secret de stat, vor dispune verificarea periodică, dar nu mai rar decît o dată la 5 ani, de

regulă, după revizuirea conținutului nomenclatoarelor departamentale/interdepartamentale detaliate de informații care urmează a fi secretizate, a tuturor informațiilor secrete de stat cărora le-au fost atribuite grade de secretizare, prilej cu care, dacă este necesar, vor fi reevaluate gradele, respectiv, parafele, precum și termenele de secretizare a acestora. Dacă este posibil, autoritatea emitentă indică pe documentul secretizat data sau termenul începând cu care informațiile pe care acesta le cuprinde li se va putea reduce gradul de secretizare sau vor putea fi desecretizate.

44. La finisarea lucrărilor efectuate în comun și a altor lucrări, integral sau etapizat, beneficiarul acestora în comun cu executantul vor examina chestiunea cu privire la păstrarea sau modificarea gradului de secretizare a informațiilor stabilit anterior și, în caz de necesitate, vor opera modificări și completări la capitolul respectiv al sarcinii în vederea executării lucrărilor.

45. Modificarea gradului de secretizare a informațiilor implică, în mod obligatoriu, modificarea parafei de secretizare pe purtătorii materiali și/sau în documentația de însoțire a acestora.

46. Modificarea parafei de secretizare se efectuează în conformitate cu prevederile articolului 15 din [Lege](#).

47. În termen de 6 luni de la data stabilită de reducere a gradului de secretizare categoriilor de informații prevăzute în Nomenclatorul informațiilor atribuite la secret de stat și în nomenclatoarele departamentale de informații care urmează a fi secretizate, autoritățile publice sau alte persoane juridice, în temeiul deciziei conducătorilor autorităților publice cu împuterniciri de dispoziție asupra acestor informații, vor asigura modificarea parafei de secretizare a purtătorilor materiali de informații atribuite la secret de stat.

48. În toate celelalte cazuri, modificarea parafei de secretizare a purtătorilor materiali de informații atribuite la secret de stat se efectuează, în temeiul deciziei persoanei cu funcție de răspundere care a secretizat informația sau a succesorului ei de drept, în termen de 3 luni de la data stabilită de reducere a gradului de secretizare a informațiilor conținute de ele.

49. Modificarea parafei de secretizare în cazul majorării gradului de secretizare a informațiilor se face imediat, în temeiul deciziei scrise a persoanei cu funcție de răspundere care a secretizat informația sau a succesorului ei de drept.

50. Decizia cu privire la modificarea parafei de secretizare urmează să fie argumentată și se emite în formă scrisă.

51. Persoana cu funcții de răspundere care a secretizat informația sau succesorul ei de drept, în cel mai restrâns termen, informează despre decizia cu privire la modificarea parafei de secretizare autoritățile sau persoanele juridice cărora le-a fost expediat documentul, iar acestea, la rândul lor, au responsabilitatea de a informa destinatarul succesiv cărora le-au transmis originalul documentului sau o copie a acestuia. În baza deciziei menționate, autoritățile sau persoanele juridice destinate să efectueze modificarea respectivă a parafei de secretizare a documentului.

52. În cazul în care propunerea cu privire la secretizarea sau modificarea parafei de secretizare a fost înaintată de către autoritatea publică sau persoana juridică care a primit documentul, expeditorul va informa destinatarul documentului despre decizia luată, indiferent de caracterul acesteia.

53. Privitor la modificarea parafei de secretizare a documentelor și articolelor se efectuează înscrieri în registrele de evidență respective, în fișe, pe documente, în documentația tehnică (de însoțire) a articolelor. Data și noul grad de secretizare vor fi indicate pe document deasupra sau sub vechea inscripție, care va fi anulată prin trasarea unei linii oblice.

54. Informațiile secrete de stat se desecretizează de către persoanele cu funcții de răspundere cu împuterniciri de secretizare a informațiilor respective dacă:

1) termenul de secretizare a expirat;

2) s-au schimbat circumstanțele obiective și, drept urmare, protecția în continuare a anumitor informații atribuite la secret de stat devine inoportună;

3) au fost operate modificări în articolele 7 și 8 din [Lege](#), în Nomenclatorul informațiilor atribuite la secret de stat sau în nomenclatoarele departamentale/interdepartamentale detaliate de informații care urmează a fi secretizate și, drept urmare, protecția în continuare a anumitor informații atribuite la secret de stat devine inoportună;

4) există o decizie privind recunoașterea secretizării informațiilor drept neîntemeiată.

55. Persoanele cu funcții de răspundere care au emis documente secrete vor evalua periodic necesitatea de desecretizare sau de micșorare a gradului de secretizare acordat anterior acestora. Ori de câte ori este posibil, emitentul unui document secretizat trebuie să precizeze dacă acesta poate fi desecretizat ori trecut la un grad inferior de secretizare, la o anumită dată sau la producerea unui anumit eveniment.

56. În scopul evaluării necesității de desecretizare sau de micșorare a gradului de secretizare acordat informațiilor, pot fi create comisii speciale în componența cărora va fi inclusă, în mod obligatoriu, o persoană din cadrul Subdiviziunii de protecție a informațiilor atribuite la secret de stat, care dispune de forma de acces corespunzătoare gradului de secretizare a acestor informații.

57. Decizia cu privire la desecretizarea informațiilor se adoptă de către persoanele cu funcții de răspundere cu împuterniciri de secretizare a informațiilor respective. Această decizie se emite în formă scrisă și urmează să fie argumentată.

58. Comisia interdepartamentală pentru protecția secretului de stat, precum și conducătorii autorităților publice și ai altor persoane juridice sînt împuterniciți de a desecretiza informațiile care au fost secretizate neîntemeiat de către persoanele cu funcții de răspundere din subordine.

59. În cazul păstrării informațiilor atribuite la secret de stat în fondurile închise ale arhivelor, purtătorii materiali ai acestora se vor desecretiza de către conducătorii arhivelor de stat, cu condiția că organizația întemeietoare a fondului sau succesorul ei de drepturi le deleagă astfel de împuterniciri. În caz de lichidare a organizației întemeietoare a fondului și de lipsă a succesorului ei de drepturi, chestiunea privind desecretizarea purtătorilor materiali de informații atribuite la secret de stat este examinată de Comisia interdepartamentală pentru protecția secretului de stat.

60. Persoanele cu funcții de răspundere împuternicite de a secretiza informațiile vor asigura informarea autorităților sau persoanelor juridice, cărora le-a fost expediat documentul, despre faptul desecretizării acestuia.

61. Informațiile secretizate, despre care s-a stabilit cu certitudine că sînt divulgate sau iremediabil pierdute, vor fi desecretizate. Desecretizarea se face numai în baza investigației prin care s-a stabilit faptul divulgării sau pierderii informațiilor respective ori a suportului material al acestora, cu acordul scris al emitentului.

62. În cazul în care se consideră că anumite informații au fost secretizate neîntemeiat, cetățenii sau persoanele juridice sînt în drept să conteste decizia de secretizare, în conformitate cu prevederile articolului 17 din [Lege](#).

Secțiunea a 3-a

Subdiviziunile interioare de protecție a informațiilor atribuite la secret de stat

63. În scopul implementării acțiunilor cu privire la asigurarea regimului secret și organizarea controlului permanent privind respectarea măsurilor de protecție a informațiilor atribuite la secret de stat în autoritățile publice și alte persoane juridice trebuie să existe, în condițiile [Legii](#), subdiviziuni interioare de protecție a informațiilor atribuite la secret de stat (în continuare – Subdiviziuni de protecție), cu atribuții specifice.

64. Crearea, reorganizarea și lichidarea Subdiviziunilor de protecție se efectuează în baza deciziei (ordinului) conducătorilor autorităților publice sau altor persoane juridice deținătoare de informații atribuite la secret de stat, prin coordonare cu Serviciul de Informații și Securitate. La crearea noilor Subdiviziuni de protecție, Serviciul de Informații și Securitate verifică existența condițiilor necesare pentru funcționarea normală a acestora.

65. Funcțiile, drepturile, obligațiile, organizarea Subdiviziunii de protecție se stabilesc în regulamentul de funcționare al acesteia, elaborat în conformitate cu cerințele prezentului Regulament, coordonat cu Serviciul de Informații și Securitate și aprobat de conducătorul autorității publice sau al altor persoane juridice.

66. În funcție de volumul și importanța activităților ce implică informații atribuite la secret de stat,

Subdiviziunile de protecție pot include subdiviziuni de regim secret, care organizează asigurarea și respectarea regimului secret în autoritățile publice sau alte persoane juridice, și subdiviziuni ale lucrărilor de secretariat secrete, care elaborează și înfăptuiesc măsuri ce țin de asigurarea regimului secret la executarea lucrărilor de secretariat secrete cu efectuarea controlului asupra respectării lor. De asemenea, reieșind din specificul activității și volumul informațiilor atribuite la secret de stat în cadrul autorităților publice sau al altor persoane juridice, pot fi create grupuri de lucru, secții sau unități secrete, iar în cadrul acestora pot fi numiți reprezentanți ai Subdiviziunii de protecție.

67. În autoritățile publice sau alte persoane juridice unde se efectuează un volum mare de lucrări secrete pot fi numiți locțiitori ai conducătorilor autorităților publice sau persoanelor juridice, responsabili de asigurarea regimului secret.

68. Atunci când autoritățile publice sau alte persoane juridice efectuează un volum redus de lucrări cu informații atribuite la secret de stat, acțiunile cu privire la asigurarea regimului secret și organizarea controlului permanent privind respectarea măsurilor de protecție a informațiilor atribuite la secret de stat se realizează de către conducătorul acestora sau de către o persoană numită prin ordin special de către conducător. În acest caz, atribuțiile Subdiviziunii de protecție vor fi îndeplinite de persoana respectivă.

69. Subdiviziunea de protecție coordonează activitatea altor subdiviziuni în partea ce ține de asigurarea protecției secretului de stat și se subordonează nemijlocit conducătorului autorității publice sau al altei persoane juridice și locțiitorului responsabil de asigurarea regimului secret.

70. Se interzice angajarea temporară a persoanelor în Subdiviziunea de protecție, în subdiviziunile de cifrare sau mobilizare ale autorităților publice sau ale altor persoane juridice.

71. Desemnarea persoanelor în funcția de locțiitori ai conducătorilor autorităților publice și ai altor persoane juridice, responsabili de asigurarea regimului secret, a șefilor Subdiviziunilor de protecție, precum și eliberarea acestora din funcție se efectuează prin coordonare cu Serviciul de Informații și Securitate.

72. În cadrul Subdiviziunilor de protecție sînt angajate persoanele care au drept de acces la secret de stat, dau dovadă de cunoștințe necesare și au experiență în organizarea regimului secret.

73. Șeful Subdiviziunii de protecție trebuie să dispună de dreptul de acces la secret de stat, corespunzător celui mai înalt grad de secretizare a informațiilor gestionate de autoritatea publică sau altă persoană juridică respectivă.

74. La desemnarea în/eliberarea din funcție a persoanelor din cadrul Subdiviziunii de protecție se va efectua inventarierea documentelor și altor purtători materiali de informații atribuite la secret de stat, aflate în gestiunea persoanelor respective, prin întocmirea unui proces-verbal de predare-primire.

75. Pentru efectuarea inventarierii poate fi instituită, după caz, o comisie formată din cel puțin trei persoane, care dispun de forma de acces la secret de stat corespunzătoare celui mai înalt grad de secretizare a informațiilor care urmează a fi predate-primite.

76. În timpul inventarierii se verifică existența documentelor și a altor purtători materiali de informații atribuite la secret de stat, prin confruntarea cu datele indicate în actele de evidență.

77. În autoritățile publice și alte persoane juridice unde se efectuează controale anuale privind verificarea disponibilului documentelor și altor purtători materiali de informații atribuite la secret de stat, cu perfectarea actelor corespunzătoare, în procesul-verbal de predare-primire se permite a se indica numărul documentelor și altor purtători materiali de informații atribuite la secret de stat pentru fiecare an în parte, iar pentru perioada care a expirat de la ultimul control anual se indică numărul documentelor și altor purtători materiali de informații atribuite la secret de stat transmise și primite, în conformitate cu toate tipurile de evidență. Când lipsesc actele controlului anual pe o anumită perioadă, în procesul-verbal de primire-predare se reflectă pentru fiecare an în parte numărul documentelor și altor purtători materiali de informații atribuite la secret de stat luate în evidență și a celor existente, în conformitate cu toate tipurile de evidență.

78. În procesul-verbal de predare-primire se indică, de asemenea, încălcările de regim depistate, alte date cu privire la starea de lucruri a Subdiviziunii de protecție. Eventualele obiecții și explicații se anexează la procesul-verbal de predare-primire.

79. Despre constatarea lipsei unor documente sau altor purtători materiali de informații atribuite la

secret de stat se informează neîntârziat conducătorul autorității sau al altei persoane juridice, iar acesta din urmă va informa, după caz, Subdiviziunea de protecție a instituției ierarhic superioare și/sau Serviciul de Informații și Securitate.

80. Procesul-verbal trebuie să fie semnat de persoana care predă documentele și alți purtători materiali de informații atribuite la secret de stat, persoana care le primește, după caz, membrii comisiei de predare-primire, și va fi aprobat de conducătorul autorității publice sau al altei persoane juridice.

81. În cazul absenței temporare a șefului Subdiviziunii de protecție (concediu, delegare, caz de boală), se întocmește un proces-verbal de predare-primire a documentelor și altor purtători materiali de informații atribuite la secret de stat necesare în lucru. Procesul-verbal se semnează de către șeful Subdiviziunii de protecție, după caz, conducătorul autorității publice sau al altei persoane juridice și persoana numită pentru îndeplinirea obligațiilor acestuia, care dispune de forma corespunzătoare de acces la secret de stat. Persoana numită pentru îndeplinirea obligațiilor șefului Subdiviziunii de protecție nu poartă răspundere pentru documentele și alți purtători materiali de informații atribuite la secret de stat care se păstrează în safeuri, dulapuri de metal, depozite, alți suportți speciali, dacă integritatea amprentelor ștampilelor pe acestea este păstrată.

82. Subdiviziunea de protecție are următoarele sarcini de bază:

- 1) preîntâmpinarea accesului neîntemeiat la informațiile atribuite la secret de stat;
- 2) descoperirea și lichidarea surselor de divulgare a informațiilor atribuite la secret de stat în procesul de activitate a autorităților publice și altor persoane juridice;
- 3) asigurarea regimului secret în procesul efectuării tuturor lucrărilor secrete de către autoritățile publice și alte persoane juridice;
- 4) organizarea lucrărilor de secretariat secrete.

83. Subdiviziunea de protecție are următoarele atribuții generale:

- 1) elaborează și propune spre aprobare conducerii autorității publice sau a altei persoane juridice actele normative interne cu privire la protecția informațiilor atribuite la secret de stat, monitorizează aplicarea normelor în vigoare de protecție a secretului de stat;
- 2) participă la elaborarea nomenclatoarelor departamentale/ interdepartamentale detaliate de informații care urmează a fi secretizate și a altor acte normative ce reglementează modul departamental de asigurare a regimului secret;
- 3) elaborează, în comun cu șefii subdiviziunilor interioare, Nomenclatorul funcțiilor care necesită acces la secretul de stat;
- 4) coordonează activitatea de protecție a informațiilor atribuite la secret de stat și efectuează controlul asupra îndeplinirii cerințelor în vigoare cu privire la asigurarea regimului secret, inclusiv în procesul lucrărilor de secretariat, analizează aspectele activității autorității publice sau al altei persoane juridice în vederea preîntâmpinării, depistării și lichidării încălcării normelor de protecție a secretului de stat;
- 5) întocmește Programul de prevenire a scurgerii de informații atribuite la secret de stat și îl supune avizării Serviciului de Informații și Securitate, iar după aprobare, acționează pentru aplicarea acestuia;
- 6) informează Serviciul de Informații și Securitate despre cazurile de divulgare a informațiilor secrete, precum și despre dispariția documentelor și altor purtători materiali de informații secrete;
- 7) participă din oficiu la efectuarea investigațiilor privind faptele de încălcare a regimului secret;
- 8) asigură colaborarea cu alte instituții referitor la protecția secretului de stat;
- 9) consiliază conducerea autorității publice sau a altei persoane juridice în legătură cu toate aspectele ce țin de protecția secretului de stat;
- 10) informează conducerea autorității publice sau al altei persoane juridice despre vulnerabilitățile și riscurile existente în sistemul de protecție a informațiilor atribuite la secret de stat și propune măsuri pentru înlăturarea acestora;
- 11) acordă sprijin Serviciului de Informații și Securitate privind verificarea cetățenilor care necesită perfectarea (reperfectarea) dreptului de acces la secret de stat;
- 12) organizează activități de instruire specifică a personalului autorităților publice sau altor persoane juridice care au acces la secret de stat;

13) ține evidența persoanelor pentru care a fost perfectat (reperfectat) dreptul de acces la secret de stat, asigură păstrarea autorizațiilor de acces și a certificatului de securitate eliberat persoanei juridice;

14) ține evidența safeurilor, dulapurilor de metal, depozitelor speciale și altor încăperi în care se permite păstrarea documentelor și altor purtători materiali de informații secrete;

15) exercită alte atribuții în domeniul protecției secretului de stat, potrivit [Legii](#) și prezentului Regulament.

84. Atribuțiile personalului din Subdiviziunea de protecție se stabilesc prin fișa postului, aprobată de conducătorul autorității publice sau al altei persoane juridice. Se interzice implicarea personalului din Subdiviziunea de protecție în executarea altor obligații ce nu decurg din prevederile prezentului Regulament.

85. Pregătirea profesională a angajaților Subdiviziunilor de protecție în domeniul asigurării regimului secret se asigură de către autoritățile publice sau persoanele juridice respective.

Capitolul II

DREPTUL DE ACCES LA SECRETUL DE STAT

Secțiunea 1

Accesul cetățenilor la secretul de stat

86. Accesul la secretul de stat este permis cu respectarea principiului necesității de a lucra cu informații atribuite la secret de stat numai cetățenilor care dețin autorizație de acces la secretul de stat, valabilă pentru gradul de secretizare a informațiilor necesare activității efectuate.

87. Accesul cetățenilor la secretul de stat se perfectează (reperfectează) benevol în condițiile stabilite de [Lege](#) și prezentul Regulament și este permis cetățenilor Republicii Moldova cu capacitate deplină de exercițiu, începînd cu vîrsta de 18 ani, care:

1) și-au exprimat în scris consimțămîntul pentru aplicarea măsurilor de verificare din partea organelor competente;

2) au fost supuși măsurilor de verificare în legătură cu perfectarea dreptului de acces la secretul de stat;

3) și-au asumat în scris obligația privind păstrarea secretului de stat care le va fi încredințat;

4) și-au exprimat în scris acordul pentru limitarea drepturilor lor în legătură cu accesul la secretul de stat;

5) au fost familiarizați, contra semnătură, cu normele ce prevăd răspunderea pentru încălcarea legislației privind secretul de stat.

88. Dreptul de acces la secretul de stat se acordă prin ordin sau dispoziție scrisă:

1) de către conducătorul autorității publice sau al altei persoane juridice în care persoana lucrează, își îndeplinește serviciul sau studiază;

2) de către persoana cu funcții de răspundere care numește în funcție conducătorul autorității publice sau al altei persoane juridice;

3) de către conducătorul autorității publice sau al altei persoane juridice care este beneficiară a lucrărilor legate de secretul de stat, în cazul în care autoritatea publică sau persoana juridică nu este subordonată altei autorități publice sau al altei persoane juridice ori nu intră în domeniul lor de administrare;

4) de către conducătorul autorității publice sau al altei persoane juridice unde se desfășoară activitatea legată de secretul de stat, dacă solicitarea persoanei de a dispune de informații atribuite la secret de stat nu este legată de locul său de muncă, de serviciu sau de studii.

89. La perfectarea dreptului de acces la secretul de stat se va decide asupra compensației care urmează a fi acordată persoanei în legătură cu îndeplinirea permanentă a lucrărilor ce prevăd accesul la secretul de stat, în mărimea și modul stabilit de Guvern.

90. Perfectarea dreptului de acces la secretul de stat, suspendarea și încetarea acestuia pentru titularii funcțiilor prevăzute în anexa nr.1 la Lege este reglementată de articolul 28 alineatele (1) și (2) din Lege.

[Pct.90 în redacția Hot.Guv. nr.770 din 13.11.2024, în vigoare 14.11.2024]

[Pct.90 completat prin [Hot.Guv. nr.886 din 22.10.2014](#), în vigoare 31.10.2014]

91. Accesul cetățenilor străini și al apatrizilor la secretul de stat se acordă în cazuri excepționale, în condițiile stabilite de articolul 28 alineatul (4) din [Lege](#).

92. În funcție de gradul de secretizare a informațiilor, sînt stabilite următoarele forme de acces la secretul de stat:

1) forma 1 – pentru lucrul cu informații atribuite la secret de stat avînd gradele de secretizare “Strict secret”, “Secret”, “Confidențial” și “Restricționat”;

2) forma 2 – pentru lucrul cu informații atribuite la secret de stat avînd gradele de secretizare “Secret”, “Confidențial” și “Restricționat”;

3) forma 3 – pentru lucrul cu informații atribuite la secret de stat avînd gradul de secretizare “Confidențial” și “Restricționat”;

4) forma 4 – pentru lucrul cu informații atribuite la secret de stat avînd gradul de secretizare “Restricționat”.

93. Dreptul de acces la secretul de stat se perfectează pentru următoarele termene:

1) forma 1 – 5 ani;

2) forma 2 – 7 ani;

3) forma 3 – 9 ani;

4) forma 4 – 12 ani.

94. Durata dreptului de acces la secretul de stat nu poate depăși durata atribuțiilor care au servit drept temei pentru acordarea acestuia.

95. Numărul persoanelor cărora urmează să li se perfecteze dreptul de acces la informațiile atribuite la secret de stat trebuie să fie strict determinat în funcție de necesitatea utilizării unor astfel de informații în procesul activității desfășurate și se va stabili în Nomenclatorul funcțiilor care necesită acces la secretul de stat (în continuare – Nomenclatorul funcțiilor), aprobat de către conducătorul autorității publice sau al altei persoane juridice (forma nr.1, anexă la prezentul Regulament) și avizat de către Serviciul de Informații și Securitate. Orice modificare/completare ce se operează în Nomenclatorul funcțiilor se avizează de către Serviciul de Informații și Securitate.

96. Nomenclatorul funcțiilor se reexaminează cel puțin o dată la 5 ani pentru a verifica dacă funcțiile aprobate corespund formei de acces indicate și principiului necesității de a lucra cu informații atribuite la secret de stat. Dacă se va constata că Nomenclatorul funcțiilor nu mai corespunde cerințelor existente, se va întocmi unul nou. La prezentarea acestuia spre avizare Serviciului de Informații și Securitate, autoritatea publică sau altă persoană juridică va indica în scrisoarea de însoțire cînd a fost avizat precedentul Nomenclator al funcțiilor, numărul de persoane și forma de acces prevăzută pentru funcțiile respective. Dacă numărul funcțiilor/persoanelor din Nomenclator se majorează, se va indica motivul majorării.

97. Materialele referitoare la cetățenii care necesită perfectarea (reperfectarea) dreptului de acces la secretul de stat se pregătesc de către subdiviziunea resurse umane, iar acolo unde aceasta lipsește – de către persoana responsabilă de lucrul cu personalul.

98. În scopul perfectării dreptului de acces la secretul de stat, cetățenii Republicii Moldova completează Chestionarul de bază (forma nr.2, anexă la prezentul Regulament) și prezintă 2 fotografii color de mărimea 4,5 x 6 cm. Pentru perfectarea dreptului de acces la informațiile cu gradul de secretizare “Strict secret” și “Secret”, concomitent cu Chestionarul de bază se completează un Chestionar suplimentar (forma nr.3, anexă la prezentul Regulament). Toate datele indicate de către cetățean trebuie să fie autentice.

99. Cetățenii care necesită perfectarea dreptului de acces la secretul de stat își manifestă în prealabil acordul scris cu privire la aplicarea măsurilor de verificare din partea organelor competente.

100. Subdiviziunea resurse umane sau persoana responsabilă de lucrul cu personalul în procesul pregătirii materialelor referitoare la cetățenii care necesită perfectarea dreptului de acces la secretul de stat confruntă informația indicată în Chestionarul de bază (suplimentar) cu datele din actele

corespunzătoare (buletin de identitate, livret militar, alte acte), concretizează dacă cetățeanul a avut anterior acces la secretul de stat, care formă de acces i-a fost perfectată, alte aspecte necesare perfectării dreptului de acces.

101. Orice modificare ulterioară a datelor indicate în Chestionarul de bază (suplimentar) se va comunica neîntârziat subdiviziunii resurse umane sau persoanei responsabile de lucrul cu personalul.

102. Subdiviziunea resurse umane sau persoana responsabilă de lucrul cu personalul vizează și prezintă Subdiviziunii de protecție materialele referitoare la perfectarea dreptului de acces la secretul de stat.

103. Subdiviziunea de protecție din cadrul autorității publice sau al altei persoane juridice care perfectează dreptul de acces la secretul de stat verifică prezența sau lipsa circumstanțelor prevăzute în articolul 25 alineatul (1) literele a), d), e) și h) din [Lege](#). În acest sens, se solicită actele confirmative necesare, inclusiv certificatul care atestă prezența sau lipsa contraindicațiilor medicale pentru lucrul cu informațiile atribuite la secret de stat, stabilite de Nomenclatorul aprobat prin ordin al ministrului sănătății.

[Pct.103 modificat prin Hot.Guv. nr.770 din 13.11.2024, în vigoare 14.11.2024]

104. Pentru aplicarea măsurilor de verificare, autoritatea publică sau altă persoană juridică va înainta Serviciului de Informații și Securitate o solicitare motivată (forma nr.5, anexă la prezentul Regulament), în scopul inițierii măsurilor de verificare privind existența sau lipsa circumstanțelor prevăzute în articolul 25 alineatul (1) literele b), c), f), g), i), j) și k) din [Lege](#). Solicitarea va fi însoțită de Chestionarul de bază, după caz, Chestionarul suplimentar și Lista rudelor și persoanelor apropiate, întocmit potrivit modelului din forma nr.6, anexă la prezentul Regulament, care include: tata, mama, frații, surorile, copiii care au împlinit vârsta de 16 ani, soția (soțul), fosta soție (fostul soț), concubinul (concubina), cumnații (cumnatele), ce se completează și se introduc în plic separat și sigilat. La prima poziție din Lista rudelor și persoanelor apropiate, se indică angajatul supus măsurilor de verificare.

105. Procedura de verificare în vederea acordării accesului la secretul de stat are drept scop identificarea riscurilor de securitate, aferente gestionării informațiilor secrete de stat.

106. Măsurile de verificare urmează a fi efectuate de către Serviciul de Informații și Securitate în termen de o lună de la data primirii solicitării autorității publice sau al altei persoane juridice, numărul acestora fiind direct proporțional gradului de secretizare a informațiilor la care va avea acces persoana.

107. Ori de câte ori apar indicii că titularul autorizației de acces la secretul de stat nu mai îndeplinește criteriile de compatibilitate privind accesul la informațiile atribuite la secret de stat, măsurile de verificare se reiau la solicitarea conducătorului autorității publice sau al altei persoane juridice.

108. În baza rezultatelor măsurilor de verificare, Serviciul de Informații și Securitate formulează concluzia cu privire la posibilitatea sau imposibilitatea de a acorda cetățeanului dreptul de acces la secretul de stat (forma nr.7, anexă la prezentul Regulament), care se perfectează în 2 exemplare, unul dintre care se remite solicitantului, iar celălalt se păstrează la Serviciul de Informații și Securitate.

109. Concluzia cu privire la imposibilitatea acordării dreptului de acces la secretul de stat trebuie să conțină temeiul corespunzător prevăzut în articolul 25 alineatul (1) din [Lege](#) și rezumatul motivelor de fapt care au servit drept temei pentru refuzul de a acorda dreptul de acces la secretul de stat, în măsura în care acest lucru este compatibil cu păstrarea confidențialității datelor obținute. Aceasta este executorie pentru persoanele cu funcții de răspundere împuternicite să adopte decizia privind acordarea dreptului de acces la secretul de stat, însă nu exclude posibilitatea înaintării unei solicitări repetate după înlăturarea circumstanțelor care fac imposibilă acordarea dreptului de acces la secretul de stat.

[Pct.109 modificat prin Hot.Guv. nr.770 din 13.11.2024, în vigoare 14.11.2024]

110. În termen de 5 zile de la primirea concluziei Serviciului de Informații și Securitate, conducătorul autorității publice sau al altei persoane juridice va adopta decizia cu privire la acordarea dreptului de acces la secretul de stat și va elibera autorizația de acces de forma corespunzătoare (forma nr.8, anexă la prezentul Regulament) sau va refuza acordarea dreptului de acces la secretul de stat.

111. Imediat după primirea concluziei pozitive a Serviciului de Informații și Securitate și pînă la adoptarea deciziei cu privire la acordarea dreptului de acces la secretul de stat, cetățeanul este

familiarizat, contra semnătură, de către Subdiviziunea de protecție cu dispozițiile legale privind protecția secretului de stat și limitarea unor drepturi ale acestuia în legătură cu accesul la secretul de stat, precum și cu normele ce prevăd răspunderea pentru încălcarea legislației cu privire la secretul de stat și semnează angajamentul de confidențialitate (forma nr.4, anexă la prezentul Regulament).

112. În decizia cu privire la acordarea dreptului de acces la secretul de stat se va indica: forma de acces la secretul de stat, termenul pentru care se perfectează, numele, prenumele, funcția cetățeanului căruia, se acordă dreptul de acces la secretul de stat, cuantumul compensației stabilite în legătură cu îndeplinirea lucrărilor ce prevăd accesul la secretul de stat.

113. Decizia privind refuzul de acordare a dreptului de acces la secretul de stat se adoptă în temeiul prevederilor articolului 25 din [Lege](#), se comunică în scris solicitantului și poate fi contestată în conformitate cu prevederile [Codului administrativ al Republicii Moldova nr.116/2018](#).

[Pct.113 modificat prin Hot.Guv. nr.770 din 13.11.2024, în vigoare 14.11.2024]

114. Pentru confirmarea dreptului de acces la secretul de stat în raport cu terții, Subdiviziunea de protecție eliberează cetățeanului, în temeiul dispoziției conducătorului autorității publice sau al altei persoane juridice, un certificat de acces la secretul de stat de forma corespunzătoare (forma nr.9, anexă la prezentul Regulament), în care se indică activitatea (delegație, însărcinare) ce implică accesul la informații secretizate, pe care acesta urmează să o îndeplinească. Certificatul se restituie Subdiviziunii de protecție imediat ce a fost îndeplinită activitatea pentru care a fost eliberat. Evidența certificatelor respective se asigură potrivit Registrului de evidență a certificatelor de acces la secretul de stat (forma nr.10, anexă la prezentul Regulament).

115. Șeful Subdiviziunii de protecție va asigura evidența strictă a tuturor cetățenilor cărora le-a fost perfectat dreptul de acces la secretul de stat și a autorizațiilor de acces eliberate în Registrul de evidență privind accesul la secret de stat (forma nr.11, anexă la prezentul Regulament). În cazul în care, potrivit legislației în vigoare, datele despre identitatea și calitatea cetățenilor nu pot fi divulgate, evidența acestora se va ține într-un registru separat.

116. Despre eliberarea autorizației de acces la secretul de stat se informează Serviciul de Informații și Securitate (forma nr.12, anexă la prezentul Regulament) în termen de 10 zile lucrătoare.

[Pct.116 în redacția Hot.Guv. nr.770 din 13.11.2024, în vigoare 14.11.2024]

117. În cazuri excepționale, determinate de situații de criză, calamități sau evenimente imprevizibile, conducătorul autorității publice sau al altei persoane juridice poate acorda acces temporar la informațiile atribuite la secret de stat anumitor cetățeni care nu dețin autorizație de acces, cu condiția asigurării unui sistem corespunzător de evidență.

118. Cetățenii care primesc dreptul de acces temporar la informațiile atribuite la secret de stat vor semna angajamentul de confidențialitate, iar informația despre aceștia va fi comunicată Serviciului de Informații și Securitate, în cel mai scurt timp posibil, pentru efectuarea măsurilor de verificare, conform procedurii stabilite.

119. În cazul informațiilor "Strict secrete" și "Secrete", accesul temporar va fi acordat, pe cât posibil, cetățenilor care au deja acces la informațiile atribuite la un anumit grad de secretizare.

120. Pentru personalul Serviciului de Informații și Securitate, procedura de verificare, perfectare (reperfectare) a dreptului de acces la secret de stat și de evidență a autorizațiilor de acces se reglementează prin acte normative interne.

121. Cetățenii care au acces la secretul de stat vor respecta cu strictețe obligațiile privind păstrarea secretului de stat, stabilite în articolul 29 din [Lege](#). Ei vor fi instruiți, obligatoriu, cu privire la protecția informațiilor atribuite la secret de stat, înainte începerii activității, iar ulterior, la intervale prestabilite și ori de câte ori este nevoie.

122. Instruirea personalului se realizează de către Subdiviziunea de protecție și urmărește însușirea corectă a cerințelor de securitate și a modului de implementare eficientă a măsurilor de protecție a informațiilor atribuite la secret de stat.

123. Activitatea de instruire se efectuează planificat, în scopul prevenirii, contracarării și eliminării

riscurilor și amenințărilor la adresa securității informațiilor atribuite la secret de stat.

124. Instruirea personalului se realizează diferențiat, potrivit gradului de secretizare a informațiilor la care autorizația de acces permite accesul și va fi înscrisă de către Subdiviziunea de protecție în Fișa individuală de instruire (forma nr.14, anexă la prezentul Regulament).

125. După fiecare instruire, cetățeanul care deține autorizație de acces va semna că a luat act de conținutul reglementărilor privind protecția informațiilor atribuite la secret de stat.

126. Organizarea și coordonarea activității de instruire a Subdiviziunilor de protecție se va asigura de către Serviciul de Informații și Securitate.

127. Reperfectarea dreptului de acces la secretul de stat se efectuează cu respectarea condițiilor necesare perfectării dreptului de acces la secretul de stat, în cazurile:

1) expirării termenului pentru care a fost perfectat acest drept, dacă este necesar să se lucreze în continuare cu informații atribuite la secret de stat;

2) perfectării unei alte forme de acces la secret de stat în legătură cu necesitatea de a lucra cu informații atribuite la secret de stat cu un grad mai înalt de secretizare.

128. Pentru reperfectarea dreptului de acces la secretul de stat, măsurile de verificare se raportează la perioada scursă de la eliberarea autorizației de acces anterioare.

129. Dacă există necesitatea să se lucreze în continuare cu informații atribuite la secret de stat de același grad de secretizare, eliberarea unei noi autorizații de acces la secretul de stat nu se efectuează la reperfectarea dreptului de acces în legătură cu expirarea termenului pentru care a fost perfectat acest drept. În acest caz, pe autorizația de acces la secretul de stat anterioară se va aplica mențiunea privind prelungirea termenului de valabilitate, cu indicarea termenului nou.

130. Mențiunea privind prelungirea termenului de valabilitate poate fi aplicată pe autorizația de acces la secretul de stat până la expirarea termenului anterior de valabilitate al acesteia. În această situație, termenul nou de valabilitate al autorizației de acces va începe din ultima zi calendaristică în care a expirat termenul anterior de valabilitate al ei.

131. Dreptul de acces la secretul de stat se suspendă sau încetează în conformitate cu prevederile articolului 27 din [Lege](#), la decizia persoanei cu funcții de răspundere împuternicită să adopte decizia cu privire la acordarea acestui drept.

132. Termenul pentru care a fost suspendat dreptul de acces la secretul de stat nu prelungeste termenul de valabilitate al autorizației de acces la secretul de stat.

133. În cazul în care se constată existența temeiurilor de încetare a dreptului de acces la secretul de stat, autorizația de acces își încetează valabilitatea și se distruge în baza unui proces-verbal.

134. Faptul suspendării, încetării valabilității, distrugerii autorizației de acces se consemnează în Registrul de evidență privind accesul la secretul de stat.

135. Despre prelungirea termenului de valabilitate, suspendarea sau încetarea valabilității autorizației de acces la secretul de stat se comunică Serviciului de Informații și Securitate în termen de 10 zile lucrătoare de la data emiterii ordinului sau deciziei, în modul stabilit în forma nr.12, anexă la prezentul Regulament.

[Pct.135 modificat prin Hot.Guv. nr.770 din 13.11.2024, în vigoare 14.11.2024]

Secțiunea a 2-a

Accesul persoanelor juridice la secretul de stat

136. Dreptul de acces la secretul de stat se acordă persoanelor juridice, cu excepția autorităților publice care desfășoară activități ce țin de utilizarea informațiilor atribuite la secret de stat, crearea mijloacelor de protejare a informației, realizarea măsurilor și/sau prestarea serviciilor de protecție a secretului de stat, în baza certificatului de securitate eliberat de Comisia interdepartamentală pentru protecția secretului de stat (în continuare – Comisia interdepartamentală), în modul stabilit de [Lege](#) și prezentul Regulament.

137. Comisia interdepartamentală eliberează certificatul de securitate doar după efectuarea unei expertize speciale a persoanei juridice privind existența condițiilor pentru desfășurarea activității legate de secretul de stat și atestării conducătorului acesteia. La eliberarea certificatului de securitate,

persoanele juridice trebuie să posede un Program de prevenire a scurgerii de informații atribuite la secret de stat, avizat conform reglementărilor în vigoare.

138. Pentru obținerea certificatului de securitate, persoanele juridice depun la Comisia interdepartamentală o cerere (forma nr.15, anexă la prezentul Regulament), la care anexează formularul completat al Chestionarului de securitate (forma nr.16, anexă la prezentul Regulament), introdus într-un plic separat și sigilat și Programul de prevenire a scurgerii de informații atribuite la secret de stat. Documentele ce confirmă datele indicate în chestionarul de securitate se prezintă în copii legalizate notarial. În caz contrar, copiile vor fi confirmate prin prezentarea originalului.

139. Comisia interdepartamentală va asigura înregistrarea corespunzătoare a tuturor documentelor prezentate de către solicitant pentru obținerea certificatului de securitate.

140. În termen de 5 zile de la primirea cererii, Comisia interdepartamentală va remite formularul completat al chestionarului de securitate și o copie a Programului de prevenire a scurgerii de informații atribuite la secret de stat Serviciului de Informații și Securitate, solicitând efectuarea expertizei speciale a persoanei juridice privind existența condițiilor pentru desfășurarea activității legate de secretul de stat.

141. Expertiza specială se efectuează în termen de până la 2 luni din momentul solicitării și are ca obiectiv verificarea:

1) îndeplinirii cerințelor stabilite de articolul 32 alineatul (3) din [Lege](#), în volumul necesar pentru asigurarea protecției informațiilor utilizate la efectuarea lucrărilor, corespunzător gradului de secretizare a acestora;

2) autenticității și/sau caracterului complet al datelor prezentate de către solicitant.

142. În vederea desfășurării măsurilor de expertizare, persoana juridică are obligația să permită accesul reprezentanților Serviciului de Informații și Securitate în sedii, la echipamente, la activități, respectiv, să prezinte documentele necesare și să furnizeze, la cerere, alte date și informații.

143. Ori de câte ori apar indicii că titularul certificatului de securitate nu mai îndeplinește condițiile necesare pentru desfășurarea activității legate de secretul de stat, măsurile de expertizare se reiau.

144. În baza rezultatelor măsurilor de expertizare, Serviciul de Informații și Securitate formulează concluzia cu privire la îndeplinirea sau neîndeplinirea condițiilor pentru desfășurarea activității legate de secretul de stat (forma nr.17, anexă la prezentul Regulament). Concluzia se întocmește în 2 exemplare, dintre care unul se păstrează la Serviciul de Informații și Securitate, iar altul se remite Comisiei interdepartamentale.

145. Concluzia cu privire la neîndeplinirea condițiilor pentru desfășurarea activității legate de secretul de stat trebuie să conțină temeiul corespunzător expus în articolul 32 alineatul (3) din [Lege](#) și/sau în punctul 141 din prezentul Regulament, care a servit drept bază pentru adoptarea acesteia. Concluzia nu exclude posibilitatea efectuării unei expertize repetate după înlăturarea circumstanțelor care nu corespund cerințelor necesare pentru desfășurarea activității legate de secretul de stat.

146. În vederea eliberării certificatului de securitate, Comisia interdepartamentală, în termen de cel mult 5 zile de la primirea concluziei cu privire la existența condițiilor pentru desfășurarea activității legate de secretul de stat, va organiza și va efectua atestarea conducătorului persoanei juridice.

147. Atestarea constă în aprecierea cunoștințelor conducătorului persoanei juridice în domeniul secretului de stat. Aprecierea se efectuează în baza unui interviu de atestare în cadrul căruia conducătorul persoanei juridice este chestionat cu privire la reglementările în vigoare în domeniul secretului de stat.

148. Ședința Comisiei interdepartamentale ce ține de atestarea conducătorului persoanei juridice se consideră deliberativă dacă la ea sînt prezenți 2/3 din numărul total de membri. Decizia Comisiei interdepartamentale se ia prin vot deschis, cu simpla majoritate de voturi a membrilor Comisiei.

149. Rezultatele atestării se reflectă în Fișa de atestare (forma nr.18, anexă la prezentul Regulament), care se întocmește de către secretarul Comisiei interdepartamentale, se semnează de membrii acesteia și se aduce la cunoștința conducătorului persoanei juridice supus atestării, contra semnătură.

150. În termen de 5 zile de la primirea încheierii de expertiză de la Serviciul de Informații și Securitate sau, după caz, de la atestarea conducătorului persoanei juridice, Comisia interdepartamentală

eliberează persoanei juridice Certificatul de securitate (forma nr.19, anexă la prezentul Regulament) sau refuză eliberarea acestuia.

151. Pentru fiecare gen de activitate, care face obiectul certificatului de securitate, Comisia stabilește condițiile pe care trebuie să le respecte solicitantul.

152. În decizia cu privire la refuzul de eliberare a certificatului de securitate trebuie să fie indicat temeiul respectiv.

153. Eliberarea certificatului de securitate este refuzată în cazul:

1) neîndeplinirii cerințelor stabilite de articolul 32 alineatul (3) din [Lege](#), în volumul necesar pentru asigurarea protecției informațiilor utilizate la efectuarea lucrărilor, corespunzător gradului de secretizare a acestora;

2) prezentării unor date neautentice și/sau incomplete de către solicitant.

154. Evidența certificatelor de securitate eliberate se realizează de către Comisia interdepartamentală, conform Registrului de evidență a certificatelor de securitate (forma nr.20, anexă la prezentul Regulament).

155. Certificatul de securitate eliberat trebuie să conțină:

1) denumirea organului care l-a eliberat;

2) seria, numărul și data eliberării. Seria se formează din ultimele două cifre ale anului în care se eliberează certificatul de securitate, iar numărul corespunde numărului de ordine din Registrul de evidență a certificatelor de securitate;

3) gradul de secretizare a informațiilor la care se permite accesul;

4) denumirea completă a persoanei juridice;

5) sediul persoanei juridice;

6) numărul de identificare de stat;

7) genul (genurile) de activitate pentru care se acordă accesul;

8) condițiile stabilite pentru practicarea genului (genurilor) de activitate;

9) termenul de valabilitate al certificatului de securitate;

10) după caz, date cu privire la prelungirea, suspendarea termenului de valabilitate al certificatului de securitate; date cu privire la modificarea denumirii, sediului persoanei juridice; date cu privire la folosirea serviciilor prestate de către Subdiviziunea de protecție a altei persoane juridice;

11) semnătura președintelui Comisiei interdepartamentale, amprenta ștampilei.

156. Termenul de valabilitate al certificatului de securitate este determinat de perioada de desfășurare a activității legate de secretul de stat, dar nu mai mult de un an.

157. Se interzice transmiterea certificatului de securitate de la o persoană juridică la alta, precum și utilizarea unui singur certificat de securitate de către mai multe persoane juridice.

158. În cazul în care genul de activitate autorizat prin certificatul de securitate se practică în mai multe obiecte (unități) separate teritorial (spre exemplu, filiale, reprezentanțe), solicitantului, odată cu certificatul, i se eliberează copii legalizate ale acestuia cu indicarea adresei fiecărui obiect.

159. Copiile certificatelor de securitate urmează a fi înregistrate în Registrul de evidență a certificatelor de securitate.

160. În cazul în care după eliberarea certificatului de securitate intervin modificări în datele prezentate de către solicitant la eliberarea certificatului, acesta este obligat, în termen de până la 15 zile, să comunice aceste modificări Comisiei interdepartamentale. Concomitent, solicitantul va prezenta Comisiei documentele care confirmă modificările intervenite, certificatul de securitate eliberat, după caz, copiile acestuia, în vederea operării modificărilor de rigoare.

161. Comisia interdepartamentală, în termen de 15 zile, va introduce modificările necesare în certificatul de securitate.

162. Până la restituirea certificatului de securitate solicitantului (inclusiv până la eliberarea noilor copii de pe acesta), persoana juridică va activa în baza unei copii legalizate, eliberate de Comisia interdepartamentală pentru această perioadă. La eliberarea certificatului de securitate cu modificările de rigoare, solicitantul va restitui Comisiei interdepartamentale copia legalizată.

163. Distrugerea certificatului de securitate se interzice, cu excepția cazurilor prevăzute în punctul

173 din prezentul Regulament. Nu se admite pierderea certificatului de securitate. În caz că a intervenit una dintre situațiile menționate, solicitantul comunică acest fapt Comisiei interdepartamentale într-un termen cât mai restrâns, însă nu mai târziu de 3 zile. Pentru termenul de valabilitate rămas al certificatului de securitate se eliberează un duplicat.

164. Dacă există necesitatea de a continua activitatea legată de secretul de stat după expirarea termenului de valabilitate al certificatului de securitate, persoana juridică va solicita prelungirea valabilității acestuia pe termenul prevăzut în punctul 156 din prezentul Regulament.

165. Cererea cu privire la prelungirea termenului de valabilitate al certificatului de securitate se depune la Comisia interdepartamentală cu cel puțin 3 luni înainte de expirarea termenului anterior de valabilitate al certificatului de securitate. La cerere se anexează documentele care confirmă necesitatea prelungirii termenului de valabilitate al certificatului.

166. Prelungirea termenului de valabilitate al certificatului de securitate se efectuează cu respectarea condițiilor necesare eliberării acestuia.

167. Pe certificatul de securitate se va aplica mențiunea privind prelungirea termenului de valabilitate, cu indicarea termenului nou. Mențiunea privind prelungirea termenului de valabilitate poate fi aplicată pe certificatul de securitate pînă la expirarea termenului anterior de valabilitate al acestuia. În acest caz, termenul nou de valabilitate al certificatului de securitate va începe din ultima zi calendaristică în care a expirat termenul anterior de valabilitate al acestuia.

168. Dreptul de acces la secret de stat al persoanelor juridice este suspendat în cazurile în care:

1) împotriva acesteia a fost pornită urmărirea penală pentru săvîrșirea unei infracțiuni incompatibile cu activitatea ce presupune utilizarea informațiilor atribuite la secret de stat, pînă la pronunțarea hotărîrii judecătorești definitive și irevocabile;

2) este necesară efectuarea unei expertize suplimentare în legătură cu posibila apariție a circumstanțelor care nu corespund condițiilor prevăzute în punctul 141 din prezentul Regulament, pînă la terminarea măsurilor de expertiză, dar nu mai mult de 30 de zile;

3) suspendarea activității persoanei juridice, pe un termen ce nu va depăși termenul de valabilitate al certificatului de securitate.

169. Decizia cu privire la suspendarea dreptului de acces la secretul de stat al persoanei juridice se comunică acesteia în termen de 10 zile din data emiterii.

170. Pe perioada suspendării, certificatul de securitate, după caz, copiile legalizate de pe acesta și duplicatul se retrag de către Comisia interdepartamentală. La expirarea termenului de suspendare, certificatul de securitate se restituie persoanei juridice sau se distruge în baza unui proces-verbal.

171. Dreptul de acces la secretul de stat al persoanelor juridice încetează în cazurile:

1) apariției sau descoperirii circumstanțelor care nu corespund cerințelor stabilite în articolul 32 alineatul (3) din [Lege](#);

2) depistării unor date neautentice și/sau incomplete la eliberarea certificatului de securitate;

3) expirării termenului pentru care a fost perfectat, dacă nu a fost solicitată prelungirea acestuia;

4) suspendării activității persoanei juridice pe un termen ce depășește termenul de valabilitate al certificatului de securitate;

5) încălcării, chiar și o singură dată, a obligațiilor asumate ce țin de protecția secretului de stat;

6) dizolvării persoanei juridice.

172. Decizia cu privire la încetarea dreptului de acces la secretul de stat al persoanei juridice se comunică acesteia în termen de 10 zile din data emiterii.

173. La încetarea dreptului de acces la secretul de stat al persoanei juridice, certificatul de securitate se retrage de către Comisia interdepartamentală și se distruge în baza unui proces-verbal.

174. Faptul suspendării, încetării, distrugerii certificatului de securitate se consemnează în Registrul de evidență a certificatelor de securitate.

Capitolul III

REGULI DE GESTIONARE A PURTĂTORILOR MATERIALI DE INFORMAȚII ATRIBUITE LA SECRET DE STAT

Secțiunea 1

Cerințe generale cu privire la purtătorii materiali de informații atribuite la secret de stat

175. Orice tip de purtători materiali de informații atribuite la secret de stat trebuie să fie identificat printr-un anumit număr de componente, amplasate conform cerințelor prezentului Regulament.

176. Documentele și alți purtători materiali de informații atribuite la secret de stat trebuie să conțină:

- 1) parafa de secretizare;
- 2) numărul de înregistrare;
- 3) data de înregistrare și termenul de secretizare a informațiilor;
- 4) funcția, numele, prenumele și semnătura persoanei cu funcție de răspundere care a secretizat informațiile.

177. Pe toate documentele ce conțin informații atribuite la secret de stat se aplică în mod obligatoriu parafa de secretizare. Parafa de secretizare se aplică pe toate exemplarele documentului, în partea dreaptă superioară a fiecărei file.

178. Atunci când documentul urmează să fie distribuit în mai multe exemplare, fiecare dintre acestea va purta numărul de exemplare, care apare pe prima pagină, sub parafa de secretizare, împreună cu numărul total de file.

179. Pe documentele care sînt adresate unei anumite persoane se aplică suplimentar, sub parafa de secretizare, mențiunea "Personal", iar cele ce se referă la mobilizare, se marchează cu litera "M".

180. Fiecărui document i se atribuie un număr de înregistrare care se înscrie pe toate exemplarele documentului și pe anexele acestora. Numărul de înregistrare este urmat de mențiunile: "SS" – pentru informațiile avînd gradul de secretizare "Strict secret", "S" – pentru informațiile avînd gradul de secretizare "Secret", "C" – pentru informațiile avînd gradul de secretizare "Confidențial" și "R" – pentru informațiile avînd gradul de secretizare "Restricționat".

181. La înscrierea numărului de înregistrare se va indica în mod obligatoriu data.

182. Termenul de secretizare a informațiilor începe de la data la care pe document a fost aplicată parafa de secretizare.

183. Fiecare filă a documentului trebuie să fie numerotată, avînd înscris numărul curent al paginii, urmat de numărul total al acestora. Filele fiecărei anexe la document vor fi numerotate separat.

184. La sfîrșitul documentului se indică funcția, numele, prenumele persoanei cu funcție de răspundere care a secretizat informațiile, cu aplicarea semnăturii acesteia, precum și numele, prenumele, semnătura celui care a întocmit documentul.

185. Cînd documentele ce conțin informații atribuite la secret de stat se semnează de o singură persoană, datele privind funcția, numele și prenumele acesteia se înscriu sub text, în centrul paginii.

186. Dacă documentele se semnează de două sau mai multe persoane, funcția, numele și prenumele conducătorului autorității publice sau al altei persoane juridice se înscriu în partea stîngă, iar ale celorlalți semnatari – în partea dreaptă, în ordinea corespunzătoare funcțiilor.

187. Cînd documentele care conțin informații atribuite la secret de stat se emit în comun de două sau mai multe autorități publice sau alte persoane juridice, denumirile acestora se înscriu separat în antet, iar la sfîrșit se semnează de către conducătorii autorităților publice sau persoanelor juridice respective, de la stînga la dreapta, aplicîndu-se ștampilele corespunzătoare.

188. Pe documente se menționează, după caz, destinatarul. Pentru documentul care urmează să fie expediat la cinci și mai mulți destinatari se întocmește o listă de expediere, aprobată de către persoana cu funcție de răspundere care a secretizat și a semnat documentul. În acest caz, pe fiecare exemplar se indică un singur destinatar. Lista de expediere se coordonează cu Subdiviziunea de protecție.

189. Documentul destinat unei alte autorități publice sau al altei persoane juridice se va întocmi pe foaie cu antet.

190. Exemplarul documentului de ieșire, care rămîne în dosar, poate să nu fie întocmit pe foaie cu

antet, însă acesta trebuie să conțină celelalte elemente necesare, inclusiv numărul de înregistrare, data și mențiunea cu privire la funcția, numele, prenumele persoanei cu funcție de răspundere care a secretizat și a semnat documentul, confirmată prin semnătura executantului.

191. În situația în care documentul de bază este însoțit de anexe, la sfârșitul textului se indică, pentru fiecare anexă: numărul anexe, denumirea (dacă denumirea anexe este indicată în textul documentului, atunci în anexă denumirea nu se indică), numărul de înregistrare, numărul de file al acesteia și gradul de secretizare. La expedierea documentelor prin scrisoare de însoțire, se va indica suplimentar numărul de exemplare anexate și numărul total de file.

192. În cazurile în care există un număr mare de anexe, se poate face inventarierea lor cu indicarea elementelor necesare ale documentelor incluse în anexă, iar în scrisoarea de însoțire se scrie: *“Anexă conform inventarului nr. _____ pe _____ file”*.

193. Anexele se secretizează în funcție de conținutul lor, și nu de cel al documentelor pe care le însoțesc.

194. Scrisoarea de însoțire a documentului nu va cuprinde informații detaliate referitoare la conținutul documentelor anexate.

195. Documentele anexate se semnează, dacă este cazul, de persoanele care au semnat documentul inițial.

196. Întocmirea documentelor ce conțin informații atribuite la secret se stat, respectiv, multiplicarea acestora, se face într-un număr strict limitat de exemplare.

197. Informațiile atribuite la secret de stat vor fi marcate, inscripționate și gestionate numai de către persoanele care au autorizație de acces la secretul de stat de forma corespunzătoare.

198. Parafa de secretizare se aplică prin ștampilare, dactilografiere, tipărire sau olograf.

199. Porțiunile clar identificabile din documentele complexe secretizate, cum sînt secțiunile, capitolele, titlurile, anexele, paragrafele, alte părți componente, care au grade diferite de secretizare sau care nu sînt secretizate, trebuie marcate corespunzător gradului de secretizare.

200. Parafa de secretizare va fi aplicată separat de celelalte mențiuni, cu caractere și/sau culori diferite.

201. Toate documentele secretizate aflate în lucru sau în stadiu de proiect vor avea înscrisă mențiunea “Proiect” și vor fi marcate potrivit gradului de secretizare a informațiilor ce le conțin. Gestionarea documentelor secretizate, aflate în lucru sau în stadiu de proiect, se face în aceleași condiții ca și ale celor în formă definitivă.

202. Atunci cînd se utilizează documente secretizate pentru întocmirea unui alt document, mențiunile de pe documentele secretizate le vor determina pe cele ale documentului rezultat. Pe documentul rezultat se vor preciza, după caz, documentele sursă care au stat la baza întocmirii lui.

203. Numărul și data inițială de înregistrare a documentului secretizat trebuie păstrate, chiar dacă i se aduc amendamente, pînă cînd documentul respectiv va face obiectul revizuirii gradului de secretizare.

204. În cazul în care mențiunile nu pot fi aplicate nemijlocit pe purtătorul material de informații atribuite la secret de stat, ele se indică în documentația de însoțire a acestuia.

205. Fotografiile, filmele, microfilmele și negativele lor, rolele, bobinele, containerele sau alți suportți de păstrare a acestora se marchează vizibil cu o etichetă care indică parafa de secretizare, numărul și data înregistrării.

206. Microfilmele trebuie să aibă afișat, la cele două capete, parafa de secretizare, iar la începutul rolei – lista elementelor de conținut.

207. Gradul de secretizare a informațiilor înregistrate pe benzi audio se imprimă verbal, atît la începutul înregistrării, cît și la sfârșitul acesteia.

208. Marcarea gradului de secretizare pe benzi video trebuie să asigure afișarea pe ecran a parafei de secretizare. În cazul în care, înainte de înregistrarea benzilor, nu se poate stabili cu exactitate gradul de secretizare, parafa se aplică prin inserarea unui segment de bandă la începutul și la sfârșitul benzii video.

209. Benzile audio și video care conțin informații atribuite la secret de stat păstrează gradul de secretizare cel mai înalt atribuit pînă în momentul:

1) distrugerii printr-un procedeu autorizat;

2) atribuirii unui grad mai înalt de secretizare prin adăugarea unei înregistrări cu grad superior de secretizare.

210. Proiecțiile de imagini trebuie să afișeze, la începutul și la sfârșitul acestora, numărul și data înregistrării, precum și parafa de secretizare.

211. Rolele, bobinele, containerele sau alți suportți de păstrare a benzilor magnetice, inclusiv cele video, pe care au fost imprimate informații atribuite la secret de stat, vor avea înscris, la loc vizibil, cea mai înaltă parafă de secretizare atribuită acestora, care va rămîne aplicată pînă la distrugerea sau demagnetizarea lor.

212. La efectuarea unei înregistrări pe bandă magnetică, atît la începutul, cît și la sfârșitul fiecărui pasaj, se va menționa gradul de secretizare. În cazul detașării de pe suportul fizic, fiecare capăt al benzii va fi marcat, la loc vizibil, cu parafa de secretizare.

213. În toate cazurile, ambalajele sau suportții în care se păstrează documente sau materiale ce conțin informații atribuite la secret de stat vor avea marcată parafa de secretizare, numărul și data înregistrării și li se va atașa o listă cu denumirea acestora.

Secțiunea a 2-a

Evidența și circulația documentelor secrete

214. Conducătorii autorităților publice sau altor persoane juridice vor asigura măsurile necesare de evidență și control a informațiilor secretizate, astfel încît să se poată stabili, în orice moment, locul în care se află aceste informații.

215. Lucrările de secretariat secrete în cadrul autorităților publice sau altor persoane juridice se organizează și se efectuează de către Subdiviziunile de protecție (subdiviziunile lucrărilor de secretariat secrete).

216. În cadrul Subdiviziunilor de protecție trebuie să fie create condițiile necesare pentru lucrul cu informații atribuite la secret de stat, conform cerințelor prezentului Regulament.

217. Evidența documentelor (de intrare, de ieșire, interne) și a altor purtători materiali de informații atribuite la secret de stat se ține, conform registrelor de evidență, în formă manuală și/sau electronică.

218. Ținerea manuală a registrelor poate fi efectuată sub formă de fișier sau prin introducerea mențiunilor în cartea pentru înregistrări.

219. Drept principiu de bază al evidenței se consideră atribuirea fiecărui document de intrare și de ieșire a unui singur număr de înregistrare. La evidența pe fișe, pentru fiecare document se întocmește o singură fișă de evidență, într-un număr necesar de exemplare.

220. În autoritățile publice sau alte persoane juridice unde există un număr neînsemnat de documente de intrare, de ieșire și interne (pînă la 500 pe an), se permite evidența lor conform Registrului de evidență a documentelor de intrare, de ieșire și a celor interne (forma nr.21, anexă la prezentul Regulament), cu un număr unic de ordine.

221. Toate registrele (cărțile pentru înregistrări și fișele de evidență) se înregistrează în Registrul unic de evidență a registrelor și dosarelor finalizate, conform modelului din forma nr.22, anexă la prezentul Regulament, în care se înregistrează din momentul deschiderii, avînd un număr propriu de evidență.

222. Cărțile pentru înregistrări trebuie să fie șnuruite, iar filele numerotate și sigilate cu ștampila Subdiviziunii de protecție. Numărul de file se indică pe ultima pagină și se autentifică de către șeful Subdiviziunii de protecție, prin aplicarea semnelor de control: semnătura și ștampila.

223. La finele anului, numărul de fișe din fișierul finisat se indică în registrul unic de evidență al registrelor, dosarelor finalizate. Înscrierea finală, autentificată de către șeful Subdiviziunii de protecție, cu indicarea numărului total de fișe, se face pe o filă aparte, plasată la începutul sau sfârșitul fișierului.

224. Înregistrarea în registrul manual trebuie executată astfel încît să excludă posibilitatea de a fi radiată (ștearsă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ștergerii, distrugerii). Rectificările, modificările și completările registrului se autentifică prin semnătura persoanei din cadrul Subdiviziunii de protecție, cu indicarea datei.

225. Gradul de secretizare a registrelor de evidență se determină în funcție de gradul de secretizare a informațiilor ce se conțin în ele.

226. Evidența documentelor având gradul de secretizare "Strict secret" se ține separat.

227. În registre se reflectă datele cu privire la circulația documentelor, din momentul primirii sau întocmirii până la finisarea executării și clasarea lor în dosare, transmiterea destinatarului sau distrugerea lor.

228. Pentru asigurarea controlului și executarea documentelor se ține Registrul de evidență și control (forma nr.23, anexă la prezentul Regulament) sau se vor întocmi fișiere informative.

229. Rezoluția referitoare la document se face pe o fișă atașabilă (fișă de însoțire), care se păstrează împreună cu documentul și prevede executantul, indicația nemijlocită, termenul de execuție, semnătura conducătorului autorității publice sau altei persoane juridice și data. Responsabil pentru executarea documentului este persoana al cărei nume este indicat primul în rezoluție, dacă nu a fost numită o altă persoană.

230. La înscrierea rezoluțiilor, efectuarea însemnărilor pe documente, precum și la fiecare recipisă de primire și restituire a documentelor se indică în mod obligatoriu data.

231. Răspunsul din partea unei subdiviziuni la un document poate fi dat sub formă de rezoluție sau referință sumară direct pe fișa atașabilă (fișă de însoțire) la documentul respectiv, care se restituie expeditorului împreună cu documentul, conform numărului de intrare. Concomitent în registrul de evidență a documentelor de intrare se indică numărul și data expedierii. În același mod se permite a expedia spre executare instituțiilor subordonate interpelările parvenite de la alte autorități publice sau persoane juridice.

232. Documentele semnate de către conducătorii autorităților publice sau ai altor persoane juridice, care urmează a fi înregistrate, expediate și clasate la dosar, precum și documentele de intrare executate se predau de către executanți Subdiviziunii de protecție.

233. În caz de necesitate, executanții pot remite altor executanți ai subdiviziunilor interioare respective, în timpul programului de muncă, documentele ce conțin informații atribuite la secret de stat, cu excepția celor care au gradul de secretizare "Strict secret", dacă aceste documente îi privește nemijlocit și le sînt adresate de către conducătorul autorității publice sau al altei persoane juridice ori de șeful subdiviziunii. În acest caz, restituirea documentului către executantul de la care a fost primit se va efectua în aceeași zi.

234. Remiterea unor astfel de documente de la un executant la altul se efectuează contra semnătură (recipisă) în Inventarul interior al documentelor care se află la executant (forma nr.24, anexă la prezentul Regulament). De asemenea, conducătorii autorităților publice sau ai altor persoane juridice, precum și șefii subdiviziunilor sînt obligați să semneze în inventarul interior pentru documentele primite de la executanți.

235. Fiecare document sau alt purtător material de informații atribuite la secret de stat va fi inscripționat cu numărul de înregistrare și data cînd este înscris în registrul de evidență. Numerele de înregistrare sînt urmate de mențiunile "SS", "S", "C" sau "R", corespunzător gradului de secretizare atribuit.

236. Emitenții și deținătorii de informații atribuite la secret de stat sînt obligați să înregistreze și să țină evidența tuturor documentelor și materialelor primite, expediate sau a celor întocmite de unitatea proprie, potrivit legii.

237. Evidența actelor normative și a celor cu caracter de dispoziție emise de către autoritatea publică sau altă persoană juridică se efectuează conform registrului prevăzut în forma nr.25, anexă la prezentul Regulament. Evidența actelor normative primite pentru informare sau executare de la autoritățile publice (hotărîri ale Parlamentului, decrete ale Președintelui, hotărîri și dispoziții ale Guvernului, acte emise de către alte autorități publice, inclusiv locale) se efectuează conform registrului prevăzut în forma nr.26, anexă la prezentul Regulament.

238. Informarea cu conținutul actelor normative și de dispoziție se efectuează contra semnătură (recipisă) pe o fișă specială, numai la indicația scrisă a conducătorului autorității publice sau al altei persoane juridice emitente.

239. În registrele de evidență a informațiilor atribuite la secret de stat vor fi menționate numele și prenumele persoanei care a primit documentul, iar aceasta va semna pentru primire.

240. Atribuirea numerelor de înregistrare în registrele de evidență se face consecutiv, pe parcursul unui an calendaristic. Numerele de înregistrare se înscriu obligatoriu pe toate exemplarele documentelor sau materialelor care conțin informații atribuite la secret de stat, precum și pe documentele anexate.

241. Anual, documentele se clasează în dosare, potrivit problematicii, termenelor de păstrare stabilite în nomenclatoarele departamentale detaliate de informații care urmează a fi secretizate, precum și altor criterii.

242. Clasarea documentelor sau altor purtători materiali de informații atribuite la secret de stat se face separat, în funcție de suportul și formatul acestora, cu folosirea mijloacelor de păstrare și protejare adecvate.

243. Informațiile având gradul de secretizare "Strict secret" și cele cu privire la mobilizare vor fi compartimentate fizic și păstrate separat de celelalte informații.

244. Atribuirea aceluiași număr de înregistrare unor documente cu conținut diferit este interzisă.

245. Registrele de evidență vor fi completate de persoanele desemnate care dețin autorizație de acces la secret de stat de forma corespunzătoare.

Secțiunea a 3-a

Evidența caietelor de lucru și pentru stenografiere, carnetelor de notițe speciale, formularelor, mapelor de lucru, servietelor și valizelor speciale

246. Caietele de lucru și pentru stenografiere, carnetele de notițe speciale se eliberează executanților pentru efectuarea însemnărilor ce conțin informații atribuite la secret de stat. Evidența acestora se ține în Registrul de evidență a caietelor de lucru, potrivit formei nr.27, anexă la prezentul Regulament. Evidența caietelor de lucru, pentru stenografiere și a carnetelor de notițe speciale poate fi efectuată într-un registru unic, însă în mod separat.

247. Ținerea caietelor de lucru pentru înscrierea informațiilor având gradul de secretizare "Strict secret" se efectuează doar cu permisiunea scrisă a conducătorilor autorităților publice sau altor persoane juridice.

248. Filele caietelor trebuie să fie șnuruite, numerotate, sigilate și semnate de către șeful Subdiviziunii de protecție. Caietele se secretizează, pe copertele acestora se indică destinația lor, numele, prenumele executantului și numărul de înregistrare.

249. Filele carnetelor de notițe speciale și cotorul acestora se numerotează, iar pe fiecare filă se indică numărul de evidență al carnetului. În cazul editării caietelor de notițe speciale cu fișe de control, cotoarele acestora nu se numerotează.

250. La eliberarea carnetelor de notițe speciale pentru unică utilizare, persoana din cadrul Subdiviziunii de protecție va indica în Fișa de evidență a documentelor (dosarelor) eliberate (forma nr.28, anexă la prezentul Regulament) numărul de file existente și numărul de file rămase la restituirea carnetului. Consemnarea cu privire la transmiterea și distrugerea filelor detașabile se efectuează pe cotoarele filelor detașate sau pe fișa de control a carnetului de notițe special.

251. Carnetele de notițe speciale, eliberate pentru unică utilizare, trebuie să fie prevăzute cu un suport rigid care exclude posibilitatea de imprimare a amprentelor documentului întocmit.

252. Inventarele interioare broșate ale documentelor care se află la executanți se iau în evidență în Registrul de evidență a caietelor de lucru sau în conturile personale (forma nr.29, anexă la prezentul Regulament). Conturile personale se iau în evidență în registre separate, conform modelului din forma nr.27, anexă la prezentul Regulament.

253. Mapele de lucru, servietele și valizele speciale se eliberează executanților contra semnătură (recipisă). La restituirea acestora Subdiviziunii de protecție, se verifică corectitudinea sigilării lor și respectarea termenului de restituire.

254. În lipsa executanților, în caz de necesitate, mapele de lucru, servietele și valizele speciale pot fi deschise, cu permisiunea șefului Subdiviziunii de protecție, de către angajații Subdiviziunii de protecție,

în prezența unui reprezentant al subdiviziunii în care activează executantul. Aceste persoane fac înscrieri, confirmate prin semnătură (recipisă), în inventarele interioare ale documentelor ce se află la executanți sau într-un registru special, ținut de Subdiviziunea de protecție, indicând cine, cînd și cu ce scop a efectuat deschiderea, corespunderea documentelor cu inventarul interior, numărul ștampilelor cu care a fost și cu care urmează a fi sigilată mapa de lucru, servieta sau valiza specială. În cazul în care este necesară extragerea documentelor din mapa de lucru, servieta sau valiza specială se indică numărul documentelor extrase și numărul de file al acestora. După deschidere, mapa de lucru, servieta sau valiza specială, se sigilează cu ștampila personală a reprezentantului subdiviziunii în care activează executantul. La întoarcere, executantul este obligat să verifice prezența documentelor.

255. Pentru sigilarea mapelor de lucru, servietelor sau valizelor speciale, a depozitelor de păstrare a documentelor, executanților li se eliberează, contra semnătură (recipisă) în contul personal sau în Registrul de evidență a ștampilelor (forma nr.30, anexă la prezentul Regulament), ștampile de metal numerotate.

Secțiunea a 4-a

Transmiterea informațiilor atribuite la secret de stat

256. La transmiterea informațiilor atribuite la secret de stat se va asigura respectarea principiului necesității de a lucra cu astfel de informații.

257. Transmiterea informațiilor atribuite la secret de stat între autoritățile publice, alte persoane juridice sau cetățeni se va efectua cu permisiunea autorității publice cu împuterniciri de dispoziție asupra acestora.

258. Transmiterea informațiilor atribuite la secret de stat, în procesul de elaborare și adoptare a actelor normative poate fi efectuată fără permisiunea emitentului acestor informații, în limitele necesare îndeplinirii cerințelor de tehnică legislativă.

259. La transmiterea informațiilor atribuite la secret de stat vor fi create, în mod obligatoriu, condiții necesare pentru protecția acestor informații. În acest sens:

1) autoritățile publice trebuie să îndeplinească cerințele prevăzute în articolul 32 alineatul (3) literele a) – e) din [Lege](#);

2) alte persoane juridice, cu excepția autorităților publice, trebuie să dispună de certificat de securitate pentru efectuarea lucrărilor cu utilizarea informațiilor avînd un anumit grad de secretizare;

3) cetățenii trebuie să dispună de dreptul de acces la informațiile atribuite la secret de stat, de forma corespunzătoare.

260. Predarea-primirea informațiilor atribuite la secret de stat între expeditor și destinatar se face cu respectarea măsurilor de protecție, prevăzute în prezentul Regulament.

261. Corespondența secretă se transmite numai prin Subdiviziunile de protecție ale autorităților publice sau ale altor persoane juridice.

262. La primirea documentelor ce urmează a fi transmise, persoana din cadrul Subdiviziunii de protecție verifică prezența tuturor exemplarelor și filelor documentelor, ciornelor, corespunderea numerelor de înregistrare de pe documente cu numerele din registrele de evidență, corectitudinea întocmirii documentelor, prezența anexelor.

263. Documentele pot fi transmise destinatarilor cu sau fără scrisoare de însoțire.

264. La transmiterea documentelor cu scrisoare de însoțire, întocmirea lor se efectuează în modul prevăzut de punctele 191-192 ale prezentului Regulament.

265. Dacă anexele se transmit către destinatari diferiți, enumerarea lor se face pentru fiecare destinatar în parte.

266. Dacă la expeditor nu rămîn copii (exemplare) ale anexelor transmise, atunci în scrisoarea de însoțire se face mențiunea "Numai destinatarului".

267. Evidența documentelor întocmite se efectuează în registrele de evidență a documentelor întocmite (formele nr.31 și nr.32, anexă la prezentul Regulament).

268. La transmiterea unui număr mare de anexe prin scrisoare de însoțire, dacă enumerarea acestora în registrele de evidență a documentelor întocmite este imposibil de efectuat, în rubrica "Tipul și

conținutul succint al documentului” se va indica, în litere, numărul total de file al anexelor.

269. Documentele pot fi transmise destinatarilor fără scrisoare de însoțire, dacă conținutul și destinația acestora nu necesită explicații suplimentare.

270. La transmiterea documentelor fără scrisori de însoțire, pe plicurile în care se pun astfel de documente se înscriu numerele de înregistrare ale tuturor documentelor, indicându-se numărul de exemplare, iar în registrele de evidență se înscrie numărul și data expedierii. Transmiterea documentelor ce se referă la mobilizare se face în plicuri aparte, separat de alte documente secretizate.

271. Toate documentele ce conțin informații atribuite la secret de stat se transmit către alte autorități publice sau alte persoane juridice în plicuri sigilate, opace și rezistente.

272. Pe verso plicului, în centru se lipește eticheta de hârtie cu amprenta de cauciuc “Pentru plicuri”, în așa fel ca ea să cuprindă toate colțurile la mijloc.

273. Etichetele trebuie să fie confecționate din hârtie subțire care nu se supune stratificării, iar mărimea acestora trebuie să depășească cu 3-4 mm diametrul amprentei ștampilei de cauciuc. Deasupra etichetelor se aplică un strat subțire de clei, care trebuie să depășească marginile etichetei de hârtie.

274. Pe plic se indică următoarele date:

- 1) parafa de secretizare – în colțul drept de sus;
- 2) după caz, mențiunea “Personal” sau litera “M” – sub parafa de secretizare;
- 3) semnătura persoanei care a efectuat împachetarea și ștampila “Pentru plicuri”;
- 4) după caz, mențiunea “Urgent”, legalizată prin ștampila “Pentru plicuri” – în partea de sus în centrul plicului;
- 5) adresa destinatarului;
- 6) adresa expeditorului;
- 7) numerele de înregistrare a documentelor ce se conțin în plic.

275. La transmiterea unui document în mai multe exemplare, fără scrisoare de însoțire, în afara numărului de înregistrare al documentului, între paranteze, se indică numerele exemplarelor.

276. Documentele având gradele de secretizare “Strict secret”, “Secret” și “Confidențial” se transmit către alte autorități publice sau alte persoane juridice în plicuri duble. În acest caz, pe plicul exterior, în colțul stîng de sus se face înscrierea de preîntîmpinare “Plic dublu”. Parafa de secretizare, din punctul de vedere al securității, nu trebuie, în nici un caz, să apară pe plicul exterior.

277. La împachetarea dublă, pe plicul interior pot fi indicate și alte date, inclusiv mențiunile restrictive, numele expeditorului și al destinatarului.

278. Transmiterea și distribuirea corespondenței secretizate se efectuează de către curieri speciali, în conformitate cu prevederile [Legii Serviciului de Stat de Curieri Speciali nr.402-XV din 2 decembrie 2004](#) și ale Regulamentului Serviciului de Stat de Curieri Speciali, aprobat prin [Hotărîrea Guvernului nr.635 din 29 iunie 2005](#) “Cu privire la Serviciul de Stat de Curieri Speciali”.

279. Conducătorii autorităților publice și ai altor persoane juridice deținătoare de informații atribuite la secret de stat vor desemna cel puțin o persoană din cadrul Subdiviziunii de protecție proprii pentru transmiterea și executarea operațiunilor de predare-primire a corespondenței secretizate, între acestea și Serviciul de Stat de Curieri Speciali.

280. În caz de necesitate, cu permisiunea scrisă a conducătorului autorității publice sau al altei persoane juridice, documentele secretizate, cu excepția celor care au gradul de secretizare “Strict secret”, pot fi transmise în raza localității respective de către angajații Subdiviziunii de protecție, desemnați în conformitate cu punctul 279 din prezentul Regulament, în serviete speciale, sigilate cu ștampila Subdiviziunii de protecție și numai însoțiți de transportul departamental. Transmiterea și distribuirea corespondenței avînd gradul de secretizare “Strict secret” de către angajații desemnați ai Subdiviziunii de protecție în raza localității respective se admite, doar în cazuri excepționale, cu asigurarea pazei corespunzătoare (înarmate).

281. Transmiterea și distribuirea corespondenței secretizate de către angajații desemnați ai Subdiviziunii de protecție, în afara localității respective, se admite, doar în cazuri excepționale, cu asigurarea pazei corespunzătoare (înarmate).

282. În interiorul aceleiași clădiri sau al unui grup de clădiri, documentele ce conțin informații atribuite la secret de stat pot fi transmise într-un singur plic închis, menționând numai numele destinatarului, cu condiția ca expedierea (distribuirea) să fie efectuată de persoana desemnată din cadrul Subdiviziunii de protecție, care dispune de acces la secretul de stat de forma corespunzătoare.

283. Predarea-primirea corespondenței în procesul transmiterii și distribuirii se face contra semnătură (recipisă), în conformitate cu formele respective de evidență.

Secțiunea a 5-a **Recepționarea și înregistrarea informațiilor** **atribuite la secret de stat**

284. Toată corespondența secretizată, parvenită în autoritățile publice sau alte persoane juridice în timpul programului de muncă este recepționată numai de către Subdiviziunea de protecție.

285. În afara programului de muncă, corespondența secretizată este recepționată de către persoanele de serviciu din cadrul autorității publice sau al altei persoane juridice, care înregistrează plicurile în Registrul de evidență a plicurilor (forma nr.33, anexă la prezentul Regulament), fără a le deschide. Corespondența recepționată în acest mod se transmite, neîntârziat, Subdiviziunii de protecție, contra semnătură (recipisă).

286. Distribuirea corespondenței secretizate, în afara programului de muncă, către autoritățile publice sau alte persoane juridice care nu dispun permanent de persoane de serviciu nu se efectuează.

287. La recepționarea corespondenței se verifică: corectitudinea adresei, integritatea ambalajului (plicului) și amprentele ștampilei, corespunderea lor denumirii expeditorului, corespunderea numerelor indicate pe plic cu numerele indicate în registrul (borderoul, inventarul) de distribuire.

288. În cazul constatării unor nereguli (spre exemplu, deteriorarea ambalajului, necorespunderea amprentelor ștampilei cu denumirea expeditorului), plicul este recepționat prin întocmirea unui proces-verbal, semnat de persoana care a distribuit plicul și de cea care l-a recepționat, fapt ce se consemnează în registru.

289. Un exemplar al procesului-verbal se remite, după caz, Serviciului de Stat de Curieri Speciali sau expeditorului pentru luarea măsurilor necesare.

290. Dacă plicul este deteriorat astfel încât permite divulgarea conținutului documentelor pe care le conține, plicul cu documentele respective se va păstra intact, iar despre acest fapt va fi informat neîntârziat conducătorul autorității publice sau al altei persoane juridice și Serviciul de Informații și Securitate.

291. Persoana care recepționează corespondența semnează lizibil în registrul (borderoul, inventarul) de distribuire, indicând prin litere numărul plicurilor recepționate, data, ora recepționării lor și legalizează semnătura sa prin ștampila respectivă. Ulterior, în registrul de evidență a plicurilor sau în Registrul de control al plicurilor (forma nr.34, anexă la prezentul Regulament) se indică numărul de expediție și se scrie prin litere numărul plicurilor recepționate. Persoana de serviciu indică suplimentar în registrul de evidență a plicurilor numărul documentelor indicat pe plicuri. Aceste înscrisuri se confirmă prin semnătura curierului special care a distribuit corespondența, indicând data și ora de predare a corespondenței.

292. Toate plicurile recepționate și înregistrate în registrul de control al plicurilor se remit contra semnătură (recipisă) șefului Subdiviziunii de protecție sau persoanei împuternicite pentru a fi deschise. La deschiderea plicurilor se verifică corespunderea numerelor de înregistrare indicate pe ele cu numerele indicate pe documentele din plic, numărul documentelor cu datele de evidență indicate în scrisoarea de însoțire, numărul de exemplare și de file ale tuturor documentelor.

293. Dacă plicul conține mai multe documente, fiecare dintre ele se înregistrează cu un număr separat.

294. Persoana care deschide plicurile trebuie să se convingă de faptul că a extras toată corespondența din ele.

295. După deschiderea plicului, documentele se înregistrează neîntârziat în Registrul de evidență a documentelor recepționate sau în Fișele de evidență a documentelor recepționate (formele nr.35 și

nr.36, anexă la prezentul Regulament) ori, respectiv, în formele de evidență ale documentației tehnice.

296. Plicurile cu mențiunea "Personal" se deschid doar de către destinatar sau de persoana împuternicită. Înscrierea datelor referitoare la document se efectuează din spusele persoanei care a deschis plicul. În Registrul de evidență a documentelor recepționate (formele nr.35 și nr.36, anexă la prezentul Regulament) se face înscrierea "Plic cu mențiunea "Personal". După ce a luat cunoștință de conținutul documentului, destinatarul acestuia restituie documentul în plic Subdiviziunii de protecție. Documentele cu mențiunea "Personal" se păstrează în plic sigilat de către Subdiviziunea de protecție. Ulterior, la decăderea necesității de a păstra documentele cu mențiunea "Personal", acestea se distrug în modul stabilit de prezentul Regulament.

297. În cazurile în care se constată necorespunderi în datele de evidență ale documentelor recepționate, acestea vor fi menționate într-un proces-verbal, întocmit în două exemplare, semnat de șeful și persoana respectivă din cadrul Subdiviziunii de protecție. Un exemplar al procesului-verbal împreună cu recto plicului în care au fost primite documentele se expediază Subdiviziunii de protecție a autorității publice sau al altei persoane juridice expeditoare, iar celălalt exemplar se clasează în dosar.

298. La primirea procesului-verbal, Subdiviziunea de protecție a autorității publice sau al altei persoane juridice expeditoare întreprinde măsurile necesare în vederea explicării și lichidării necorespunderilor indicate în procesul-verbal.

299. Documentele expediate greșit se restituie expeditorului sau, de comun acord cu acesta, se expediază conform destinației, în plicuri noi, pe care se vor indica numerele lor de înregistrare, anexînd recto plicului expeditorului, iar în registrul de control al plicurilor se înscrie numărul acestuia și data expedierii.

300. Numărul de înregistrare a documentelor recepționate se indică în mod obligatoriu în Registrul de control al plicurilor.

301. La înregistrarea documentelor recepționate, în partea inferioară a primei pagini se aplică ștampila, în care se indică denumirea autorității publice sau al altei persoane juridice, numărul de evidență (de intrare), data înregistrării, numărul de file ale documentului de bază și ale anexelor la acesta (filele anexelor nesecretizate se indică separat). Pe prima filă a anexelor se aplică ștampila "La nr. _____ de intrare", indicîndu-se anul de înregistrare.

302. Documentele recepționate de la structurile subordonate sau interioare, ce dispun de Subdiviziuni de protecție, care au fost semnate de către conducătorii autorităților publice, altor persoane juridice sau organelor ierarhic superioare, pot fi transmise destinatarului cu numărul de înregistrare atribuit conform Registrului de evidență a documentelor, indicat în forma nr.37, anexă la prezentul Regulament.

303. Edițiile, materialele broșate, alte documente parvenite fără scrisori de însoțire trec în evidență în Registrul de control al plicurilor, în care se înscriu numerele de inventar sau alte numere de evidență, atribuite acestor documente la înregistrarea lor în registrele respective.

304. În cazul în care anexele nu pot fi clasate în dosar (spre exemplu, broșurile, documentele de format mare), se efectuează inventarierea lor, cu mențiunea respectivă în scrisorile de însoțire și în registrele de evidență a documentelor recepționate, iar scrisorile de însoțire se clasează în dosar. Anexele nesecretizate la documente, dacă nu se păstrează în comun, vor fi remise la secretariat, contra semnătură (recipisă) în Registrul de evidență a documentelor recepționate, efectuîndu-se consemnarea respectivă pe scrisoarea de însoțire.

305. Documentele recepționate, luate în evidență corespunzătoare, se remit, contra semnătură (recipisă), conducătorului autorității publice sau al altei persoane juridice căreia îi sînt adresate spre examinare.

306. Documentele avînd gradul de secretizare "Strict secret" se remit conducătorului autorității publice sau al altei persoane juridice, contra semnătură (recipisă), doar de către șeful Subdiviziunii de protecție sau de persoana numită pentru îndeplinirea obligațiilor acestuia.

307. Remiterea documentelor spre executare se efectuează numai prin intermediul Subdiviziunii de protecție.

308. Remiterea documentelor neînregistrate spre executare nu se admite.

309. Documentele care au gradul de secretizare "Strict secret" pot fi aduse la cunoștință doar persoanelor care dispun de acest drept, în virtutea funcțiilor exercitate, numai în privința aspectelor legate nemijlocit de activitatea acestora și doar cu permisiunea scrisă a conducătorului autorității publice, altei persoane juridice sau a persoanei căreia i-au fost adresate.

310. La primirea documentelor de la executanți, angajații Subdiviziunii de protecție verifică corespunderea numerelor de înregistrare respective și a numărului de file ale documentelor cu mențiunile din registrul de evidență respectiv și din Inventarul interior al documentelor care se află la executant, semnând pentru recepționarea documentelor.

Secțiunea a 6-a

Multiplicarea

311. Multiplicarea documentelor ce conțin informații atribuite la secret de stat se efectuează numai de către persoane autorizate să aibă acces la astfel de informații, în încăperi special destinate. Autoritățile publice sau alte persoane juridice care lucrează cu un volum neînsemnat de documente secrete pot efectua multiplicarea acestora în încăperea Subdiviziunii de protecție.

312. Documentele secrete se multiplică într-un număr strict stabilit de exemplare și se transmit numai acelor subdiviziuni, autorități publice sau alte persoane juridice, cărora le sînt necesare în procesul activității.

313. Multiplicarea documentelor secrete se face în baza Foii de comandă privind multiplicarea documentelor secrete, potrivit formei nr.38, anexă la prezentul Regulament.

314. Se interzice multiplicarea documentelor secrete într-un număr de exemplare mai mare decît cel indicat în Foaia de comandă privind multiplicarea documentelor secrete, cu excepția înlocuirii filelor rebutate.

315. Multiplicarea documentelor ce conțin informații atribuite la secret de stat, cu excepția celor care au gradul de secretizare "Strict secret", se face în baza aprobării șefului subdiviziunii interioare, cu avizul Subdiviziunii de protecție, ambele înscrise pe Foaia de comandă privind multiplicarea documentelor secrete.

316. Multiplicarea documentelor avînd gradul de secretizare "Strict secret" se face în baza aprobării conducătorului autorității publice sau al altei persoane juridice, cu avizul Subdiviziunii de protecție, ambele înscrise pe foaia de comandă privind multiplicarea documentelor secrete.

317. La solicitare, multiplicarea documentelor ce conțin informații atribuite la secret de stat pentru alte autorități publice sau persoane juridice se poate efectua în baza Foii de comandă privind multiplicarea documentelor secrete, întocmite de către acestea. Executarea lucrărilor de multiplicare în asemenea cazuri se autorizează de către conducătorul autorității publice sau al persoanei juridice – executant, prin efectuarea înscrierii respective în Foaia de comandă privind multiplicarea documentelor secrete.

318. Foile de comandă privind multiplicarea documentelor secrete se înregistrează de către Subdiviziunea de protecție în Registrul de evidență a foilor de comandă (forma nr.39, anexă la prezentul Regulament). Pe foile de comandă privind multiplicarea documentelor secrete, parvenite de la alte autorități publice sau persoane juridice, se indică prin fracție și numărul de înregistrare al scrisorii de expediere.

319. Documentele secrete care urmează a fi multiplicare, împreună cu Foaia de comandă respectivă, se transmit, prin intermediul Subdiviziunii de protecție, către subdiviziunea de multiplicare, contra semnătură (recipisă), în formele corespunzătoare de evidență. Documentele se transmit doar pe termenul necesar îndeplinirii comenzii.

320. Subdiviziunile de multiplicare asigură înregistrarea documentelor primite și a Foilor de comandă privind multiplicarea documentelor secrete ce le însoțesc în Registrul de evidență a documentelor secrete multiplicare (forma nr.40, anexă la prezentul Regulament).

321. Pe documente, precum și în registrele de evidență respective se fac mențiuni cu privire la data, numărul de copii sau de extrase efectuate, de pe care pagini sau părți ale documentului, numărul de înregistrare a copiilor sau extraselor.

322. Consemnarea operațiunii de multiplicare se face atât pe original, cât și pe toate copiile rezultate. Pe documentul original mențiunea cu privire la multiplicare se aplică în partea de jos a ultimei pagini sau pe verso documentului original, indicându-se numărul copiilor făcute de pe el, data, numărul de înregistrare al acestora și cui au fost expediate. Dacă numărul destinatarilor este mare, poate fi întocmit un tabel de distribuire, care se înregistrează ca document anexat la original.

323. Pe copiile rezultate în urma multiplicării, marcarea se aplică pe prima pagină, sub numărul de înregistrare al documentului, prin aplicarea mențiunii “Copie”.

324. În cazul copierii succesive, la date diferite, a unui document secret, originalul va fi marcat la fiecare operațiune, care va fi, de asemenea, înscrisă în registru. Exemplarele rezultate în urma copierii documentului secret se numerotează în ordine succesivă, chiar dacă operațiunea se efectuează de mai multe ori și la date diferite.

325. Extrasul dintr-un document care conține informații atribuite la secret de stat se face în baza Foi de comandă privind multiplicarea documentelor secrete, analogic procedurii stabilite pentru multiplicare, iar documentul rezultat va avea menționat sub numărul de exemplar cuvântul “Extras” și numărul de înregistrare al documentului original.

326. Multiplicarea documentelor parvenite de la alte autorități publice sau alte persoane juridice se face doar cu consimțământul conducătorului autorității publice sau al altei persoane juridice cu împuterniciri de dispoziție asupra acestuia.

327. Parafa de secretizare atribuită unui document original se aplică, în mod identic, reproducerilor sau traducerilor.

328. Traducerea documentului se înregistrează cu același număr de înregistrare ca și originalul documentului, efectuându-se înscrierea corespunzătoare în formele de evidență.

329. Dacă emitentul dorește să aibă control exclusiv asupra reproducerii, documentul va conține o indicație vizibilă cu următorul conținut: “Reproducere interzisă”.

330. Informațiile atribuite la secret de stat, înscrise pe documente cu regim restrictiv de reproducere, care au mențiunea “Reproducerea interzisă”, nu se multiplică.

331. În cazul multiplicării unui document care conține informații atribuite la secret de stat se procedează astfel:

- 1) se stabilește numărul de exemplare în care va fi multiplicat;
- 2) se completează și se aprobă, în modul stabilit, Foaia de comandă, după care aceasta se înregistrează în registrul de evidență a foilor de comandă;
- 3) documentul original, împreună cu Foaia de comandă, se predă subdiviziunii de multiplicare pe bază de semnătură (recipisă);
- 4) după verificarea exemplarelor rezultate, acestea, împreună cu documentul original și Foaia de comandă, se predau, pe bază de semnătură (recipisă) în Registrul de evidență a documentelor secrete multiplicare, Subdiviziunii de protecție în vederea distribuirii sau expedierii.

332. La finisarea operațiunilor de multiplicare se vor întreprinde măsurile necesare în vederea excluderii posibilității de reproducere neautorizată a informațiilor multiplicare, fapt consemnat în Foaia de comandă privind multiplicarea documentelor secrete sau în Registrul de evidență a documentelor secrete multiplicare.

333. Stenografierea, redactarea după dictare sau de pe dispozitivele de redare a sunetului documentelor ce conțin informații atribuite la secret de stat, cu excepția celor având gradul de secretizare “Strict secret”, se efectuează numai în încăperi izolate, unde este exclusă posibilitatea de ascultare a conținutului acestora de către persoanele neautorizate.

334. Înregistrările stenografice a informațiilor atribuite la secret de stat, cu excepția celor care au gradul de secretizare “Strict secret”, se efectuează numai în caietele pentru stenografiere.

335. Purtătorii de informații magnetici sau de altă natură, destinați pentru imprimarea informațiilor atribuite la secret de stat, și caietele pentru stenografiere se înregistrează în Registrul de evidență al caietelor de lucru, iar după finalizarea activității se predau spre păstrare Subdiviziunii de protecție. Pe purtătorul de informații se aplică numărul de înregistrare.

336. Toți purtătorii materiali de informații atribuite la secret de stat, utilizați în activitatea de

multiplicare, pînă la transmiterea lor Subdiviziunii de protecție sau pînă la distrugere, se păstrează în condiții care să asigure protecția corespunzătoare a secretului de stat (safeuri, dulapuri de metal, depozite speciale sigilate, alți suportți speciali).

Secțiunea a 7-a **Multiplicarea tipografică**

337. Primirea documentelor secrete pentru multiplicare tipografică, evidența, păstrarea și transmiterea edițiilor secrete se efectuează prin intermediul Subdiviziunilor de protecție sau al subdiviziunilor documentației tehnice.

338. Documentele secrete primite spre multiplicare tipografică se înregistrează în Registrul de evidență a lucrărilor tipografice secrete (forma nr.41, anexă la prezentul Regulament).

339. Tirajul edițiilor secrete și lista destinatarilor acestora se aprobă de către beneficiar, după coordonarea cu Subdiviziunea de protecție a autorității publice cu împuterniciri de dispoziție asupra informației respective.

340. Edițiile cu tiraj mare (spre exemplu: cărți, instrucțiuni, broșuri) se tipăresc cu numerele de inventar atribuite originalelor acestora în Registrul de evidență a edițiilor secrete (forma nr.42, anexă la prezentul Regulament), pînă la predarea lor tipografiei. Dacă în ediție sînt incluse mai multe documente care au numere de evidență separate, atunci acestei ediții i se atribuie un număr unic de inventar.

341. Ordinele, instrucțiunile, indicațiile și alte acte cu caracter organizatoric și de dispoziție, precum și documentația tehnică care se ține în evidența de inventar se tipăresc cu numerele de evidență atribuite acestora.

342. Dacă într-o ediție au fost incluse documente cu diferite grade de secretizare, atunci acestei ediții i se aplică parafa de secretizare care corespunde celui mai înalt grad.

343. Pe copertă și pe foaia de titlu a fiecărui exemplar al ediției (documentului) se indică: parafa de secretizare, numărul exemplarului și numărul de inventar sau de evidență atribuit ediției (documentului). Pe verso ultimei file de text se înscrie o mențiune cu privire la: filele copertei pe care sînt indicate informații secrete, numărul de pagini, numărul planșelor (schemelor) nenumotate.

344. Dacă ediția secretă este formată din cîteva părți (capitole, articole) cu diverse grade de secretizare, parafa de secretizare se aplică la începutul fiecărei dintre aceste părți.

345. Dacă în ediția secretă sînt incluse scheme, desene, hărți, alte elemente componente de dimensiuni mai mari decît formatul ediției, atunci ele, de regulă, se plasează la sfîrșitul ediției, iar pe verso foii de titlu se indică numărul de planșe, numerele acestora și numărul de file intercalate. Dacă planșele nu se plasează la sfîrșitul ediției, atunci se menționează între care pagini au fost intercalate.

346. În cazul în care există un număr mare de planșe, acestea se broșează în blocuri separate, la sfîrșitul ediției sau în albume aparte.

347. Pe planșe se aplică parafa de secretizare respectivă, numărul comenzii tipografice și anul de ediție.

348. Evidența documentelor în tipografie se ține conform Registrului de evidență a lucrărilor tipografice secrete.

349. Foaia de comandă privind multiplicarea documentelor secrete executate, împreună cu originalele documentelor, se transmit Subdiviziunii de protecție sau subdiviziunii documentației tehnice, în bază de semnătură (recipisă) în registrul de evidență a lucrărilor tipografice secrete.

350. Imprimările de corectură se iau în evidență în registre corespunzătoare, cu numerele de evidență a originalelor. Ele se expediază beneficiarilor, în modul stabilit, pentru transmiterea documentelor secrete.

351. Pînă la începutul paginării, șpalturile se păstrează de către persoana desemnată special în acest scop sau nemijlocit de către zețar în regalurile pentru forme (dulapuri, safeuri), încuiate și sigilate.

352. La finisarea lucrărilor, toate materialele secrete se pun în safeuri (dulapuri de metal) și depozite, iar încăperile unde acestea se păstrează se verifică, se încuie, se sigilează și se predau sub pază. La sfîrșitul schimbului, formele de zaț care se află în mașinile de tipar se acoperă cu scuturi și se sigilează.

353. La finisarea multiplicării tipografice a documentelor secrete, executanții, împreună cu angajații Subdiviziunii de protecție, verifică locurile de muncă și tehnica de multiplicare pentru a exclude posibilitatea de a rămâne producție tipărită secretă (inclusiv rebutată).

354. După executarea comenzii (obținerea permisiunii de a publica ediția) și după verificarea corectitudinii textului ediției, tot materialul rebutat (imprimările de corectură, șpalturile, paginația, ultima corectură, matrițele) se verifică și, de comun acord cu beneficiarul, se distrug în modul stabilit de prezentul Regulament.

355. Tirajele ediției tipărite se țin în evidență în același registru în care au fost luate în evidență originalele cu numerele atribuite originalelor. Edițiile secrete ale publicațiilor cu tiraj mare, primite din alte autorități publice sau alte persoane juridice, se țin în evidență în Registrul de evidență a edițiilor secrete.

356. În cazul în care se depistează lipsa sau pierderea unor file (exemplare) în procesul de multiplicare tipografică a documentelor secrete, executantul informează imediat conducătorul tipografiei și șeful Subdiviziunii de protecție.

357. Completarea filelor sau a exemplarelor care lipsesc se efectuează cu permisiunea autorității publice cu împuterniciri de dispoziție asupra informațiilor respective, în baza Foii de comandă privind multiplicarea documentelor secrete, aprobată în modul corespunzător.

358. Edițiile și documentele secrete editate, până la remiterea lor beneficiarului, se păstrează împachetate și sigilate în safeuri sau în încăperi speciale.

359. Transmiterea documentelor (tirajului ediției) secrete multiplicat tipografic se efectuează în modul stabilit de prezentul Regulament, în conformitate cu lista de expediere, în care se enumără destinatarii și numărul de exemplare expediate. În registrul de evidență a edițiilor secrete se face o înscrisoare cu privire la data transmiterii documentelor și locul de aflare a listei destinatarilor, cu indicarea numărului de înregistrare al acesteia.

Secțiunea a 8-a **Nomenclatorul dosarelor. Clasarea** **documentelor și dosarelor**

360. În scopul întocmirii corecte a dosarelor, păstrării sigure a documentelor și selectării lor urgente, se întocmește Nomenclatorul dosarelor (forma nr.43, anexă la prezentul Regulament), ținându-se cont de sarcinile și funcțiile autorității publice sau ale altei persoane juridice.

361. În Nomenclatorul dosarelor se includ toate dosarele care reflectă activitatea autorității publice sau al altei persoane juridice, dosarele subdiviziunilor care activează provizoriu (spre exemplu, a comisiilor tehnice, a altor comisii), dosarele nefinalizate și cele sosite din alte autorități publice sau alte persoane juridice pentru a fi continuate, precum și Registrul unic de evidență al registrelor, dosarelor finalizate. Dosarele pe problemele care se soluționează pe parcursul mai multor ani (dosare transmisibile) se introduc în Nomenclatorul dosarelor pe fiecare an, având același număr de ordine pe întreaga perioadă de timp necesară pentru soluționarea acestor probleme, cu efectuarea mențiunii respective în Nomenclatorul dosarelor pe anul care a expirat: "*Transmisibil, început în anul _____*".

362. Nomenclatoarele dosarelor se împart în nomenclatoare individuale (pentru documentele unei subdiviziuni interioare concrete) și nomenclatoare de totalizare (formate din nomenclatoarele individuale ale subdiviziunilor interioare din autoritatea publică sau altă persoană juridică). Pentru persoanele juridice cu activitate economică și documentație similară se întocmește într-un nomenclator-tip al dosarelor.

363. Nomenclatorul dosarelor se întocmește de către Subdiviziunea de protecție în comun cu șefii subdiviziunilor interioare și, după caz, șeful arhivei secrete a autorității publice sau al altei persoane juridice. Elaborarea Nomenclatorului dosarelor se efectuează în conformitate cu regulile stabilite de Serviciul de Stat de Arhivă, ținându-se cont de importanța documentelor, uniformitatea documentelor intrate la dosar, termenele lor de păstrare. În cazul unui număr mic de dosare secrete (până la zece), Nomenclatorul dosarelor poate fi întocmit pentru câțiva ani, însă nu mai mult de cinci.

364. Nomenclatorul dosarelor semnat de către șeful Subdiviziunii de protecție, coordonat cu Serviciul de Stat de Arhivă și aprobat de către conducătorul autorității publice sau al altei persoane

juridice se aplică începînd cu 1 ianuarie al anului următor.

365. Nomenclatorul dosarelor se ține în evidență conform Registrului de evidență a documentelor întocmite (formele nr.31 și nr.32, anexă la prezentul Regulament) și se păstrează pe parcursul anului la șeful Subdiviziunii de protecție sau la persoana responsabilă de păstrarea lui. După efectuarea controlului anual, Nomenclatorul dosarelor se clasează într-un dosar, separat cu nomenclatoarele. Evidența nomenclatoarelor broșate se ține în Registrul unic de evidență a registrelor și dosarelor finalizate (forma nr.22, anexă la prezentul Regulament).

366. Nomenclatorul dosarelor se întocmește în așa fel încît fiecare executant să aibă posibilitatea a lua cunoștință de volumul informațiilor secrete necesare pentru îndeplinirea obligațiilor de serviciu.

367. În caz de necesitate, în Nomenclatorul dosarelor pot fi operate modificări și completări, în ordinea stabilită pentru aprobarea acestuia.

368. Termenele de păstrare a dosarelor incluse în Nomenclatorul dosarelor se stabilesc conform listelor tip sau listelor departamentale desfășurate ale documentelor ce conțin termenele de păstrare.

369. Volumele dosarelor și registrelor se introduc în Nomenclatorul dosarelor pe măsura deschiderii lor, cu indicarea numelui executantului responsabil de întocmirea dosarului (volumului), registrului.

370. În Nomenclatorul dosarelor se fac înscrieri cu privire la data deschiderii și finalizării dosarului (volumului), numărul de file și alte date necesare. Dacă pe parcursul anului în autoritatea publică sau altă persoană juridică se deschid noi dosare, acestea se includ suplimentar în Nomenclatorul dosarelor. În acest scop, la fiecare capitol al Nomenclatorului dosarelor se rezervă numere. La expirarea anului, la sfîrșitul Nomenclatorului dosarelor se indică numărul de dosare (volume) deschise care se păstrează provizoriu și care permanent și numărul de dosare transmisibile pentru anul următor.

371. Nomenclatorul dosarelor reprezintă documentul de evidență principal pentru anul în curs și constituie baza organizării evidenței, conform Registrului unic de evidență a registrelor și dosarelor finalizate (forma nr.22, anexă la prezentul Regulament).

372. Numerele de ordine ale dosarelor, conform Nomenclatorului dosarelor, reprezintă numerele dosarelor respective. În cazul unui număr mare de dosare incluse în Nomenclatorul dosarelor, acestora li se pot atribui indici care se formează din semnele convenționale ale subdiviziunii interioare și numărul de ordine al dosarelor (în limitele nomenclatorului dosarelor pentru subdiviziunea interioară).

373. Documentele se clasează în dosare pe diferite criterii (problematică, tip de documente, grad de secretizare, termen de păstrare, corespondență cu anumite autorități sau alte persoane juridice etc.). Întocmirea dosarelor se efectuează în conformitate cu regulile stabilite de Serviciul de Stat de Arhivă al Republicii Moldova.

374. Dosarele se întocmesc pe măsura clasării documentelor anului în curs. Dosarele transmisibile se întocmesc într-un număr strict limitat.

375. Documentele păstrate permanent se includ în dosare separat de cele păstrate provizoriu.

376. În dosare se clasează numai documentele executate și întocmite corect. La recepționarea documentelor executate pentru a fi clasate în dosare se verifică corectitudinea întocmirii acestora.

377. Pe coperta dosarului se va aplica: parafa de secretizare corespunzătoare gradului de secretizare a informațiilor care se conțin în documentele clasate, denumirea autorității publice sau a altei persoane juridice (a subdiviziunii interioare), numărul dosarului, după caz, titlul dosarului, data, luna, anul deschiderii și finalizării dosarului, numărul de file al acestuia, precum și termenul de păstrare.

378. Data deschiderii și finisării dosarului corespunde datei clasării primului și ultimului document în dosar.

379. Concomitent cu dosarul se întocmește și fișa de evidență privind eliberarea documentelor (dosarelor), conform formei nr.28, anexă la prezentul Regulament, care se păstrează într-un plic lipit pe partea interioară a copertei dosarului și se predă în arhivă împreună cu dosarul. La completarea deplină a fișei de evidență privind eliberarea documentelor (dosarelor) se întocmește o fișă nouă, care se anexează la cea completată și se păstrează împreună cu dosarul.

380. Fișa completată se include în Inventarul interior al dosarului (forma nr.44, anexă la prezentul Regulament), mai jos de însemnările totale, dar nu se consideră ca filă la dosar și nu se numerotează.

381. Toate dosarele finisate trebuie să fie corect perfectate: filele dosarului trebuie să fie broșate, numerotate și incluse în inventarul interior, iar pe inventar și pe o filă specială cusută la sfârșitul dosarului se face o înscrisoare de confirmare.

382. Toate documentele cusute la dosar se numerotează pe fiecare filă, în colțul drept de sus. Denumirea documentelor, numărul de evidență și data acestora cu numărul de file se includ în inventarul interior al documentelor, care se află în dosar.

383. Filele inventarului interior se numerotează separat. Numărul acestora se va indica în mențiunea de confirmare, după numărul total de file ale dosarului.

384. După finalizarea dosarului, la sfârșitul inventarului interior se indică, în cifre și în litere, numărul documentelor incluse în el. De asemenea, se indică funcția, numele, prenumele persoanei din cadrul Subdiviziunii de protecție care a întocmit inventarul, iar pe fila specială cusută la sfârșitul dosarului se efectuează o înscrisoare, în cifre și în litere, privind numărul filelor cusute în el, conform modelului stabilit în forma nr.44, anexă la prezentul Regulament.

385. Dosarul cu documente se coase, se sigilează și se legalizează prin semnătura persoanei din cadrul Subdiviziunii de protecție care l-a întocmit.

386. Sigilarea dosarului se efectuează cu ajutorul unei etichete de hârtie cu amprente ștampilei Subdiviziunii de protecție, care se lipește în așa mod încât să cuprindă ațele șireturilor cu care a fost cusut dosarul.

387. Fiecare dosar poate să conțină cel mult 250 de file. În cazul în care documentele clasate în dosar depășesc acest număr, se întocmește un alt volum, indicându-se numărul lui de ordine.

388. Se interzice includerea în dosar a documentelor care nu se atribuie la acesta, a ciornelor, precum și a documentelor care urmează a fi restituite.

389. Rectificările efectuate în inventarul interior al dosarului trebuie să fie legalizate prin semnăturile persoanei care-l întocmește și a șefului Subdiviziunii de protecție.

390. În vederea asigurării regimului secret, documentele, pe parcursul anului, pot fi păstrate în biblioraft sau în mape cu clape, iar la finele anului se clasează în dosar.

391. Pentru dosarele cu șine și mapele cu clape se întocmește inventarul interior al documentelor care se află în ele și foaia de titlu pe care se fac mențiunile stabilite de prezentul Regulament.

392. Eliberarea dosarelor sau a unor documente aparte, necesare în activitatea de serviciu, se efectuează de către Subdiviziunea de protecție doar executanților care au drept de acces la acestea, contra semnătură (recipisă) în fișa de evidență privind eliberarea documentelor (dosarelor), în care se indică datele cu privire la dosarul sau documentul eliberat (numărul dosarului sau al documentului eliberat, numărul exemplarului documentului și numărul de file al acestuia).

393. Dosarele și documentele eliberate ce conțin informații cu gradul de secretizare "Strict secret" se restituie în aceeași zi.

394. Dacă este necesar ca executantul să ia cunoștință numai de conținutul anumitor documente ce se află în dosar, care nu au legătură nemijlocită cu activitatea desfășurată, informarea cu aceste documente se face cu permisiunea scrisă a șefului subdiviziunii în care lucrează executantul, în prezența unei persoane din cadrul Subdiviziunii de protecție.

395. Lucrul cu documentele și dosarele având gradul de secretizare "Strict secret" se efectuează în condiții care asigură păstrarea acestora și exclud posibilitatea de acces al altor persoane la conținutul lor.

396. Retragerea din dosar a documentelor sau transferarea acestora dintr-un dosar în altul se efectuează, în cazuri excepționale, numai cu permisiunea șefului Subdiviziunii de protecție, prin anexarea în dosarul respectiv a unei Adeverințe de substituie, în conformitate cu forma nr.45, anexă la prezentul Regulament. În cazul în care din dosar se retrag definitiv unele documente, în inventarul interior al dosarului și în formele de evidență se vor face mențiunile respective.

397. La retragerea documentelor din dosarele înregistrate în registrele de evidență ale anilor precedenți, acestea trebuie înregistrate din nou în registrele de evidență a documentelor secrete ale anului în curs, cu efectuarea mențiunilor respective în adeverința de substituie.

398. Adeverința de substituie este semnată de către șeful Subdiviziunii de protecție.

399. Mențiunile cu privire la modificarea numărului de file ale dosarului la retragerea definitivă a documentelor din acesta se indică pe copertă, în inventarul interior și pe fila specială de confirmare.

400. La retragerea definitivă a documentelor din dosar, renumerotarea filelor acestuia nu se efectuează.

401. Toate dosarele finisate se țin în evidență în Registrul unic de evidență al registrelor, dosarelor finalizate.

402. În cazul în care dosarul conține mai multe volume, fiecare dintre acestea se înregistrează în Registrul unic de evidență a registrelor, dosarelor finalizate, cu un număr aparte, care se aplică pe copertă.

403. În Registrul unic de evidență a registrelor, dosarelor finalizate se fac mențiuni cu privire la data deschiderii și finisării dosarului, termenele de păstrare, numărul de file ale acestuia, după caz alte date necesare.

404. Dosarele finisate se transmit pentru păstrare în arhivă. Despre predarea dosarului în arhivă sau, eventual, distrugerea acestuia se va indica în Registrul unic de evidență a registrelor și dosarelor finalizate.

405. Autoritățile publice sau alte persoane juridice care dețin informații atribuite la secret de stat vor organiza și vor efectua expertiza valorii documentelor în vederea predării acestora spre păstrare în arhivele secrete departamentale sau pentru distrugere. În acest sens, în autoritățile publice sau alte persoane juridice se creează comisii de expertiză, formate din cel puțin 3 membri.

406. Pentru păstrarea documentelor finisate, în autoritățile publice sau alte persoane juridice se creează arhive secrete departamentale, subordonate Subdiviziunilor de protecție, care trebuie să asigure selectarea, evidența, păstrarea și utilizarea documentelor Fondului Arhivistic al Republicii Moldova, constituite ca urmare a activității lor și a subdiviziunilor subordonate.

407. Dosarele finisate se păstrează cel puțin un an în Subdiviziunea de protecție, după care se transmit în arhiva secretă departamentală, în baza inventarelor întocmite în acest sens. Un exemplar al inventarului cu recipisa de la arhivă pentru primirea dosarelor se restituie depunătorului și se păstrează în Subdiviziunea de protecție.

408. La predarea-primirea documentelor în arhiva secretă departamentală se verifică corectitudinea întocmirii și selectării acestora. Documentele, dosarele și inventarele la a căror întocmire s-au admis încălcări, urmează a fi rectificate de către persoanele responsabile pentru predarea documentelor în arhivă.

409. Documentele se păstrează în arhivele secrete departamentale pe parcursul termenului de secretizare a acestora.

410. La expirarea termenului de secretizare, documentele desecretizate care prezintă valoare istorică, științifică, culturală se transmit spre păstrare permanentă la Arhiva Națională a Republicii Moldova, în modul stabilit de legislația în vigoare.

411. La dosarele selectate pentru păstrarea permanentă se întocmesc inventare, care vor fi aprobate de către comisiile de expertiză și control ale instituțiilor de arhivă respective. Inventarele dosarelor care se vor păstra temporar se întocmesc separat de inventarele dosarelor care vor fi păstrate permanent. Aceste inventare se întocmesc în două exemplare și nu se expediază în instituțiile de arhivă.

412. În cazul reorganizării sau lichidării autorității publice sau altei persoane juridice, pentru soluționarea chestiunilor privind păstrarea ulterioară a documentelor Fondului arhivistic de stat se instituie o comisie, în componența căreia vor intra inclusiv reprezentanți ai organului de stat pentru supravegherea și administrarea Fondului Arhivistic al Republicii Moldova și angajați ai Subdiviziunii de protecție.

413. Documentele și dosarele secretizate, păstrate provizoriu la expirarea termenelor stabilite, se distrug în modul prevăzut de prezentul Regulament.

414. Angajații arhivei fondurilor secrete întocmesc schema amplasării documentelor și dosarelor și planul evacuării lor în situații excepționale. Schema și planul se coordonează cu șeful Subdiviziunii de protecție și se aprobă de către conducătorul arhivei.

415. Evidența și păstrarea documentelor și dosarelor în arhiva secretă departamentală se

efectuează în conformitate cu regulile de activitate a Arhivei de Stat și cu prezentul Regulament.

416. Documentele și dosarele, cu excepția celor avînd gradul de secretizare "Strict secret" care se păstrează în arhivele secrete departamentale, pot fi eliberate pentru utilizare temporară executanților care au acces la secretul de stat, cu permisiunea șefilor subdiviziunilor lor interioare și Subdiviziunii de protecție. Dosarele se eliberează executanților la locul de muncă în cazuri excepționale, în baza fișei de evidență privind eliberarea documentelor (dosarelor).

417. Documentele de arhivă și dosarele care au gradul de secretizare "Strict secret" nu se eliberează executanților la locul de muncă. Informarea cu conținutul unor astfel de documente se efectuează în încăperea arhivei sau Subdiviziunii de protecție, cu permisiunea șefului Subdiviziunii de protecție și a conducătorului autorității publice sau al altei persoane juridice.

418. Controlul disponibilului de documente secrete în arhivele secrete departamentale se efectuează cel puțin o dată la 5 ani.

419. Modificarea parafei de secretizare și desecretizarea documentelor și dosarelor, care se păstrează în arhiva secretă departamentală, se efectuează în modul stabilit de prezentul Regulament.

420. Despre modificarea parafei de secretizare sau desecretizarea documentelor și dosarelor, care se află la păstrare în arhiva secretă departamentală se fac mențiunile respective pe acestea, indicîndu-se numărul și data deciziei cu privire la modificarea parafei de secretizare sau cu privire la desecretizare.

421. Dosarele desecretizate se transmit pentru păstrare obișnuită, conform actului de inventar, cu efectuarea mențiunilor respective în formele de evidență a documentației din arhivă.

422. Modificarea parafei de secretizare a documentelor secrete selectate pentru arhivele de stat se efectuează de către arhivele de stat împreună cu autoritățile publice sau cu alte persoane juridice și, după caz, cu succesorii lor de drept, ale căror documente se păstrează în arhive.

423. Desecretizarea purtătorilor materiali de informații atribuite la secret de stat care se păstrează în fondurile închise ale arhivelor se efectuează de către conducătorii arhivelor de stat, cu condiția că organizația întemeietoare a fondului sau succesorul ei de drept le delegă astfel de împuterniciri. În caz de lichidare a organizației întemeietoare a fondului și de lipsă a succesorului ei de drept, problema desecretizării purtătorilor materiali de informații atribuite la secret de stat este examinată de către Comisia interdepartamentală pentru protecția secretului de stat.

424. Documentele și dosarele avînd gradul de secretizare "Strict secret", care se află la păstrare de stat, pot fi eliberate pentru utilizare provizorie cetățenilor care dispun de dreptul de acces la secret de stat, autorităților publice sau altor persoane juridice care dețin certificat de securitate, cu permisiunea autorității publice cu împuterniciri de dispoziție asupra acestor informații, care a predat aceste documente și dosare la păstrare, sau a succesorilor acestora.

Secțiunea a 9-a

Bibliotecile secrete

425. Pentru asigurarea specialiștilor cu informație tehnico-științifică și cu altă informație secretă, în autoritățile publice sau alte persoane juridice pot fi create biblioteci ale edițiilor, documentației tehnico-științifice și a microhărților secrete.

426. Pentru bibliotecile secrete se eliberează încăperi speciale, care trebuie să dispună de depozite, săli de lectură dotate cu locuri de lucru pentru executanți (abonați), separate prin pereți despărțitori de protecție, cu ferestre (bariere) pentru eliberarea și restituirea documentelor, care ar permite supravegherea vizuală a executanților (abonaților) cărora li s-au eliberat documente secrete.

427. Se interzice păstrarea documentelor avînd gradul de secretizare "Strict secret" în bibliotecile secrete ale autorităților publice sau ale altor persoane juridice.

428. Evidența documentelor din bibliotecile secrete se ține de către Subdiviziunea de protecție sau reprezentantul acesteia în Registrul de evidență a edițiilor secrete sau în Registrul de evidență a materialelor broșate (forma nr.46, anexă la prezentul Regulament).

429. Documentele secrete se eliberează pentru utilizare în sala de lectură executanților (abonaților), care dispun de dreptul de acces la acestea, la prezentarea permisului scris (cu indicarea tematicii sau a denumirii ediției, documentului), eliberat de șeful subdiviziunii interioare respective și

vizată de șeful Subdiviziunii de protecție.

430. Documentele pot fi eliberate executanților (abonaților) la locul de muncă, în cazuri excepționale, cu respectarea cerințelor prezentului Regulament.

431. Eliberarea documentelor se face contra semnătură (recipisă) în Fișa de evidență privind eliberarea documentelor (dosarelor).

432. Însemnările necesare de pe documentele eliberate se efectuează în caiete de lucru ținute la evidență.

433. Pentru fiecare executant (abonat) care utilizează serviciile bibliotecii secrete se întocmește o fișă în care se introduc numerele de evidență a documentelor eliberate acestuia.

434. Eliberarea documentelor din bibliotecile secrete reprezentanților altor autorități publice sau persoane juridice se efectuează la prezentarea dispoziției eliberate abonatului de aceste autorități publice sau al persoanei juridice, a certificatului de acces la secret de stat de forma corespunzătoare și a permisului scris, eliberat de conducătorul autorității publice sau al persoanei juridice în gestiunea căreia se află biblioteca sau de șeful subdiviziunii interioare care a primit reprezentantul menționat. Acești abonați fac înscrieri necesare numai în caietele de lucru luate în evidență. La finisarea lucrului cu documentele secrete eliberate, aceste înscrieri se examinează și se vizează de șeful subdiviziunii interioare respective, caietele fiind predate Subdiviziunii de protecție pentru transmiterea lor conform destinației, în modul stabilit de prezentul Regulament.

435. Controlul asupra disponibilului documentelor în bibliotecile secrete și asupra respectării regulilor de utilizare a acestora se efectuează cel puțin o dată în an, în modul stabilit de prezentul Regulament, de către comisii special instituite în acest scop.

Secțiunea a 10-a

Distrușgerea purtătorilor materiali de informații atribuite la secret de stat

436. Sînt supuse distrușgerii purtătorii materiali de informații atribuite la secret de stat care și-au pierdut importanța practică sau al căror termen de secretizare a expirat și nu au valoare istorică sau altă valoare.

437. Distrușgerea documentelor și a altor purtători materiali de informații atribuite la secret de stat (în continuare – materiale) se face pe calea arderii, topirii, fragmentării (în fragmente cu suprafața de cel mult 2,5 mm²), dizolvării sau descompunerii chimice, transformării într-o masă moale fără formă sau praf, prin alte metode, astfel încît să nu mai poată fi reconstituite.

438. Documentele și dosarele avînd gradul de secretizare "Strict secret" se distrușg numai prin ardere.

439. Selectarea pentru distrușgere a materialelor cu termenele de păstrare expirate se face de către comisia de experți, care a efectuat expertiza valorii acestora. Materialele selectate pentru distrușgere se includ într-un proces-verbal, conform formei nr.47, anexă la prezentul Regulament, care va fi semnat de membrii comisiei de experți și aprobat de conducătorul instituției.

440. Materialele secretizate cu parafa "Strict secret", altele decît cele menționate în punctul 439 din prezentul Regulament luate în evidență, se distrușg în prezența șefului Subdiviziunii de protecție și a unei persoane autorizate să aibă acces la astfel de informații, în baza unui proces-verbal întocmit conform formei nr.47, anexă la prezentul Regulament, aprobat de conducătorul autorității publice sau al altei persoane juridice. Procesul-verbal de distrușgere este semnat de către șeful Subdiviziunii de protecție și de persoana care asistă la distrușgere.

441. Distrușgerea materialelor avînd gradele de secretizare "Secret", "Confidențial" și "Restricționat", altele decît cele menționate în punctul 439 din prezentul Regulament, luate în evidență, se face în baza unui proces-verbal întocmit conform formei nr.47, anexă la prezentul Regulament, în prezența a două persoane care dispun de dreptul de acces la secretul de stat de forma respectivă, dintre care cel puțin una este din cadrul Subdiviziunii de protecție. Procesul-verbal este semnat de către persoanele care asistă la distrușgere, avizat de Subdiviziunea de protecție și aprobat de conducătorul autorității publice sau al altei persoane juridice.

442. După finisarea verificării anuale a disponibilului de documente, fișele de evidență provizorie de asemenea se distrug, fapt ce va fi consemnat într-un proces-verbal.

443. Documentele de lucru, ciornelile sau materialele acumulate sau create în procesul de elaborare a unui document, care conțin informații atribuite la secret de stat, de regulă, se distrug. În cazul în care se păstrează, acestea vor fi datate, parafate conform gradului cel mai înalt de secretizare a informațiilor conținute, arhivate și protejate corespunzător gradului de secretizare a documentului final.

444. Distrugerea ciornelor documentelor ce conțin informații atribuite la secret de stat se realizează de către persoanele care le-au elaborat, în comun cu un angajat al Subdiviziunii de protecție. Procesul-verbal de distrugere a ciornelor se întocmește în cazul în care acestea au fost înregistrate într-o formă de evidență.

445. În situații de urgență, protecția, inclusiv prin distrugere, a materialelor secretizate cu parafa "Strict secret" are întotdeauna prioritate față de alte materiale.

446. Dacă din dosarele supuse distrugerii se extrag anumite documente necesare activității ulterioare, în procesul-verbal se indică tipul documentelor și din care dosare sînt extrase (numărul de înregistrare, denumirea documentelor, numerele dosarelor și filelor), precum și în care dosare noi, după care numere de file sînt cusute documentele extrase sau înregistrate în registrele anului în curs.

447. În registrele de evidență se fac însemnările privind locul aflării documentelor extrase, iar în procesul-verbal de distrugere se indică numărul real al filelor rămase la dosarul ce urmează a fi distrus.

448. Dosarele se distrug împreună cu inventarul interior, după verificarea obligatorie a fiecărei file, cu înscrierile respective în actele și inventarele interioare ale dosarelor.

449. Denumirea, numărul de înregistrare, numărul exemplarului, parafa de secretizare, numărul de exemplare și de file ale fiecărui document (material) care urmează a fi distrus se verifică pînă la includerea acestuia în procesul-verbal, conform registrelor de evidență.

450. Materialele selectate și incluse în procesul-verbal de distrugere se păstrează separat de alte materiale, în ambalaj sigilat.

451. Operarea unor rectificări în procesele-verbale de distrugere nu se admite. În cazuri excepționale, operarea rectificărilor se va certifica prin semnăturile tuturor celor care au semnat procesul-verbal.

452. Se interzice distrugerea materialelor pînă la aprobarea procesului-verbal în modul stabilit.

453. Pînă la distrugere, se verifică corespunderea materialelor cu informația indicată în procesul-verbal.

454. Distrugerea materialelor trebuie să se efectueze în cel mai scurt termen posibil, după aprobarea procesului-verbal. Dacă materialele destinate distrugerii sînt transportate în afara autorității publice sau al altei persoane juridice, atunci ele se distrug în aceeași zi.

455. Transportarea materialelor la locul de distrugere se efectuează în ambalaj sigilat.

456. Materialele se distrug de către persoanele care au participat la verificarea acestora și au semnat procesul-verbal de distrugere.

457. După distrugerea materialelor, în procesul-verbal se fac înscrierile respective cu privire la acest fapt, iar în registrele de evidență se va indica numărul procesului-verbal de distrugere și data înregistrării lui.

458. Se interzice operarea modificărilor în procesul-verbal de distrugere după verificarea materialelor, efectuarea înscrierilor în registrele de evidență pînă la distrugerea materialelor sau transportarea proceselor-verbale, inventarelor sau altor documente, care nu sînt destinate distrugerii, la locul de distrugere a materialelor.

459. Procesele-verbale de distrugere se clasează și se păstrează în dosare speciale ale Subdiviziunii de protecție.

460. Procesele-verbale de distrugere a dosarelor se păstrează permanent, iar procesele-verbale de distrugere a altor materiale – timp de 10 ani.

461. Subdiviziunea de protecție, cel puțin o dată în trimestru, verifică disponibilul tuturor documentelor primite, luate în evidență în perioada de control, care nu sînt clasate în dosare sau nu sînt completate în mape separate.

462. Anual, pînă la data de 1 martie, se verifică disponibilul tuturor documentelor și dosarelor avînd gradele de secretizare "Strict secret", "Secret", "Confidențial" și "Restricționat", indiferent de timpul primirii sau întocmirii lor și de faptul unde și la cine se află, cu excepția arhivelor.

463. Controlul se efectuează de către o comisie specială, instituită prin ordinul (decizia) conducătorului autorității publice sau al altei persoane juridice, formată din cel puțin trei persoane, care au atribuție directă la documentele verificate și acces la secretul de stat de forma respectivă, cu includerea obligatorie în componența ei a angajaților din Subdiviziunea de protecție.

464. În cazul existenței unui număr neînsemnat de documente atribuite la secret de stat, controlul poate fi efectuat de către conducătorul sau unul din angajații autorității publice sau altei persoane juridice, în comun cu un angajat al Subdiviziunii de protecție.

465. În timpul controlului se verifică circulația (primirea, transmiterea, multiplicarea, distrugerea) documentelor atribuite la secret de stat din anul supus verificării, efectuîndu-se concomitent confruntarea datelor de evidență cu documentele efectiv disponibile. În acest scop, se utilizează registre de evidență a documentelor, recipise, inventare, procese-verbale de distrugere a documentelor și alte forme de evidență, inclusiv cele în care se înregistrează multiplicarea documentelor.

466. Rezultatele controlului se înscriu într-un proces-verbal în care se indică:

- 1) tipul controlului efectuat;
- 2) denumirea subdiviziunii în care s-a efectuat controlul;
- 3) temeiul efectuării controlului;
- 4) componența comisiei de control;
- 5) termenele efectuării controlului;
- 6) caracterizarea succintă a situației lucrărilor de secretariat secrete și asigurarea regimului secret în activitatea executanților cu documentele secrete;
- 7) numărul total de documente luate în evidență în perioada de control, separat, pe toate tipurile de evidență;
- 8) numărul și denumirea documentelor care nu sînt luate în evidență, la cine au fost depistate și din care motive nu au fost luate în evidență;
- 9) numărul documentelor și numărul de evidență a documentelor care nu au fost prezentate în timpul verificării, pe numele cui au fost trecute și motivele neprezentării lor;
- 10) încălcările cerințelor prezentului Regulament admise de către angajații Subdiviziunilor de protecție, de alți angajați cu indicarea faptelor concrete, a numelui, prenumelui și funcției celor care le-au comis;
- 11) deciziile și propunerile privind rezultatele controlului și măsurile de lichidare a încălcărilor depistate.

467. Procesul-verbal privind controlul efectuat este semnat de către membrii comisiei și aprobat de conducătorul autorității publice sau al altei persoane juridice ori de către locțiitorul acestuia.

468. Despre rezultatele controlului asupra disponibilului documentelor secrete se fac mențiunile respective în inventarul interior al documentelor care se află la executant, în prezența acestuia.

469. Dacă în timpul controlului se constată lipsa unor documente secrete, comisia va informa imediat despre acest fapt conducătorul autorității publice sau al altei persoane juridice, precum și șeful Subdiviziunii de protecție, care, la rîndul lor, vor asigura informarea autorităților publice cu împuterniciri de dispoziție asupra informațiilor respective și a Serviciului de Informații și Securitate.

470. Subdiviziunea de protecție, cel puțin o dată în trimestru, verifică respectarea modului de asigurare a regimului secret de către executanți la locul de muncă. Controlul se efectuează în prezența executanților, iar în cazurile în care aceștia lipsesc – în prezența șefului subdiviziunii interioare sau a locțiitorului acestuia.

471. Rezultatele controlului, încălcările depistate și măsurile întreprinse pentru înlăturarea acestora sînt înscrise într-un registru special pentru evidența controalelor la locurile de muncă ale executanților,

ținut de Subdiviziunea de protecție.

472. Executanții vizați sînt informați, contra semnătură, despre înscrierile cu privire la control efectuate în registru.

473. Conducătorii autorităților publice și ai altor persoane juridice, Subdiviziunile de protecție, precum și șefii subdiviziunilor interioare sînt obligați să întreprindă măsuri de înlăturare a tuturor încălcărilor depistate în urma controalelor și să asigure, în limita competențelor, respectarea regimului secret, în conformitate cu prevederile [Legii](#) și ale prezentului Regulament.

Secțiunea a 12-a

Evacuarea documentelor secrete în situații de urgență

474. În situațiile de urgență, sarcina principală a Subdiviziunii de protecție a autorității publice sau a altei persoane juridice este de a asigura regimul secret în lucrul cu documentele secrete în locurile de evacuare și la obiectivele neevacuate, conform cerințelor prezentului Regulament și planurilor de evacuare.

475. Subdiviziunea de protecție trebuie să fie pregătită permanent pentru desfășurarea activității în condițiile unor situații de urgență. Fiecare persoană din cadrul Subdiviziunii de protecție trebuie să-și cunoască obligațiile și succesiunea acțiunilor, în caz de situații de urgență.

476. În vederea pregătirii pentru situații de urgență, Subdiviziunea de protecție, în comun cu alți specialiști din cadrul autorității publice sau ai altei persoane juridice, elaborează și înaintează spre aprobare ai conducătorului acesteia documentele prin care se determină:

1) nomenclatorul documentelor și dosarelor secrete, care urmează a fi transportate la locurile de evacuare, distruse sau predate în arhivă pentru păstrarea de stat, precum și a celor care rămîn la fața locului;

2) listele persoanelor responsabile pentru evidența și păstrarea documentelor și dosarelor secrete, care urmează a fi evacuate și paza acestora în momentul transportării, distrugerii sau predării la păstrare în arhiva de stat;

3) măsurile cu privire la paza documentelor și dosarelor secrete în locurile de evacuare.

477. Toate documentele și dosarele secrete se repartizează pe următoarele categorii, conform destinației acestora:

1) categoria I – include documentele și dosarele care se transportă la locurile de evacuare;

2) categoria a II-a – include documentele și dosarele care urmează a fi distruse la fața locului;

3) categoria a III-a – include documentele și dosarele care se predau spre păstrare în Fondul Arhivistic al Republicii Moldova;

4) categoria a IV-a – include documentele și dosarele care rămîn pe loc.

478. Repartizarea documentelor pe categorii se efectuează de către comisii special instituite, formate din șefi de subdiviziune (locuitori ai acestora), angajați ai Subdiviziunii de protecție. Repartizarea documentelor se aprobă de către conducătorii autorităților publice sau ai altor persoane juridice respective.

479. În locurile de păstrare a acestor documente și dosare (safeuri, containere, dulapuri de metal, saci, serviete, alți suportți speciali) trebuie să fie afișate inscripții cu privire la destinația documentelor și dosarelor, precum și numele, prenumele, funcția persoanelor responsabile pentru evidența și păstrarea lor.

480. Pentru transportare se selectează documentele și dosarele secrete necesare în activitatea zilnică în locurile de evacuare.

481. Distrugerea documentelor și dosarelor secrete se efectuează în condițiile stabilite de prezentul Regulament, după adoptarea deciziei cu privire la evacuarea autorității publice sau al altei persoane juridice.

482. Predarea documentelor și dosarelor secrete selectate pentru păstrarea de stat se efectuează în modul stabilit de prezentul Regulament. Locurile de predare a documentelor și dosarelor de arhivă se determină din timp de către autoritățile publice sau a altei persoane juridice.

483. La obiectivul (sau o parte a acestuia) care nu se evacuează se păstrează numai documentele

necesare activității curente, într-un număr strict limitat.

484. În timpul situației de urgență, autoritățile publice sau alte persoane juridice vor asigura respectarea regimului secret stabilit.

485. În zona de evacuare, la indicația conducătorului autorității publice sau al altei persoane juridice care se evacuează, se stabilește regimul secret, în conformitate cu cerințele prezentului Regulament.

486. Odată cu apariția situației de urgență se intensifică controlul asupra disponibilului documentelor și dosarelor secrete la locul de evacuare și la obiectivul evacuat. Despre rezultatele controalelor efectuate este informat șeful Subdiviziunii de protecție. Verificarea completă a documentelor și dosarelor se efectuează imediat după încheierea evacuării.

487. În autoritățile publice sau alte persoane juridice, amplasate în zona de frontieră, arhive secrete nu se creează. Documentele și dosarele secrete ce prezintă valoare istorică sînt transmise pentru păstrare în arhivele departamentale sau în alte locuri de către autoritățile publice sau alte persoane juridice în cauză, la indicația acestora.

488. Documentele și dosarele secrete ale autorităților publice sau ale altor persoane juridice din zona de frontieră se repartizează în două categorii:

- 1) categoria I, include documentele și dosarele care se transportă la locurile de evacuare;
- 2) categoria a II-a, include documentele care urmează a fi distruse la fața locului.

489. La evacuare, documentele și dosarele secrete din categoria I trebuie să fie împachetate în ambalaje speciale care, la inițiativa Subdiviziunii de protecție, se pregătesc din timp, într-un număr suficient. Transportarea acestor documente și materiale se efectuează cu mijloace de transport acoperite, iar ordinea de transportare a acestora se stabilește de către șeful Subdiviziunii de protecție.

490. Pentru organizarea transportării și sigilării ambalajului în care se află documentele și dosarele secrete, conducătorul autorității publice sau al altei persoane juridice numește din timp o persoană responsabilă din cadrul Subdiviziunii de protecție.

491. Transportarea se efectuează în conformitate cu prevederile prezentului Regulament.

492. Pentru amplasarea Subdiviziunii de protecție, la locul de evacuare trebuie să fie destinate încăperi (spații) aparte, asigurate cu pază.

493. La locul de evacuare, documentele și dosarele secrete se păstrează în cadrul Subdiviziunii de protecție numai în dulapuri de metal sau containere speciale. În afara programului de muncă, executanții sînt obligați să predea documentele secrete Subdiviziunii de protecție pentru păstrare în ambalaj sigilat (spre exemplu, mape de lucru, serviete).

494. Se interzice de a scoate documentele secrete din zona de evacuare fără paza corespunzătoare.

495. În locurile de evacuare, lucrările de secretariat secrete se țin în conformitate cu cerințele stabilite de prezentul Regulament.

496. Pentru a asigura eliberarea la timp a documentelor și dosarelor secrete, selectate și pregătite în prealabil, necesare activității în timpul situațiilor de urgență, se permite păstrarea acestora în mape de lucru (serviete, valize, containere) separate și sigilate de către executanți. Pentru aceste documente se întocmește un inventar în două exemplare, unul dintre care se predă contra semnătură (recipisă) responsabilului desemnat pentru organizarea transportării, iar al doilea se păstrează în mapa executantului.

497. Executanții care pleacă la locul evacuării predau cheile de la safeurile personale Subdiviziunii de protecție. Încăperile în care se află documentele și dosarele secrete ce rămîn pe loc se asigură cu pază corespunzătoare.

498. După evacuarea obiectivului sau a unei părți a acestuia, Subdiviziunea de protecție va asigura verificarea încăperilor, depozitelor, safeurilor, fapt consemnat într-un proces-verbal.

499. Documentele și dosarele secrete din categoria a II-a se distrug pe loc, despre care fapt se întocmește un proces-verbal, potrivit cerințelor prezentului Regulament.

500. În caz de infectare a documentelor și dosarelor care urmează a fi transportate (categoria I) cu substanțe radioactive, otrăvitoare, alte substanțe, se efectuează dezinfectarea (dezactivarea, degazarea)

acestora. Dacă asemenea posibilități nu există, documentele și dosarele respective se transportă, cu respectarea tuturor măsurilor de precauție, în locuri sigure pentru dezinfectare.

501. În cazul unor pericole eminente de atac (acaparare), se efectuează distrugerea imediată sau evacuarea tuturor documentelor și a dosarelor secrete.

Capitolul IV

REGULI SPECIFICE DE OPERARE CU DOCUMENTAȚIA TEHNICĂ SECRETĂ

Secțiunea 1

Cerințe generale

502. Organizarea evidenței, păstrării și utilizării documentației tehnice secrete se pune în sarcina subdiviziunilor de protecție ale autorităților publice și ale altor persoane juridice.

503. În autoritățile publice și alte persoane juridice în care există un volum mare de documentație tehnică se creează subdiviziuni ale documentației tehnice secrete, ce activează sub controlul Subdiviziunii de protecție.

504. Pentru păstrarea documentației tehnice și pentru lucrul cu o astfel de documentație, sînt destinate încăperi speciale, care să asigure protecția corespunzătoare a informațiilor atribuite la secret de stat.

Secțiunea a 2-a

Evidența preliminară a documentației tehnice secrete

505. Toate filele destinate pentru elaborarea manuscriselor și originalelor documentației tehnice secrete se înregistrează de către executanți în subdiviziunile documentației tehnice secrete, iar dacă acestea lipsesc – în Subdiviziunea de protecție.

506. Înregistrarea filelor destinate pentru executarea manuscriselor și a originalelor se efectuează în Registrul de evidență preliminară a documentației tehnice secrete sau Fișa de evidență preliminară a documentației tehnice secrete, potrivit formelor nr.48 și nr.49, anexă la prezentul Regulament. Filele destinate pentru executarea documentației tehnice secrete care au diferite denumiri și/sau grade de secretizare se iau în evidență preliminară cu numere de înregistrare diferite.

507. Filele suplimentare necesare în procesul executării documentației tehnice secrete se înregistrează cu același număr de evidență preliminară, indicîndu-se noua dată de înregistrare și numărul de file.

508. Pe recto primei file se indică denumirea documentației tehnice secrete elaborate.

509. Parafa de secretizare se aplică pe fiecare pagină a documentației tehnice secrete, în colțul drept de sus, iar fiecare pagină se numerotează.

510. Pe fiecare filă luată în evidență se aplică ștampila de înregistrare, indicîndu-se numărul și data, iar pe prima pagină se va indica numărul total de file.

511. Pe filele de formatul A₀ și A₁, B₀ și B₁, ștampila de înregistrare se aplică suplimentar pe recto în două colțuri pe diagonală.

512. Pe filele lipite (prinse), ștampila de înregistrare se aplică în locul în care acestea sînt lipite (prinse), iar în registrul de evidență se indică numărul acestora.

513. Pe filele broșate, ștampila de înregistrare se aplică pe copertă și pe prima filă.

514. Aplicarea unor etichete pe filele luate în evidență preliminară se efectuează numai cu permisiunea Subdiviziunii de protecție sau a subdiviziunilor documentației tehnice secrete, despre care fapt, pe documente, se efectuează o însemnare legalizată.

515. După elaborarea manuscrisului documentației tehnice secrete se pregătește originalul acesteia. Lista persoanelor care sînt în drept să permită executarea originalului după manuscris se aprobă de conducătorul autorității publice sau al altei persoane juridice.

516. Executarea originalului prin copiere manuală se efectuează pe file luate în evidență preliminară, indicîndu-se pe ele parafa de secretizare, numărul exemplarului, denumirea și marcarea

documentului.

517. În cazul fotocopierii originalului, ștampila și numărul de înregistrare se va asigura prin reproducerea de pe manuscris.

518. Semnele de înregistrare și ștampilele se aplică în locurile stabilite de standardele respective.

519. După executarea originalului și înregistrarea acestuia în registrul de evidență, manuscrisul documentației tehnice secrete se distruge în modul stabilit de prezentul Regulament.

520. Executarea copiilor documentației tehnice secrete, care se află în evidență preliminară, se efectuează ca excepție, pentru prezentarea acestora spre coordonare preventivă.

521. În cazul în care drept bază pentru elaborarea manuscrisului documentației tehnice secrete este necesar a se utiliza copia documentației tehnice secrete elaborate anterior, care se află în evidență preliminară sau de inventar, atunci această copie se radiază din evidența anterioară și se înregistrează preliminar cu noua ei denumire.

522. Evidența preliminară poate fi asigurată în formă unică pentru toate tipurile de documentație tehnică secretă sau poate fi ținută separat pentru diferite tipuri de documentație tehnică secretă, adăugându-se la numărul de evidență un indice distinctiv.

523. Evidența se ține anual, începând cu primul număr. Documentația tehnică secretă care urmează a fi transferată pe anul următor se înregistrează cu numere noi.

524. Registrele de evidență preliminară a documentației tehnice secrete se păstrează în decurs de un an de la închiderea tuturor numerelor de evidență și se distruge în baza unui proces-verbal.

525. Evidența fișelor de evidență a documentației tehnice secrete se ține în Registrul de evidență a circulației fișelor, potrivit formei nr.50, anexă la prezentul Regulament.

526. Fișele de evidență preliminară a documentației tehnice secrete se țin neîntrerupt. Fișele epuizate după verificarea anuală se distruge în baza unui proces-verbal, făcându-se însemnările respective în Registrul de înregistrare și de evidență a circulației fișelor.

Secțiunea a 3-a

Evidența de inventar a documentației tehnice secrete

527. Se supune evidenței de inventar:

1) documentația tehnică secretă, elaborată de autoritatea publică sau altă persoană juridică și aprobată în modul stabilit;

2) documentația tehnică secretă, aprobată în modul stabilit, primită de la alte autorități publice sau persoane juridice, după înregistrarea acesteia în Registrul de control al plicurilor.

528. Nu se supune evidenței de inventar documentația tehnică secretă care se clasează (coase) în dosar și documentația tehnică secretă care a fost primită pentru coordonare sau pentru utilizare provizorie.

529. Evidența de inventar poate fi ținută separat, conform diferitor criterii de clasificare (spre exemplu: denumire, tipul documentației, tipul de executare).

530. Evidența de inventar se ține conform formelor nr.51, nr.52 și nr.46, anexă la prezentul Regulament. Fișele evidenței de inventar a documentației tehnice secrete se țin în evidență conform Registrului de înregistrare și de evidență a circulației fișelor.

531. Copiile documentației tehnice secrete executate în autoritățile publice sau alte persoane juridice și expediate destinatarilor se țin în evidență în Fișele evidenței de inventar a copiilor documentației tehnice secrete (forma nr.53, anexă la prezentul Regulament). Despre întocmirea acestor fișe se face o însemnare în Registrul evidenței de inventar a documentației tehnice secrete/Fișa evidenței de inventar a documentației tehnice secrete.

532. Autoritățile publice sau alte persoane juridice, care nu elaborează documentație tehnică secretă și nu dispun de originale și duplicate, pot ține evidența copiilor, precum și a edițiilor secrete în Registrul evidenței de inventar a materialelor scrise broșate.

533. Documentației tehnice secrete luate în evidență după radierea ei din evidența preliminară i se acordă un singur număr de inventar, indiferent de numărul de file pe care a fost editată și numerele de evidență care au fost incluse în ea. În cazurile în care se ține evidența diferitor tipuri de documentație

tehnică secretă, la numerele de inventar se vor adăuga indici distinctivi.

534. După ce documentația tehnică secretă a fost luată în evidența de inventar, aceasta se radiază din evidența preliminară.

535. La radierea documentației tehnice secrete din evidența preliminară, în Registrul de evidență preliminară a documentației tehnice secrete/Fișa de evidență preliminară a documentației tehnice secrete se introduce numărul de inventar acordat acesteia, iar în Registrele prevăzute în formele nr.51, nr.52 și nr.46, anexă la prezentul Regulament, se face însemnarea cu privire la numărul de evidență preliminară a acestei documentații.

536. Pe fiecare filă din document, în locul stabilit de standardele respective, se aplică ștampila, indicându-se numărul de inventar și data când a fost luat în evidență.

537. Dacă copiile originalului documentației tehnice secrete urmează a fi broșate, numărul de inventar se aplică suplimentar pe câmpul primei pagini și al foii de titlu (dacă există). Pe documentația tehnică secretă în formă textuală, numărul de inventar se aplică în partea de sus a primei pagini și a foii de titlu, iar pe cele grafice – mai sus de înscrierea principală.

538. Pe documentația tehnică secretă recepționată de la alte autorități publice sau persoane juridice, numărul de inventar și datele luării în evidență se aplică:

1) pe originale – pe câmpul de coasere a fiecărei file, iar numerele de înregistrare se vor trasa cu tuș în linii subțiri;

2) pe duplicate – în rubrica stabilită a fiecărei file;

3) pe documentele completate în mape sau broșate în albume – pe etichete sau în colțul stîng de sus al copertei, precum și pe prima pagină sau foaie de titlu a inventarului și pe foaia de titlu (dacă există) a mapei (albumului);

4) pe copiile ce se păstrează în file aparte – în colțul stîng de sus al fiecărei file.

539. Documentația tehnică secretă care se ține în evidență de inventar poate fi eliberată executanților în caz de necesitate de serviciu.

540. Originalele documentației tehnice secrete se eliberează pentru executarea copiilor și duplicatelor, operarea în ele a modificărilor, precum și pentru restabilirea lor. Originalele se eliberează executanților numai la indicația scrisă a șefului subdiviziunii interioare, iar originalele documentației tehnice avînd gradul de secretizare "Strict secret" – la indicația scrisă a conducătorului autorității publice sau al altei persoane juridice.

Secțiunea a 4-a

Păstrarea documentației tehnice secrete

541. Documentația tehnică secretă se păstrează conform regulilor stabilite în standardele de stat, respectîndu-se cerințele prezentului Regulament.

542. Originalele documentației tehnice secrete pot fi completate și păstrate în mape.

543. Copiile documentației tehnice secrete se păstrează și se expediază altor autorități publice sau persoane juridice atît pe file aparte, cît și completate în mape sau broșate în albume.

544. Documentația tehnică secretă se completează în mape (albume), în caz de necesități de producție, respectîndu-se condițiile cu privire la informarea executanților numai cu informația necesară lor.

545. Mapei sau albumului i se atribuie un număr nou de inventar, iar parafa de secretizare se aplică în conformitate cu gradul de secretizare a informațiilor cuprinse în documentația tehnică secretă din mapă (album).

546. În inventarul anexat la mapă (album) se enumeră, în ordine succesivă, documentația tehnică secretă conținută în aceasta (denumirea documentelor, gradul de secretizare, numărul de evidență, numerele exemplarelor, numărul de file). Enumerarea filelor la întocmirea inventarului anexat la mapa (albumul) documentației tehnice secrete se începe cu foaia de titlu.

547. Numărul de inventar al documentației tehnice secrete incluse în mapă (album), se închide prin mențiunea "inclus în numărul de inventar ____", înscrisă în registrele prevăzute în formele nr.51, nr.52 și nr.46, anexă la prezentul Regulament.

548. Copiile broșate ale documentației tehnice secrete în formă textuală poartă numărul de inventar al originalului.

549. Fotoimprimările secrete anexate la copii se lipesc pe filele luate în evidență. Numărul acestora se confirmă prin semnătura legalizată și se înscrie în registrele prevăzute în formele nr.51 și nr.52, anexă la prezentul Regulament.

550. Se interzice aplicarea unor imprimări sau etichete care conțin informații atribuite la secret de stat pe coperta documentației tehnice secrete.

551. Registrele evidenței de inventar a documentației tehnice secrete nu pot fi eliberate executanților.

552. Pentru căutarea documentației tehnice secrete luate în evidența de inventar se întocmesc fișiere și cataloage speciale, care pot fi ținute atât în formă manuală, cât și electronică, cu respectarea cerințelor stabilite pentru asigurarea protecției secretului de stat.

Secțiunea a 5-a

Operarea modificărilor în documentația tehnică secretă

553. Operarea modificărilor în documentația tehnică secretă, precum și anularea (abrogarea) ei se efectuează conform avizului cu privire la modificare și regulilor expuse în standardele de stat corespunzătoare, respectându-se cerințele prezentului Regulament.

554. Avizul cu privire la modificări se întocmește de autoritățile publice sau alte persoane juridice, deținători ai originalelor. Avizele secrete cu privire la modificări se iau în evidența de inventar conform formelor nr.51 și nr.52, anexă la prezentul Regulament.

555. Toate modificările în documentația tehnică secretă se operează de angajați special desemnați din subdiviziunile documentației tehnice secrete din cadrul autorităților publice sau altor persoane juridice. În caz de necesitate, în această activitate pot fi antrenate persoane din cadrul subdiviziunilor interioare de producție, care au acces la documentația tehnică secretă supusă modificării.

556. Modificările se înregistrează în tabelul de modificări sau în lista de înregistrare a modificărilor. Dacă pe document nu există loc suficient pentru operarea modificărilor sau în timpul efectuării modificărilor poate fi afectată claritatea imaginii, se pregătesc file aparte ale originalului, cu luarea în calcul a modificărilor respective și păstrându-se numărul de inventar precedent.

557. Dacă originalul documentației tehnice secrete se înlocuiește în întregime cu un alt original, acestuia din urmă i se acordă un nou număr de inventar. Această documentație tehnică secretă se înregistrează în registrele prevăzute în formele nr.51 și nr.52, anexă la prezentul Regulament. Pe originalul anterior al documentației tehnice secrete se face o mențiune despre înlocuirea lui, cu referire la numărul nou de inventar.

558. Dacă se înlocuiesc unele file din original, pe ele se păstrează numărul de inventar. Mențiunea cu privire la înlocuirea acestor file (fără modificarea numărului total de file) se înscrie în Registrul evidenței de inventar a documentației tehnice secrete/Fișa evidenței de inventar a documentației tehnice secrete. Totodată, modificarea numărului de file va fi reflectată și în Fișa evidenței de inventar a copiilor documentației tehnice secrete.

559. Originalele (unele file) înlocuite ale documentației tehnice secrete se păstrează de rînd cu originalele în vigoare.

560. Înlocuirea unor file ale copiilor documentației tehnice secrete se efectuează prin rebroșare și efectuarea unei noi înscrieri legalizate pe o filă separată, atașată după fila cu înscrierea legalizată anterioară, care la fel rămîne în broșură. Noua înscriere poate fi făcută pe aceeași filă cu înscrierea anterioară, dacă există loc suficient. Filele înlocuite ale copiilor se distrug în modul stabilit, imediat după operarea modificărilor.

561. În documentația tehnică secretă editată prin metode tipografice, modificările se operează prin trasarea textului sau imaginilor grafice cu tuș. Dacă se modifică o parte a textului, atunci pe filele modificate se face o referință la suplimentele editate.

562. Pregătirea (restabilirea) originalelor documentației tehnice secrete în locul celor care au devenit inutilizabile se efectuează numai după întocmirea procesului-verbal despre anularea lor.

563. Restabilirea originalelor se efectuează pe file luate în evidență preliminară. Originalele restabilite se iau în evidență sub aceleași numere de inventar prin efectuarea înscrierii respective în registrele prevăzute în formele nr.51 și nr.52, anexă la prezentul Regulament. Pe originalul restabilit se aplică mențiunea “original restabilit nr.____”, indicîndu-se numărul de ordine al procedurii de restabilire. Originalul care conține cîteva file poate fi restabilit parțial, indicîndu-se acest fapt în registrele prevăzute în formele nr.51 și nr.52, anexă la prezentul Regulament. Pe fila de înregistrare a modificării originalului restabilit se reproduc datele cu privire la toate modificările operate anterior în acest document. Originalele anulate care au devenit inutilizabile se retrag din circulație și se păstrează separat de cele în vigoare, în decurs de un an, iar apoi se distrug, fapt care se consemnează într-un proces-verbal.

564. Duplicatelor nu se restabilesc. La necesitate, ele se execută repetat.

Capitolul V

REGULI PRIVIND EFECTUAREA LUCRĂRILOR SECRETE DE FILMARE ȘI FOTOGRAFIERE

Secțiunea 1

Lucrările de filmare și fotografiere, evidența documentelor cinematografice și fotografice secrete

565. Lucrările de filmare pentru producerea filmelor secrete se efectuează în cazurile în care există un scenariu (plan de scenariu), coordonat cu autoritățile publice interesate și cu beneficiarul respectiv, aprobat de către conducătorul autorității publice cu împuterniciri de dispoziție asupra acestor informații.

566. Filmarea și fotografierea unor procese secrete se efectuează în conformitate cu planurile de activitate ale autorităților publice și ale altor persoane juridice, aprobate de conducerea autorității publice cu împuterniciri de dispoziție asupra acestor informații.

567. Accesul grupului de filmare (executantului) la filmări (fotografieri) se efectuează cu permisiunea în scris a conducătorului autorității publice cu împuterniciri de dispoziție asupra acestor informații, în care se indică lista obiectelor (proceselor) care urmează a fi filmate (fotografiate), componența grupului de filmare și termenul de îndeplinire a lucrărilor.

568. Gradul de secretizare a filmului în întregime, a unor imagini, fonograme sincronice și textului crainicului, a altor elemente ale acestuia se determină de către autoritatea publică sau altă persoană juridică – beneficiar, în timpul scrierii și coordonării scenariului (planului de scenariu), în conformitate cu prevederile prezentului Regulament.

569. Este interzisă filmarea, fotografierea și prezentarea video a proceselor de fabricare și testare a articolelor avînd gradul de secretizare “Strict secret”. În caz de necesitate, aceste acțiuni pot fi efectuate doar cu permisiunea conducătorilor autorităților publice cu împuterniciri de dispoziție asupra informațiilor respective și a beneficiarului, în prezența șefului Subdiviziunii de protecție a autorității publice sau al altei persoane juridice unde se efectuează filmările, fotografierea sau prezentarea video.

570. Lucrările de filmare pentru producerea filmelor secrete pot fi efectuate de către autoritățile publice, precum și în studiourile și laboratoarele cinematografice ale persoanelor juridice care dispun de certificatul de securitate respectiv.

571. Numărul persoanelor care participă nemijlocit la procesul de filmare și creare a documentelor cinematografice și fotografice trebuie să fie cît mai limitat. Componența grupurilor de filmare și autorii scenariilor secrete (planurilor de scenariu) se aprobă de către autoritatea publică cu împuterniciri de dispoziție asupra informațiilor respective. Responsabil pentru filmare este o persoană din cadrul Subdiviziunii de protecție.

572. Filmarea și fotografierea informațiilor secrete, prelucrarea materialului filmat, executarea, copierea filmelor secrete se efectuează în conformitate cu Foaia de comandă privind executarea lucrărilor fotografice secrete (forma nr.54, anexă la prezentul Regulament) cu utilizarea materialelor cinematografice și fotografice marcate și luate în evidență de Subdiviziunea de protecție, pînă la începerea acestor lucrări. Numerele de inventar ale materialelor cinematografice și fotografice se indică în foile de comandă privind executarea lucrărilor fotografice secrete.

573. Evidența de inventar a negativelor fotografice, a pozitivelor (imprimărilor foto), a diapozitivelor imprimate de pe ele, a suporturilor electronici se ține în Registrul de evidență a negativelor fotografice și fotoimprimărilor (forma nr.55, anexă la prezentul Regulament). În acest registru se țin în evidență și negativile fotografice, imprimările fotografice și diapozitivele, suportii electronici primiți de la alte autorități publice sau alte persoane juridice.

574. Documentele cinematografice și fotografice (negativele, pozitivele, diapozitivele, suportii electronici) cu aceeași denumire, grad de secretizare al unuia și aceluiași obiect se iau în evidență în Registrul de evidență a negativelor fotografice și fotoimprimărilor cu același număr de inventar, indicându-se numărul exemplarului.

575. În cazurile în care nu există posibilitatea de a marca capetele peliculei, aparatul de filmare sau de fotografiere încărcat cu o atare peliculă trebuie să fie sigilat. Descărcarea și încărcarea aparatelor de filmat și de fotografiat sigilate în procesul filmării (fotografierii) se efectuează în prezența unei persoane din cadrul Subdiviziunii de protecție. Caseta filmată se plasează într-o cutie specială, care se sigilează. Dacă nu există posibilitatea de a marca pelicula și placa fotografică, ele se eliberează la unitate și de fiecare format aparte. Informația de pe suportul electronic se transferă, în prezența unei persoane din cadrul Subdiviziunii de protecție, pe un alt tip de suport, cu întocmirea unui proces-verbal în conformitate cu prezentul Regulament. Suportul de informație se plasează într-o cutie specială, care se păstrează în conformitate cu prezentul Regulament. Informația inițială după copiere se nimicește prin formatarea dispozitivului de fotografiere sau filmare folosit.

576. Se interzice de a diviza (fragmenta) peliculele cinematografice și materialele fotografice cu capetele marcate, pregătite pentru filmare. Dacă în timpul filmărilor secrete s-au produs rupturi ale peliculelor, acest fapt se consemnează în procese-verbale corespunzătoare.

577. Peliculele uzate se expun iluminării și se distrug, fapt ce se reflectă în Registrul de evidență a negativelor fotografice și fotoimprimărilor.

578. Filmelor cinematografice secrete și altor documente cinematografice secrete, în caz de necesitate, li se atribuie denumiri convenționale. Filmarea, prelucrarea, sonorizarea, copierea, montarea și tirajarea documentelor cinematografice secrete se înregistrează în registrele de evidență, elaborate de subdiviziunile de protecție, ținându-se cont de cerințele prezentului Regulament.

579. Pe fiecare negativ dezvoltat, căruia i s-a atribuit un număr de evidență, executantul lucrării indică parafa de secretizare, numărul de evidență, data, numărul exemplarului, metrajul peliculei, numărul cadrelor, numele și prenumele său. În cazul suporturilor electronici, se va indica capacitatea acestora.

580. Dacă din cauza dimensiunii mici a peliculei este imposibil de a face aceste înscriri pe negativ, pînă la începerea filmării, ele se efectuează pe șabloane speciale, care se fixează în partea dreaptă, mai sus de obiectul filmării și împreună cu acestea se fotografiază.

581. În cazul în care nu este posibil de a fixa șablonul pe obiectul de filmare, acesta se fotografiază la începutul și sfîrșitul filmării. În cazul filmării mai multor teme pe una și aceeași peliculă, șabloanele se filmează înainte și la finalizarea fiecărei teme. Parafa de secretizare se indică pe cadrul de titlu al filmului și la începutul textului crainicului. Pe fotografiile, parafa de secretizare se aplică pe recto documentelor fotografice.

582. Negativele cinematografice și fotografice, peliculele fotografice, suportii electronici se păstrează în dulapuri de metal, separate de alte documente. Pe capacul cutiilor de metal se indică: parafa de secretizare, denumirea convențională, numărul rolei (bobinei), numărul de evidență al acesteia, desenul și numărul lipiturilor.

583. Cînd există un număr mare de negative cinematografice și pelicule fotografice, ele se păstrează în încăperi speciale dotate cu mijloace de protecție împotriva incendiilor. După dispariția necesității practice și după expirarea termenului de păstrare, negativele și fotografiile se distrug în baza unui proces-verbal, cu reflectarea acestui fapt în Registrul de evidență a negativelor fotografice și fotoimprimărilor.

584. Fotografiile montate în alte documente secrete se radiază din Registrul de evidență a negativelor fotografice și fotoimprimărilor, în care se înscriu numerele de inventar și numerele

exemplarelor documentelor la care acestea se anexează.

585. În ambalajul în care materialele secrete (cinematografice și fotografice) filmate se prezintă studioului cinematografic (laboratorului cinematografic și fotografic) sau beneficiarului filmului pentru a fi prelucrate, se plasează un inventar în care se indică: parafa de secretizare, denumirea convențională a documentelor cinematografice și fotografice și numărul bobinelor. Persoana din cadrul studioului (laboratorului) cinematografic este obligată să controleze integritatea ștampilelor la primirea materialelor în Subdiviziunea de protecție, iar după dezvoltarea peliculei – marcarea și integritatea ei. Se interzice prelucrarea materialelor cinematografice și fotografice secrete care nu au fost luate în evidență în modul stabilit.

586. Dacă filmul cinematografic conține câteva părți, pe fiecare parte a acestuia trebuie să existe racorduri standard, pe care se indică: parafa de secretizare, metrajul (volumul), numărul lipiturilor, numărul părții (bobinei), tema, comanda și numărul de inventar.

587. Fiecare parte se plasează într-o cutie de metal aparte, pe care se înscriu toate datele menționate în racorduri.

588. Cadrele rebutate, precum și cadrele neprevăzute în comandă (scenariu) se retrag (se decupează) și se distrug, în modul stabilit. La fel se retrag și se distrug și resturile (fragmente) peliculei în procesul montării filmului.

589. Filmul cinematografic finisat este recepționat de o comisie, în componența căreia se includ reprezentanți ai autorităților publice interesate și ai beneficiarului.

590. Comisia întocmește un proces-verbal în care se va consemna faptul dacă filmul cinematografic corespunde scenariului aprobat (planului de scenariu), parafei de secretizare, va menționa metrajul (volumul) și alte date necesare. Procesul-verbal se aprobă de persoana care a aprobat scenariul (planul de scenariu) și va servi drept bază pentru ca filmul cinematografic să fie luat în evidență de inventar.

591. Multiplicarea filmelor cinematografice secrete și transmiterea lor se efectuează într-un număr strict limitat, determinat de conducerea autorității publice care a aprobat scenariul cinematografic. Se interzice efectuarea fotografiilor de pe cadrele cinematografice. În caz de necesitate, de pe anumite cadre, cu permisiunea conducătorului autorității publice cu împuterniciri de dispoziție asupra informațiilor respective, de comun cu beneficiarul, pot fi executate fotografii sau diapozitive, care sînt luate în evidență de inventar ca documente cinematografice și fotografice separate.

592. Aparatele de filmat și de fotografiat pentru filmări secrete se iau în evidență și se păstrează în laboratoarele cinematografice și fotografice și se eliberează contra recipisă în registrul de evidență.

593. Scenariile (planurile de scenariu), planurile de filmare, sarcinile și alte documente ce se referă la lucrările cinematografice și fotografice se clasează în dosare separate.

594. Eliberarea copiilor de pe documentele cinematografice secrete pentru o singură vizionare se efectuează cu permisiunea în scris a conducătorului autorității publice cu împuterniciri de dispoziție asupra acestor informații și avizul Subdiviziunii de protecție. Copiile documentelor cinematografice avînd gradul de secretizare "Secret", "Confidențial" și "Restricționat" pot fi eliberate cu permisiunea în scris a locțiitorului conducătorului autorității publice responsabil de asigurarea regimului secret sau cu permisiunea scrisă a șefului Subdiviziunii de protecție.

595. Transmiterea filmelor cinematografice secrete se face prin intermediul Serviciului de Stat de Curiere Speciali. Filmul cinematografic se prezintă împreună cu pașaportul tehnic al acestuia, care se restituie împreună cu filmul.

596. Demonstrarea filmelor cinematografice secrete se efectuează cu respectarea cerințelor stabilite pentru ședințele secrete.

597. Se interzice începerea demonstrării filmelor cinematografice secrete în lipsa persoanei desemnate responsabilă pentru vizionare. Vizionarea filmelor cinematografice secrete se înregistrează de Subdiviziunea de protecție într-un registru special în care se indică data, denumirea filmului cinematografic sau tema, parafa de secretizare, scopul demonstrării, timpul (ora) prezentării, numele, prenumele persoanei responsabile pentru vizionare și ale persoanei care demonstrează filmul.

598. În toate cazurile de demonstrare a filmelor cinematografice secrete se întreprind măsuri care

ar exclude pierderea sau extinderea informației în afara zonei controlate.

599. Modificarea metrajului filmului secret și a numărului de lipituri în cazurile în care se rupe pelicula cinematografică în timpul demonstrării filmului se consemnează într-un proces-verbal și se reflectă în pașaportul tehnic al filmului cinematografic, indicându-se temeiul operării modificărilor. Procesul-verbal se semnează de persoana responsabilă pentru demonstrarea filmului cinematografic și se aprobă de șeful Subdiviziunii de protecție.

Secțiunea a 2-a

Microfilmarea, evidența și păstrarea microfilmelor

600. Documentele secrete pot fi microfilmate sau stocate pe discuri optice ori pe suporturi magnetici în următoarele condiții:

1) procesul de microfilmare sau stocare să fie realizat cu aprobarea autorității cu împuterniciri de dispoziție asupra informației respective de către personalul care dispune de dreptul de acces la secretul de stat de forma corespunzătoare gradului de secretizare a informațiilor respective;

2) pentru microfilmele, discurile optice sau suporturi magnetici de stocare să se asigure aceeași protecție ca și pentru documentul original;

3) toate microfilmele, discurile optice sau suporturi magnetici de stocare să fie înregistrate într-o evidență specifică și supuse, ca și documentele originale, verificării anuale.

601. Lucrările de microfilmare a documentelor secrete se efectuează prin intermediul Subdiviziunii de protecție, în baza Foii de comandă privind executarea lucrărilor fotografice secrete. Foaia de comandă privind executarea lucrărilor fotografice secrete se eliberează după verificarea seturilor pregătite pentru microfilmare și a stării documentelor recepționate, precum și după întocmirea schemei de formare a bobinelor.

602. Peliculele eliberate pentru microfilmarea documentelor secrete se compostează la ambele capete de către Subdiviziunea de protecție, fapt ce se reflectă în Foaia de comandă privind executarea lucrărilor fotografice secrete.

603. Înainte de începerea lucrărilor de microfilmare, Subdiviziunea de protecție va asigura sigilarea casetelor fotografice (camerelor) încărcate cu peliculă.

604. Evidența documentației ce urmează a fi microfilmată de către laboratoarele de microfilmare (laboratoarele speciale) se ține în Registrul de evidență a documentației primite pentru microfilmare (forma nr.56, anexă la prezentul Regulament). În caz de necesitate, fiecare unitate din set (dosar, document aparte) se înregistrează cu un număr aparte.

605. Microfilmul trebuie să conțină microimaginea deplină a setului cu originalele documentelor. În cazurile în care există un volum mic de documente, se permite plasarea câtorva microfilme pe un singur purtător al microimaginilor (bobină, microfîșă, alt purtător material).

606. La microfilmarea documentelor din cîteva cadre, fiecare cadru trebuie să conțină o parte din imaginea documentului inclus în cadrul precedent sau în cel ce urmează.

607. După încheierea filmării, casetele (camerele) cu pelicula sigilată se transmit sectorului (subdiviziunii) de dezvoltare a microfilmelor, împreună cu foaia de comandă, în așa mod ca să fie asigurată evidența acestora. Originalul documentului se restituie Subdiviziunii de protecție.

608. Microfilmul secretizat trebuie să conțină un cadru de control cu imaginea obiectului și șablonului de identificare, care include:

- 1) parafa de secretizare;
- 2) genul microfilmului (de bază, de rezervă);
- 3) numărul de înregistrare a foii de comandă;
- 4) numărul de înregistrare a microfilmului;
- 5) marcarea microfilmului sau a unei părți a acestuia;
- 6) deținătorul originalului;
- 7) denumirea persoanei juridice care a efectuat microfilmarea;
- 8) felul documentației;
- 9) denumirea sau semnul convențional al art.(obiectului);

- 10) marcarea documentației;
- 11) datele cu privire la numărul de file filmate în microfilm;
- 12) date cu privire la numărul de cadre în microfilm (fără a se lua în calcul șablonul);
- 13) proporția micșorării imaginii;
- 14) data microfilmării.

609. Dacă microfilmul este alcătuit din câteva bobine sau microfîșe, atunci la sfîrșitul fiecărei bobine sau microfîșe, cu excepția ultimei, se aplică mențiunea “Va urma”, iar la începutul fiecărei bobine, cu excepția primei, se aplică mențiunea “Continuare”.

610. În caz de necesitate, pe șablon se aplică mențiuni cu privire la modificări și completări – “Imprimare suplimentară” sau “Modificare”.

611. După șablon se microfilmează lista de însoțire a documentației, iar ulterior – setul de documente indicat în lista respectivă. Șablonul se plasează la începutul și la sfîrșitul microfilmului și pe fiecare parte a acestuia.

612. Bobinele rebutate ale microfilmului sau ale unor cadre ale acestuia se distrug în baza unui proces-verbal.

613. Filmarea suplimentară a unor cadre aparte sau a bobinei în întregime pentru înlocuirea celor rebutate se efectuează cu același număr de înregistrare, atribuit microfilmului (bobinei) în această documentație, dar în baza unei noi foi de comandă.

614. Bobinele microfilmelor secrete finisate, după ce au fost luate în evidența de inventar și după verificarea calității acestora, se pun în cutii de metal speciale, se sigilează și se transmit, contra semnătură (recipisă), Subdiviziunii de protecție. Pe capacul cutiei se aplică numărul atribuit microfilmului (bobinei), parafa de secretizare, forma imaginii, tipul microfilmului (de bază, de rezervă), metrajul și numărul lipiturilor. Subdiviziunea de protecție înregistrează microfilmul în Registrul de evidență a microfilmelor (forma nr.57, anexă la prezentul Regulament) și expediază cutia cu microfilm (bobină) persoanei care a făcut comanda pentru păstrare permanentă.

615. Păstrării se supun două tipuri de microfilme: de bază și de rezervă. Microfilmul de bază este destinat pentru executarea copiilor documentelor, iar cel de rezervă – pentru restabilirea microfilmului de bază, în caz de deteriorare. Microfilmului de bază și celui de rezervă i se atribuie un singur număr și aceeași marcare.

616. Bobina micropeliculei ce conține microimaginele documentației modificate se lipește de microfilmul produs anterior sau se păstrează separat. Toate modificările care se includ în microfilme sînt reflectate în documentele de evidență.

617. Microhărțile efectuate de pe microfilmele secrete se trec în evidență în Registrul de evidență a negativelor fotografice și fotoimprimărilor. Pe fiecare filă a microhărții în colțul drept de sus se indică: parafa de secretizare, numărul microfilmului, numărul exemplarului, numărul de inventar al filei, iar prin cratimă – numărul cadrelor în microhartă.

Capitolul VI

REGULI DE OPERARE CU ARTICOLE SECRETE

Secțiunea 1

Respectarea regimului secret la producerea articolelor secrete și utilizarea lor

618. Asigurarea măsurilor privind respectarea regimului secret la proiectarea, producerea, păstrarea, transportarea și exploatarea articolelor secrete se efectuează de către conducătorii autorităților publice și ai altor persoane juridice, șefii subdiviziunilor respective, în colaborare cu Subdiviziunile de protecție.

619. Articolelor și părților lor componente li se pot atribui denumiri sau semne convenționale, care nu trebuie să dezvăluie existența acestora, caracterul, destinația, particularitățile tehnice și de alt gen. Denumirile convenționale ale articolelor pot fi indicate, în caz de necesitate, numai în documentele secrete.

620. Expunerea la expoziții a articolelor secrete, de regulă, nu se admite. În caz de necesitate, cu permisiunea autorităților publice cu împuterniciri de dispoziție asupra acestor informații și sub controlul Subdiviziunilor de protecție respective, pot fi organizate expoziții secrete speciale. Aceste expoziții pot fi vizitate de către persoanele care au acces la secretul de stat de forma respectivă și au atribuție la articolele secrete expuse în cadrul expoziției.

621. Posibilitatea de expunere la expoziție a noilor mostre de articole se coordonează cu beneficiarul.

622. Numărul de persoane care au dreptul să lucreze și să ia cunoștință de articolele secrete, documentația tehnică și alt tip de documentație trebuie să fie cât mai limitat și se determină de către șeful subdiviziunii respective de producție, de comun acord cu Subdiviziunea de protecție.

623. Verificarea disponibilului articolelor având gradele de secretizare "Secret", "Confidențial" și "Restricționat" se efectuează cel puțin o dată în trimestru, iar a celor cu parafa "Strict secret" – cel puțin o dată în lună.

624. Controlul general al disponibilului articolelor secrete se efectuează anual, în conformitate cu prevederile prezentului Regulament, de către comisii speciale, desemnate de către conducătorii autorităților publice și ai altor persoane juridice respective.

Secțiunea a 2-a

Evidența articolelor secrete și radierea lor din evidență

625. Articolele secrete se țin în evidență atât în perioada elaborării, fabricării, păstrării, testării și transportării, cât și în perioada exploatării lor.

626. Autoritățile publice și alte persoane juridice trebuie să întreprindă măsurile necesare ce ar exclude dezvăluirea informației cu privire la existența articolelor secrete.

627. Evidența articolelor secrete se efectuează:

1) la producția experimentală (în caz de lipsă a documentației tehnologice) – de la începutul fabricării acesteia, conform schițelor secrete, sau începând cu etapa de producție, indicată de constructorul-elaborator sau de beneficiar;

2) la producția în serie – din momentul indicat în fișele tehnologice sau de însoțire, iar în lipsa acestora – începând cu etapa indicată în schiță.

628. Articolele secrete recepționate de la alte autorități sau persoane juridice se iau în evidență din momentul recepționării lor.

629. Evidența articolelor secrete se ține separat de evidența celor nesecrete, conform semnelor distinctive de pe schițe, numerelor de uzină sau de inventar, care se aplică nemijlocit pe articole sau pe etichete speciale.

630. Articolele secrete pe care este imposibil de aplicat numere de evidență se iau în evidență cantitativ (spre exemplu: conform numărului de unități, conform greutateii). Cele care se păstrează în ambalaj sigilat se iau în evidență conform numerelor de inventar aplicate pe marcajul ambalajului.

631. Numerotarea articolelor secrete se efectuează de către producător în modul care ar exclude posibilitatea de determinare a cantității totale a articolelor fabricate.

632. Modul de marcare a articolelor secrete se determină de comun acord cu beneficiarul.

633. Evidența articolelor secrete se efectuează conform registrelor luate în evidență de către Subdiviziunile de protecție. Termenul de păstrare a acestor registre este de cel puțin 5 ani. În documentele de evidență pot fi indicate numai denumirile sau semnele convenționale ale articolelor secrete.

634. Evidența, păstrarea și controlul asupra circulației articolelor secrete în subdiviziunile autorității publice sau ale altei persoane juridice se efectuează de către reprezentanții Subdiviziunii de protecție.

635. Șefii subdiviziunilor și reprezentanții Subdiviziunii de protecție poartă răspundere personală pentru organizarea și efectuarea evidenței corespunzătoare a articolelor și documentației tehnice secrete în subdiviziuni și la locurile de muncă.

636. Dacă la proiectarea și fabricarea articolelor secrete sînt antrenate mai multe subdiviziuni, atunci se efectuează evidența centralizată a acestor articole, asigurînd controlul asupra circulației

fiecărui articol secret în subdiviziuni, din momentul înregistrării și pînă la radierea din evidență.

637. Evidența centralizată se efectuează de către subdiviziunile de protecție. Reprezentanții Subdiviziunii de protecție din cadrul subdiviziunilor de producție informează regulat Subdiviziunea de protecție despre circulația articolelor, pentru efectuarea înscrierilor corespunzătoare în Registrul de evidență a articolelor secrete (forma nr.58, anexă la prezentul Regulament) sau în Registrul (Fișa) de evidență numerică a articolelor secrete (forma nr.59, anexă la prezentul Regulament).

638. Articolele se eliberează executanților la locul de muncă în bază de semnătură (recipisă) în Registrul de evidență a articolelor secrete sau în Fișa de evidență pe articol (forma nr.60, anexă la prezentul Regulament).

639. În cazul în care în baza particularităților procesului tehnologic de producție (producere în masă) eliberarea contra semnătură a articolelor secrete executanților este imposibilă din cauza timpului redus de executare a operațiunilor de către aceștia, în subdiviziuni (unități, sectoare) se numesc reprezentanți ai subdiviziunilor de protecție. Reprezentanții subdiviziunilor de protecție primesc articolele contra semnătură (recipisă) în Contul personal (forma nr.29, anexă la prezentul Regulament) sau în Registrul de evidență privind eliberarea articolelor (forma nr.61, anexă la prezentul Regulament) la locul de muncă, efectuînd controlul asupra disponibilului și circulației acestora.

640. Transmiterea articolelor de la un sector de producție la altul se efectuează potrivit registrului din forma nr.62, anexă la prezentul Regulament, care este ținut în subdiviziunea respectivă de reprezentanții Subdiviziunii de protecție și servește drept bază pentru anularea semnăturii de primire a articolelor în Registrul de evidență privind eliberarea articolelor sau în Contul personal și plasarea fișelor de evidență pe articol dintr-un sector al fișierului în altul.

641. Predarea articolelor secrete pe schimburi se efectuează de persoanele responsabile pentru evidența și păstrarea lor, contra semnătură (recipisă). Disponibilul articolelor predate se verifică conform unităților, după numere sau greutate.

642. Predarea articolelor secrete dintr-o subdiviziune în alta se efectuează prin intermediul reprezentantului Subdiviziunii de protecție, în baza sarcinii (planului) de producție, conform Foi de însoțire (forma nr.63, anexă la prezentul Regulament), cu informarea Subdiviziunii de protecție despre acest fapt.

643. Schițele și documentația tehnică, de cercetare științifică, precum și altă documentație prevăzută pentru crearea articolelor secrete se eliberează la locurile de muncă contra semnătură (recipisă) și numai pentru orele de muncă ale schimbului.

644. Se interzice predarea articolelor și documentației tehnice secrete sau altei documentații secrete ce se referă la aceste articole dintr-o subdiviziune în alta, eludînd Subdiviziunea de protecție sau reprezentanții acesteia.

645. Pentru montarea blocurilor, rețelelor și detaliilor secrete în articole se întocmește un proces-verbal, conform formei nr.64, anexă la prezentul Regulament, într-un singur exemplar, care se aprobă de șeful subdiviziunii, iar la experimentări – de către conducătorul tehnic sau de constructorul principal. Numerele de evidență ale blocurilor, rețelelor și detaliilor se înscriu în pașaportul tehnic (formularul) al articolului. Procesele-verbale și înscrierile efectuate în pașapoartele tehnice (formulare) se confirmă prin semnătura persoanelor responsabile de montare. În cazul retragerii sau înlocuirii elementelor secrete de completare se întocmește un proces-verbal, conform formei nr.65, anexă la prezentul Regulament, care servește temei pentru luarea în evidență a articolului sau pentru includerea lui în procesul-verbal cu privire la distrugere.

646. În cazul în care, conform condițiilor de fabricare, în timpul schimbului de muncă se efectuează de mai multe ori montarea și retragerea elementelor secrete de completare cu scopul de a obține caracteristicile necesare ale articolului în care ele se montează, procesul-verbal cu privire la montare se întocmește numai pentru elementul montat definitiv, iar apoi se fac înscrierile respective în documentele luate în evidență.

647. Persoanele care au efectuat montarea elementelor de completare, imediat după întocmirea procesului-verbal respectiv, sînt obligate să predea elementele nepotrivite reprezentantului Subdiviziunii de protecție.

648. Pentru toate articolele secrete sau lotul de articole secrete fabricate se întocmesc pașapoarte tehnice. Dacă datele înscrise în pașaportul tehnic conțin informații secrete, atunci acestuia i se atribuie parafa de secretizare respectivă și numărul din Registrul evidenței de inventar a documentației tehnice secrete, care se înscrie în registrele respective, în care a fost luat în evidență articolul (Registrul de evidență a articolelor secrete sau Registrul (Fișa) de evidență numerică a articolelor secrete).

649. Efectuarea ștersăturilor în orice formă în documentația cu privire la evidența articolelor secrete nu se admite. În caz de necesitate, operarea unor modificări în această documentație se legalizează prin semnătura persoanei care le-a efectuat, cu indicarea datei.

650. Articolele secrete se radiază din evidență la transmiterea lor în alte autorități publice sau persoane juridice, distrugerea acestora, consumarea lor în procesul testărilor și altor lucrări, montării lor în alte articole sau la desecretizarea acestora.

651. Temei pentru radierea articolului secret din evidență servește:

- 1) recipisa destinatarului în foaia de însoțire, legalizată prin ștampilă sau confirmată prin procura de primire a documentelor secrete;
- 2) procesul-verbal cu privire la distrugerea articolelor secrete;
- 3) procesul-verbal cu privire la consumarea articolelor secrete în timpul efectuării lucrărilor de testare și a altor lucrări;
- 4) procesul-verbal cu privire la montarea articolelor de completare;
- 5) decizia cu privire la desecretizare.

Secțiunea a 3-a

Păstrarea articolelor secrete

652. Articolele secrete se păstrează în încăperi (depozite, arhive, încăperi accesorii) care corespund cerințelor prezentului Regulament.

653. Articolele secrete se păstrează separat de cele nesecrete. În cazurile în care articolele nesecrete constituie o parte a articolului secret, ele pot fi păstrate împreună cu articolele secrete.

654. În încăperile unde se păstrează articolele secrete, accesul persoanelor care nu lucrează aici, dar care dispun de dreptul de acces la secret de stat de forma corespunzătoare, se înfăptuiește în modul următor:

- 1) în depozitele din secție și depozitele uzinei – conform listei aprobate de șeful secției sau depozitului respectiv, coordonate cu șeful Subdiviziunii de protecție;
- 2) în depozitele de producție finită având gradul de secretizare “Strict secret” – cu permisiunea scrisă a conducătorului persoanei juridice.

655. În procesul activității sau a testării se permite păstrarea articolelor secrete la locurile de muncă, sub responsabilitatea executanților și a șefilor subdiviziunilor respective de producție.

656. În afara orelor de muncă, articolele secrete trebuie păstrate în depozite speciale, care se încuie și se sigilează de către persoanele responsabile pentru păstrarea lor.

657. Depozitele destinate pentru păstrarea producției cu gradul de secretizare “Strict secret” trebuie să fie amplasate în locuri separate, izolate de sarcinile de producție, înzestrate cu mijloace tehnice de pază, comunicație și antiincendiar.

658. În afara programului de lucru, la locurile de muncă sau pe standurile de testare pot să rămână articolele a căror testare tehnologică sau operațiune nu poate fi întreruptă, precum și articolele de gabarit mare. Ele trebuie să se păstreze în adăposturi montabile-demontabile de metal, lemn, cauciuc, prelată sau în alte adăposturi sigilate, care ar asigura integritatea și camuflarea acestora.

659. Lista articolelor secrete cu indicarea locurilor de păstrare a acestora se aprobă de către șeful autorității publice sau al altei persoane juridice, după coordonarea cu șeful Subdiviziunii de protecție.

Secțiunea a 4-a

Primirea și transmiterea articolelor secrete

660. Reprezentanții autorităților publice sau ai altor persoane juridice, destinatari ai articolelor secrete, trebuie să aibă procură, perfectată în modul stabilit, legalizată prin ștampila autorității sau a altei

persoane juridice respective. Procurile sînt vizate de cître șeful Subdiviziunii de protecție.

661. Primirea (predarea) articolelor secrete se efectuează în baza Foii de însoțire (forma nr.66, anexă la prezentul Regulament), actului de predare-primire și altor documente de însoțire, verificîndu-se în mod obligatoriu integritatea ambalajului și a plumburilor. Numărul de plumburi, a cleștelor de plumbuit și descrierea amprentelor acestora se indică în documentele de însoțire.

662. La depistarea semnelor de deschidere a vagoanelor, a ambalajului sau în cazul unor defecte ale amprentelor sigiliilor (plumburilor), persoanele care efectuează primirea (predarea) articolelor secrete întocmesc un proces-verbal. Faptele enunțate se comunică imediat expeditorului, autorității cu împuterniciri de dispoziție asupra acestor informații și Serviciului de Informații și Securitate.

663. Deschiderea coletelor și a ambalajului, confruntarea articolelor secrete primite cu informația indicată în documentele de însoțire, verificarea stării și integrității acestora se efectuează de cître persoanele responsabile de evidența și păstrarea articolelor secrete și de cître reprezentanții subdiviziunii controlului tehnic.

664. Dacă în procesul verificării se depistează lipsa unor articole sau încălcarea integrității acestora, atunci se întocmește un proces-verbal, un exemplar fiind remis expeditorului pentru întreprinderea măsurilor de rigoare.

665. Autoritățile publice sau alte persoane juridice care au primit din greșeală articole secrete ce nu le aparțin sînt obligate să le primească spre păstrare provizorie, dacă stabilirea adresei destinatarului și expedierea imediată a acestora potrivit destinației nu este posibilă. Deschiderea ambalajului unor astfel de articole este interzisă.

666. În cazul în care în baza documentelor de însoțire nu se poate determina caracterul articolelor secrete primite din greșeală sau pericolul de explozie al acestora, atunci păstrarea lor pînă la momentul transmiterii se va face separat de alte articole.

667. Transmiterea articolelor secrete se efectuează cu permisiunea scrisă a conducătorului autorității publice sau al altei persoane juridice, conform foii de însoțire.

668. Pentru comanda mijloacelor de transport și a corpului de pază, necesare pentru însoțirea articolelor în timpul transportării, se eliberează dispoziția de expediere pentru livrarea articolelor secrete, conform formei nr.67, anexă la prezentul Regulament.

669. Drept temei pentru scoaterea articolelor secrete de pe teritoriul păzit al autorității publice sau al altei persoane juridice servește permisul special semnat de cître șeful de producție, șeful secției și șeful Subdiviziunii de protecție, în baza foii de însoțire și dispoziției de expediere pentru livrarea articolelor secrete.

670. Documentația de exploatare și reparație necesară pentru articolele secrete transmise se expediază prin poșta specială, concomitent cu articolele. În anumite cazuri se admite expedierea acestei documentații prin intermediul persoanei care însoțește articolele secrete și are procură întocmită în modul stabilit de prezentul Regulament.

671. La transmiterea articolelor secrete, în documentele de însoțire (spre exemplu, scrisori de însoțire, foi de ambalaj (forma nr.68, anexă la prezentul Regulament), pașapoarte tehnice) trebuie să fie înscrise acele denumiri sau semne convenționale ale articolelor care sînt indicate în marcările lor.

672. În documentele de transport și financiar-contabile se indică denumirile sau semnele convenționale ale articolelor și numărul acestora. Pentru confirmarea transmiterii încărcăturii, pe aceste documente se indică numerele de ieșire ale documentelor de însoțire.

Secțiunea a 5-a

Transportarea articolelor secrete

673. Transportarea articolelor secrete, coletelor poștale cu valoare declarată, încasărilor și corespondenței speciale se efectuează de cître persoanele responsabile care au drept de acces la secretul de stat de forma respectivă, numite de conducătorii autorităților publice sau ai altor persoane juridice.

674. Persoanele responsabile de transportarea articolelor secrete, coletelor poștale cu valoare declarată, încasărilor și corespondenței speciale trebuie să cunoască și să respecte cu strictețe regulile

de pază și tehnica securității, să păstreze caracterul secret în procesul transportării.

675. Locurile destinate pentru lucrările de încărcare-descărcare a articolelor secrete trebuie să fie protejate sigur, pentru a exclude posibilitatea examinării vizuale sau prin mijloace tehnice de către persoane străine.

676. Articolele secrete supuse transportării trebuie să fie împachetate în așa fel încât să se excludă posibilitatea determinării caracterului acestora. În același mod vor fi împachetate și articolele nesecrete transportate, dispozitivele, utilajul, care după aspectul lor exterior pot determina caracterul articolelor secrete pentru care sînt destinate.

677. Vagoanele destinate transportării articolelor secrete nu trebuie să se deosebească, după aspectul lor exterior, de vagoanele destinate transportării articolelor nesecrete.

678. Pe vagoanele în care sînt transportate articolele secrete nu se scrie denumirea stațiilor de plecare și de destinație, denumirea încărcăturilor și a destinatarilor.

679. Paza înarmată a articolelor secrete la transportare se va asigura în funcție de gradul de secretizare a acestora.

680. Călătoria unor persoane străine împreună cu încărcătura păzită este interzisă.

681. Distribuirea articolelor secrete, coletelor poștale cu valoare declarată, încasărilor și corespondenței speciale prin intermediul Serviciului de Stat de Curieri Speciali se efectuează în modul stabilit de prezentul Regulament.

Secțiunea a 6-a

Testarea articolelor secrete

682. Testarea articolelor secrete se efectuează în locuri special repartizate în aceste scopuri, care se asigură cu pază.

683. Pînă la începerea lucrărilor de testare se iau măsuri în vederea excluderii posibilității de examinare vizuală sau prin mijloace tehnice, de către persoane străine, a articolelor secrete supuse testărilor și a rezultatelor acestora.

684. Acțiunile concrete cu privire la asigurarea regimului secret pe parcursul testărilor, precum și cerințele privind eficacitatea acestora se includ în programele de testări.

685. La lucrările de testare a articolelor secrete pot asista numai persoanele cu drept de acces la secretul de stat, care au atribuție directă la acestea.

686. Participanții la testări pot lua cunoștință numai de acele informații cu privire la caracterul și rezultatul testărilor care se referă nemijlocit la activitatea îndeplinită de către ei în cadrul testării respective.

687. Documentația de construcție și exploatare a articolelor secrete trebuie să conțină metode de verificare și indicații cu privire la pregătirea aparatelor de măsurat, care în timpul măsurării (testării) parametrilor articolelor secrete nu ar dezvălui conținutul informațiilor secrete, neprevăzute de verificare.

688. Punerea în funcțiune de probă, testarea și exploatarea articolelor secrete trebuie să se efectueze în condiții care ar exclude pierderea eventuală a informației secrete prin canale tehnice.

689. Pentru articolele secrete consumate în procesul testărilor sau al altor lucrări experimentale se întocmește un proces-verbal, care servește temei pentru trecerea acestora la pierderi și radierea din evidență.

690. Dacă în baza resturilor inutilizabile de la articolele secrete pot fi determinate caracteristicile secrete sau destinația specială a articolelor respective, aceste resturi se supun distrugerii. În acest scop, la finisarea testării se va examina locul de testare a articolelor secrete pentru identificarea și distrugerea resturilor respective, iar cu privire la rezultatele acestei examinări se va întocmi un proces-verbal.

691. În timpul testărilor, comisiile de stat (de recepție) apreciază eficacitatea acțiunilor cu privire la asigurarea caracterului secret al acestora, reflectînd rezultatele acestei aprecieri în documentele de dare de seamă.

Secțiunea a 7-a

Distrugerea articolelor secrete

692. Sînt supuse distrugerii articolele secrete rebutate în procesul de producție, de testare și de exploatare sau articolele secrete care și-au pierdut necesitatea practică.

693. Selectarea și distrugerea articolelor secrete se efectuează de către o comisie special instituită în acest scop, cu participarea unui angajat sau reprezentant al Subdiviziunii de protecție, în baza unui proces-verbal cu privire la distrugerea articolelor secrete (forma nr.69, anexă la prezentul Regulament).

694. Procesul-verbal de distrugere a articolelor secrete se aprobă de către conducătorul autorității publice sau al altei persoane juridice, iar în unele cazuri, cu permisiunea acestuia – de către șefii subdiviziunilor de producție.

695. După aprobarea procesului-verbal, distrugerea articolelor secrete (demontarea, desfacerea, distrugerea sau deformarea) se efectuează conform tehnologiei menționate de elaborator în pașaportul tehnic al articolului secret. Modalitatea de distrugere a articolelor secrete trebuie să facă imposibilă restabilirea caracteristicilor autentice, parametrilor sau destinației lor speciale.

696. Faptul distrugerii se consemnează în procesul-verbal, prin semnăturile persoanelor care au efectuat distrugerea.

697. Pașapoartele tehnice ale articolelor secrete distruse la fel sînt supuse distrugerii, în modul stabilit de prezentul Regulament, cu consemnarea acestui fapt în procesul-verbal cu privire la distrugerea articolelor secrete.

698. În procesul-verbal cu privire la distrugerea articolelor secrete se reflectă, de asemenea, faptul retragerii pieselor de completare secrete utilizabile din articolele distruse, care se iau în evidența corespunzătoare.

699. Blocurile, detaliile și materialele nesecrete utilizabile pot fi retrase din articolele secrete supuse distrugerii și transmise, conform foilor de însoțire, la depozitele generale pentru utilizarea lor ulterioară în procesul de producție.

700. Din articolele secrete supuse distrugerii se retrag, în mod obligatoriu, metalele prețioase.

701. Procesele-verbale cu privire la distrugerea articolelor secrete se păstrează în dosare speciale cel puțin 5 ani. Gradul de secretizare a acestora se determină în funcție de informațiile pe care le conțin.

Capitolul VII

REGULI DE OPERARE CU CORESPONDENȚA CIFRATĂ ÎN AUTORITĂȚILE PUBLICE SAU ALTE PERSOANE JURIDICE

Secțiunea 1

Dispoziții generale

702. Utilizarea mijloacelor de comunicații cifrate se admite numai în cazul în care nu există posibilitate sau nu este rațional a transmite informația urgentă referitor la problemele secrete, precum și informația urgentă nesecretă interzisă de a fi transmisă în formă deschisă prin mijloace tehnice neprotejate, prin intermediul altor mijloace de comunicație.

703. Organizarea și efectuarea întregului complex de lucrări ce țin de corespondența cifrată se pune în sarcina organelor de cifrare ale autorităților publice sau ale altor persoane juridice – subdiviziuni, amenajate cu aparatajul respectiv (mijloace de comunicații cifrate).

704. Organizarea, funcțiile, drepturile, obligațiile organelor de cifrare se stabilesc în regulamentul de funcționare al acestora, elaborat în conformitate cu cerințele prezentului Regulament, coordonat cu Serviciul de Informații și Securitate și aprobat de conducătorul autorității publice sau al altei persoane juridice.

705. Crearea, reorganizarea și lichidarea organelor de cifrare se efectuează în baza deciziei (ordinului) conducătorilor autorităților publice sau a altor persoane juridice, prin coordonare cu Serviciul de Informații și Securitate. La crearea noilor organe de cifrare, Serviciul de Informații și Securitate verifică existența condițiilor necesare pentru asigurarea regimului secret la organizarea lucrărilor cu corespondența cifrată a acestora.

706. În funcție de specificul activității și volumul informațiilor vehiculate, în cadrul autorităților publice sau al altor persoane juridice lucrările ce țin de corespondența cifrată pot fi realizate de către o

persoană numită special de către conducătorii acestora. În acest caz, atribuțiile organului de cifrare vor fi îndeplinite de această persoană, care va efectua primirea și transmiterea corespondenței cifrate nemijlocit, prin utilizarea aparatului respectiv.

707. În autoritățile publice sau alte persoane juridice în care lipsesc organele de cifrare lucrările ce se referă la corespondența cifrată (întocmire, evidență, utilizare, transmitere, păstrare și distrugerea mesajelor cifrate) se pun în sarcina Subdiviziunii de protecție a acestora. Ultima efectuează primirea și transmiterea corespondenței cifrate, prin intermediul organelor de cifrare ale altor autorități publice sau persoane juridice.

Secțiunea a 2-a

Reguli generale de operare cu corespondența cifrată în autoritățile publice sau alte persoane juridice în care lipsesc organele de cifrare

708. Modul de întocmire, evidență, utilizare, transmitere, păstrare și distrugere a mesajelor cifrate trebuie să asigure integritatea acestora și să excludă posibilitatea divulgării informațiilor ce le conțin.

709. Evidența și păstrarea mesajelor cifrate, precum și aducerea conținutului acestora la cunoștința persoanelor cărora le sînt adresate și executanților se efectuează de către șeful Subdiviziunii de protecție sau de o persoană desemnată din cadrul acesteia.

710. Mesajele cifrate, registrele de evidență și alte documente ce se referă la corespondența cifrată se păstrează de către Subdiviziunea de protecție în safeuri sau dulapuri de metal.

711. Acces la mesajele cifrate avînd gradele de secretizare "Strict secret", "Secret", "Confidențial", "Restricționat" au doar persoanele care, potrivit caracterului obligațiilor de serviciu, au atribuție nemijlocită la acestea și dispun de dreptul de acces la secretul de stat de forma respectivă. Numărul acestor persoane trebuie să fie limitat.

712. Subdiviziunea de protecție deține lista persoanelor care au acces la lucrul cu corespondența cifrată, aprobată de conducătorul autorității publice sau al altei persoane juridice, în care se menționează, inclusiv, persoanele cu drept de a semna mesajele cifrate de ieșire. La necesitate, lista se actualizează în cel mai scurt termen posibil.

713. La prelucrarea mesajelor cifrate, persoanele sînt admise numai după un instructaj detaliat și după familiarizarea, contra semnătură, cu procedura de utilizare a mesajelor cifrate.

714. Persoanele care lucrează cu mesajele cifrate nu au dreptul să divulge informațiile cunoscute din corespondența cifrată, să poarte discuții cu privire la conținutul mesajelor cifrate, în cazul utilizării canalelor de comunicații neprotejate, să păstreze la sine ciornele mesajelor cifrate, să facă înscrisuri neautorizate despre conținutul mesajelor cifrate în caiete de lucru, carnete, pe file neînregistrate, să transmită unul și același text al mesajului în mod deschis și cifrat.

715. Executanții și reprezentanții altor autorități publice sau persoane juridice pot lua cunoștință de conținutul mesajelor cifrate numai conform indicației în scris a destinatarului sau a persoanelor care au semnat mesajul cifrat. Reprezentanții altor autorități publice sau persoane juridice trebuie să prezinte certificatul de acces de forma respectivă și actele de identificare.

716. Conținutul mesajelor cifrate poate fi făcut public în cadrul ședințelor, adunărilor, a altor întruniri, numai dacă toți participanții la acestea au dreptul de acces la secretul de stat de forma respectivă.

717. Se interzice a face referire la faptul că informațiile sînt primite prin corespondență cifrată.

718. Controlul asupra respectării regulilor cu privire la întocmirea, evidența, păstrarea, utilizarea corespondenței cifrate în cadrul autorităților publice și altor persoane juridice se asigură de către subdiviziunile de protecție și conducătorii acestora.

719. Verificarea disponibilului mesajelor cifrate în autoritățile publice și alte persoane juridice se efectuează în modul stabilit pentru documentele secrete.

Secțiunea a 3-a

Reguli de transmitere a mesajelor cifrate în autoritățile publice sau alte persoane juridice care nu dispun de organe de cifrare

720. Întocmirea mesajelor cifrate de ieșire (forma nr.70, anexă la prezentul Regulament) se efectuează în condiții care exclud posibilitatea divulgării conținutului acestora unor persoane care nu au atribuție la ele.

721. Dreptul de a semna mesajele cifrate de ieșire se acordă conducătorilor autorităților publice sau ai altor persoane juridice, adjuncților acestora sau, cu permisiunea conducătorilor, altor persoane cu funcții de conducere (șefi de subdiviziuni).

722. Semnătura persoanei cu funcție de răspundere de pe mesajul cifrat de ieșire, remisă pentru transmitere organului de cifrare al altei autorități publice sau persoane juridice, se legalizează prin ștampila autorității publice sau persoanei juridice respective.

723. Mesajele cifrate de ieșire se scriu de mână sau cu utilizarea mijloacelor tehnice pe blanchete, ținute în evidență prealabilă, într-un singur exemplar, lizibil, succint, fără utilizarea prescurtărilor libere ale cuvintelor. Se admite întocmirea mesajelor cifrate pe file luate în evidență de către Subdiviziunea de protecție, pe care se va aplica mențiunea "Mesaj cifrat". Sub formularul sau fila pe care se întocmește mesajul cifrat trebuie să fie plasat un suport rigid (garnitură), care ar exclude imprimarea textului mesajului pe alte formulare sau file. La întocmirea mesajelor cifrate cu utilizarea mijloacelor tehnice, suportul rigid (garnitura) nu se folosește.

724. Se interzice întocmirea mesajelor cifrate în câteva exemplare, precum și multiplicarea acestora.

725. Toate rectificările și completările operate în text se stipulează și se legalizează prin semnătura executantului sau a persoanei care semnează mesajul cifrat.

726. Mesajele cifrate de ieșire, întocmite ilizibil, inclusiv cele care conțin rectificări nestipulate, nu sînt admise pentru expediere.

727. Blanchetele destinate pentru întocmirea mesajelor cifrate se broșează în carnete, care se trec în evidență în Registrul de evidență a caietelor de lucru. Filele acestor carnete se numerează. Eliberarea carnetelor sau a unor blanchete aparte executanților, precum și restituirea acestora Subdiviziunii de protecție se efectuează contra semnătură (recipisă) în registrul de evidență.

728. Pe mesajele cifrate de ieșire se aplică parafa de secretizare, mențiunea cu privire la caracterul urgent (prioritar) al mesajului cifrat, numele, prenumele, funcția destinatarului, numele, prenumele, funcția persoanei care a semnat mesajul cifrat, data semnării, numărul de înregistrare, numele, prenumele executantului.

729. Gradul de secretizare și caracterul urgent se determină de către executant sau persoana care a semnat mesajul cifrat.

730. Mesajele cifrate de ieșire, transmise la doi și mai mulți destinatari, se întocmesc într-un singur exemplar, cu indicarea tuturor destinatarilor. În caz de necesitate (cînd există mai mulți destinatari), pe verso mesajului cifrat sau pe o foaie separată se întocmește lista de expediere, care se legalizează prin semnătura executantului sau a persoanei care semnează mesajul cifrat.

731. Mesajele cifrate, care conțin informații secretizate cu parafa "Strict secret", se transmit prin intermediul organelor de cifrare ale altor autorități publice sau persoane juridice numai în cazuri excepționale, la indicația scrisă a conducătorului autorității publice sau persoanei juridice care le-a semnat.

732. Întocmirea mesajelor cifrate de ieșire avînd gradul de secretizare "Strict secret" poate fi efectuată doar cu permisiunea conducătorului autorității publice sau al altei persoane juridice. Acestea se înregistrează în Subdiviziunea de protecție, fiind comunicate de executant.

733. Pentru a fi transmise către anumiți destinatari, mesajele cifrate avînd gradul de secretizare "Strict secret" se prezintă Subdiviziunii de protecție în plicuri sigilate, care conțin, după caz, pe lîngă parafa de secretizare, și mențiunea "Personal" sau "Strict personal".

734. Mesajele cifrate de ieșire se predau de către executant Subdiviziunii de protecție. Blanchetele și filele luate în evidență, deteriorate în procesul întocmirii mesajelor cifrate, se restituie Subdiviziunii de protecție pentru a fi distruse în modul stabilit de prezentul Regulament.

735. Mesajele cifrate de ieșire se înregistrează în Registrul de evidență a mesajelor transmise (forma nr.71, anexă la prezentul Regulament).

736. După înregistrare, mesajele se transmit imediat organului de cifrare respectiv, într-un plic sigilat.

737. Pe plic se indică adresa destinatarului și a expeditorului, numărul mesajului cifrat, parafa de secretizare, mențiunea cu privire la caracterul urgent (prioritar) al mesajului și mențiunea "Mesaj cifrat". După cifrare, mesajele destinate transmiterii rămân la organul de cifrare.

738. Transmiterea și distribuirea plicurilor cu mesajele cifrate se efectuează în modul stabilit pentru transmiterea și distribuirea documentelor secrete.

Secțiunea a 4-a

Reguli de recepționare a mesajelor cifrate în autoritățile publice sau alte persoane juridice care nu dispun de organe de cifrare

739. Plicurile cu mesajele cifrate primite de autoritățile publice sau alte persoane juridice se înregistrează imediat în Registrul de control al plicurilor și se transmit persoanei responsabile pentru evidența și păstrarea corespondenței cifrate, contra semnătură (recipisă) în acest registru, indicându-se data și ora primirii plicului.

740. După deschiderea plicurilor, mesajele cifrate se înregistrează în Registrul de evidență a mesajelor cifrate primite (forma nr.72, anexă la prezentul Regulament). Dacă în plic există câteva mesaje cifrate, fiecare dintre ele se înregistrează cu un număr de intrare aparte. Se interzice de a comunica și de a transmite executanților mesajele cifrate care nu au fost luate în evidență.

741. Rezoluțiile se aplică nemijlocit pe mesajele cifrate. Aplicarea rezoluțiilor pe file separate nu se admite.

742. Transmiterea mesajelor cifrate în interiorul autorității publice sau al altei persoane juridice se efectuează numai prin intermediul Subdiviziunii de protecție, iar în afara acestora – prin intermediul organului de cifrare.

743. Mesajele cifrate pot avea mențiunile "Personal" sau "Strict personal". Plicurile cu mesajele cifrate cu mențiunea "Personal" se deschid de către destinatar sau de către persoana împuternicită de acesta, iar plicurile cu mențiunea "Strict personal" se deschid numai de către destinatar și doar ca excepție (în cazul în care lipsește destinatarul) pot fi deschise de către persoana care-l înlocuiește. În registrul de evidență a mesajelor cifrate primite se înscrie: "Plic cu mențiunea "Personal" sau "Plic cu mențiunea "Strict personal". Alte mențiuni cu privire la mesajele cifrate se efectuează în registru din spusele destinatarului sau executantului. Ștampila de înregistrare se aplică pe plic, indicându-se numărul de intrare și data. Persoana care deschide plicul trece aceste date pe mesajul cifrat.

744. Informarea cu conținutul mesajelor cifrate care au gradul de secretizare "Strict secret" se permite doar cu permisiunea scrisă a conducătorului autorității publice sau al altei persoane juridice, numai a persoanelor care au nevoie să cunoască conținutul acestora, reieșind din atribuțiile exercitate și care au drept de acces la secretul de stat de forma respectivă.

745. Eliberarea mesajelor cifrate executanților pentru lucru și recepționarea acestora se efectuează contra semnătură (recipisă) în Registrul de evidență a mesajelor cifrate primite. Se interzice de a transmite mesajele cifrate de la unii executanți către alții, cu eludarea Subdiviziunii de protecție.

746. Persoanele care au luat cunoștință de conținutul mesajelor cifrate semnează lizibil pe acestea, indicând data, după caz, ora când au luat cunoștință.

747. Pe mesajele cifrate, executanții sînt obligați să facă însemnări cu privire la executarea acestora, pe care le confirmă prin semnătură, indicând data, după caz, ora executării.

748. După dispariția necesității de a lucra cu mesajele cifrate, acestea se restituie imediat Subdiviziunii de protecție.

749. Mesajele cifrate se clasează în dosare numai cu însemnările respective privind executarea lor.

750. Din conținutul mesajelor cifrate, cu excepția celor avînd gradul de secretizare "Strict secret", pot fi efectuate însemnări succinte în carnete speciale cu file detașabile. Aceste carnete se iau în evidență de către Subdiviziunea de protecție și se eliberează executanților contra semnătură. Filele carnetelor speciale ce conțin înscrisuri inutilizabile în activitatea ulterioară se extrag periodic și se distrug.

751. În caz de necesitate, reieșind din conținutul mesajelor cifrate de ieșire și de intrare, cu

excepția celor care au gradul de secretizare "Strict secret", pot fi întocmite informații sumare sau extrase care se iau în evidență de către Subdiviziunea de protecție, se păstrează și se distrug în modul stabilit pentru documentele cu gradul de secretizare respectiv.

752. Despre întocmirea informațiilor sau extraselor pe mesajele cifrate respective și în registrele de evidență a acestora se efectuează însemnări cu privire la numărul de exemplare întocmite și numărul de evidență al acestora.

753. Cu permisiunea conducătorilor autorităților publice sau a altor persoane juridice, informațiile ce le conțin mesajele cifrate, cu excepția celor având parafa de secretizare "Strict secret", pot fi incluse în alte documente secrete, cu condiția ca gradul de secretizare a acestora să nu fie mai înalt decât gradul de secretizare a documentelor în care se includ informațiile. Despre includerea acestor informații în documentele secrete, pe mesajele cifrate respective și în registrele de evidență ale acestora, se fac însemnări, indicându-se numerele de evidență ale documentelor în care au fost incluse.

754. Mesajele cifrate de intrare care au fost executate se restituie, în cel mai scurt termen, organelor de cifrare de la care au fost primite. În unele cazuri, atunci când există acordul comun al autorităților publice sau al altor persoane juridice și permisiunea organelor respective ale securității statului, mesajele cifrate, cu excepția celor care au gradul de secretizare "Strict secret", pot fi păstrate de către subdiviziunile de protecție, în dosare aparte. Termenele de păstrare a mesajelor cifrate în autoritățile publice sau alte persoane juridice se determină de către conducătorii acestora și trebuie să fie minime. La dispariția necesității de a lucra în continuare cu mesajele cifrate sau la expirarea termenului de păstrare al acestora, mesajele cifrate se distrug, cu permisiunea conducătorului autorității publice sau al altei persoane juridice, în modul stabilit pentru distrugerea documentelor secrete. Mesajele cifrate având gradul de secretizare "Strict secret" se restituie organului de cifrare.

Capitolul VIII

REGULI DE DESFĂȘURARE A REUNIUNILOR SECRETE

755. Reuniunile de serviciu în cadrul cărora se examinează chestiuni secrete se desfășoară cu permisiunea conducătorilor autorităților publice sau ai altor persoane juridice, care desemnează persoana responsabilă de organizarea unor astfel de reuniuni.

756. Persoana responsabilă de organizarea reuniunilor secrete, în comun cu Subdiviziunea de protecție și specialiștii tehnici respectivi, întreprind măsurile organizatorice și tehnice de securitate, care asigură păstrarea caracterului secret al chestiunilor puse în discuție și exclude posibilitatea de divulgare sau pierdere a informațiilor atribuite la secret de stat în timpul desfășurării acestora. Abordarea chestiunilor secrete curente în cadrul reuniunilor care nu implică reprezentanți ai altor autorități sau persoane juridice poate fi efectuată sub conducerea șefilor de subdiviziuni ai autorității publice sau al altei persoane juridice respective, fără implicarea Subdiviziunii de protecție.

757. Măsurile de securitate se axează în special pe:

1) măsuri de protecție la locul reuniunii pentru a se asigura că aceasta se desfășoară fără nici un incident care ar putea compromite securitatea informațiilor atribuite la secret de stat;

2) controlul personalului care are acces la locul reuniunii și verificarea materialelor introduse în încăperea destinată reuniunii;

3) coordonarea cu autoritățile publice și alte persoane juridice, care urmează să delege participanți la reuniune;

4) stabilirea unor instrucțiuni de securitate (inclusiv a acestora în materialele destinate reuniunii sau comunicarea conținutului acestora participanților).

758. Responsabilitatea pentru asigurarea regimului secret în cadrul reuniunilor secrete o poartă autoritatea publică sau persoana juridică organizatoare.

759. La reuniuni se admit numai persoanele care au acces la secretul de stat de forma corespunzătoare gradului de secretizare a chestiunilor ce urmează a fi puse în discuție. Reprezentanții altor autorități publice sau persoane juridice prezintă, pînă la deschiderea reuniunii, subdiviziunii de protecție a organizatorului certificatele de acces la secretul de stat de forma corespunzătoare.

760. La întocmirea programului (ordinii de zi) privind desfășurarea reuniunii secrete se va ține cont

de succesiunea abordării subiectelor, pentru a exclude participarea la discuție a persoanelor care nu au atribuție sau acces la aceste probleme.

761. Persoana responsabilă de organizarea reuniunii trebuie să prezinte Subdiviziunii de protecție programul de desfășurare a reuniunii și lista participanților cu indicarea numelui, prenumelui, funcției (instituției al cărei reprezentant este) formei de acces, subiectele la abordarea cărora urmează să participe.

762. Lista persoanelor invitate la reuniune este coordonată de către persoana responsabilă de organizarea reuniunii cu Subdiviziunea de protecție și se aprobă de către conducătorul autorității publice sau al altei persoane juridice care a permis desfășurarea reuniunii.

763. Participanții vor fi admiși la reuniune conform listei, la prezentarea actelor de identificare (documentelor de legitimare). Aceștia li se pot elibera permise speciale de acces la reuniune.

764. Materialele secrete necesare pentru desfășurarea reuniunii se expediază persoanelor invitate conform listei aprobate de către conducătorul autorității publice sau al altei persoane juridice care a permis organizarea acesteia. Participanților li se expediază doar acele materiale care țin de chestiunile ce-i vizează nemijlocit. Asigurarea controlului privind restituirea în termen a acestor materiale este pusă în sarcina Subdiviziunii de protecție.

765. Persoana responsabilă de organizarea reuniunii, la deschiderea acesteia, va anunța gradul de secretizare a reuniunii în scopul excluderii posibilității de divulgare a informațiilor și preîntâmpinării participanților despre efectuarea înscrierilor secrete numai în caietele de lucru luate în evidență și eliberate de Subdiviziunea de protecție înainte de începerea reuniunii. În timpul unor întreruperi îndelungate, precum și la finele reuniunii, caietele de lucru se predau subdiviziunii de protecție.

766. Decizia adoptată în cadrul reuniunii, precum și alte documente ce se referă la ea pot fi transmise la adresa participanților, la indicația conducătorului care a permis desfășurarea reuniunii, conform listei de expediere aprobate de către acesta. Dacă documentele în cauză se transmit numai pentru informare, atunci ele trebuie restituite în termenul fixat.

767. Caietele de lucru, predate Subdiviziunii de protecție la finele reuniunii, se transmit la adresa participanților sau se distrug, în modul stabilit de prezentul Regulament.

768. La încheierea lucrărilor, persoana responsabilă de organizarea reuniunii va inspecta încăperea unde aceasta s-a desfășurat, pentru a asigura colectarea tuturor materialelor utilizate la reuniune și a exclude orice posibilitate de acces neautorizat la informațiile atribuite la secret de stat.

Capitolul IX

MĂSURI DE PROTECȚIE FIZICĂ A SECRETULUI DE STAT

769. Obiectivele, sectoarele și locurile în care sînt gestionate informațiile atribuite la secret de stat trebuie protejate fizic împotriva accesului neautorizat.

770. Măsurile de protecție fizică – grilaje la ferestre, încuietori la uși, pază la intrări, sisteme automate pentru supraveghere, control, acces, patrulă de pază, dispozitive de alarmă, mijloace pentru detectarea observării, ascultării sau interceptării, vor fi stabilite în raport cu:

- 1) gradul de secretizare a informațiilor, volumul și localizarea acestora;
- 2) tipul safeurilor, dulapurilor de metal, ambalajelor și altor suporturi în care sînt păstrate (depozitate) informațiile;
- 3) locul de amplasare a spațiilor/locurilor unde se păstrează sau se concentrează informațiile atribuite la secret de stat ori se desfășoară astfel de activități;
- 4) caracteristicile clădirii și zonei de amplasare.

771. Zonele în care sînt manipulate sau stocate informațiile atribuite la secret de stat trebuie organizate și administrate în așa fel încît să corespundă uneia dintre următoarele categorii:

- 1) zonă de securitate clasa I, care presupune că orice persoană aflată în interiorul acesteia are acces la informații atribuite la secret de stat de gradul "Strict secret" și "Secret" și care necesită:
 - a) perimetru clar delimitat și protejat, în care toate intrările și ieșirile sînt supravegheate;
 - b) controlul sistemului de intrare, care să permită numai accesul persoanelor verificate corespunzător și autorizate în mod special;

c) indicarea gradului de secretizare a informațiilor existente în zonă;

2) zonă de securitate clasa a II-a, care presupune gestionarea informațiilor cu gradul de secretizare "Confidențial" și "Restricționat" și se realizează prin aplicarea unor măsuri specifice de protecție împotriva accesului persoanelor neautorizate și care necesită:

a) perimetru clar delimitat și protejat, în care toate intrările și ieșirile sînt supravegheate;

b) controlul sistemului de intrare care să permită accesul neînsoțit numai persoanelor verificate și autorizate să pătrundă în această zonă;

c) reguli de însoțire, supraveghere și prevenire a accesului persoanelor neautorizate la informațiile atribuite la secret de stat.

772. Încăperile în care nu se lucrează zilnic 24 de ore vor fi inspectate imediat după terminarea programului de lucru, pentru a verifica dacă informațiile atribuite la secret de stat sînt asigurate în mod corespunzător.

773. În jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilită o zonă administrativă, cu perimetru vizibil delimitat, în interiorul căreia să existe posibilitatea de control al personalului și al vehiculelor.

774. Accesul în zonele de securitate clasa I și clasa a II-a va fi controlat prin verificarea permisului de acces sau printr-un sistem de recunoaștere individuală aplicat personalului.

775. Autoritățile publice sau alte persoane juridice deținătoare de informații atribuite la secret de stat vor institui un sistem propriu de control al vizitatorilor, destinat interzicerii accesului neautorizat al acestora în zonele de securitate.

776. Permisul de acces nu va specifica, în clar, identitatea autorității publice sau al altei persoane juridice ori locul în care deținătorul are acces.

777. Autoritățile publice sau alte persoane juridice vor organiza, la intrarea sau la ieșirea din zonele de securitate clasa I sau clasa a II-a, controale planificate și inopinate ale bagajelor, incluzînd colete, genți și alte tipuri de suporturi în care s-ar putea transporta materiale și informații atribuite la secret de stat.

778. Personalul inclus în sistemul de pază și apărare a obiectivelor, sectoarelor și locurilor în care sînt gestionate informații atribuite la secret de stat trebuie să dețină autorizație de acces de forma corespunzătoare gradului de secretizare a informațiilor necesare îndeplinirii atribuțiilor ce îi revin.

779. Este interzis accesul necontrolat cu aparate de fotografiat, filmat, înregistrare audio-video, de copiat din baze de date informatice sau de comunicare la distanță în locurile în care se află informații atribuite la secret de stat. Regulamentul privind accesul cu aparate de fotografiat, filmat, înregistrare audio-video, de copiat din bazele de date informatice sau de comunicare la distanță în locurile în care se află informații atribuite la secret de stat se aprobă de către conducătorul autorității publice sau al altei persoane juridice respective.

780. Conducătorii autorităților publice sau ai altor persoane juridice deținătoare de informații atribuite la secret de stat vor stabili reguli cu privire la circulația și ordinea interioară în zonele de securitate, astfel încît accesul să fie permis exclusiv titularilor de autorizații de acces, cu respectarea principiului necesității de a lucra cu informații atribuite la secret de stat.

781. Accesul pentru intervenții tehnice, reparații sau activități de deservire în locurile în care se lucrează cu informații atribuite la secret de stat ori în care se păstrează, se prelucrează sau se multiplică astfel de informații este permis numai angajaților autorității publice sau ai altei persoane juridice, care dețin autorizații de acces de forma corespunzătoare celui mai înalt grad de secretizare a informațiilor pe care le-ar putea cunoaște.

782. Pentru a distinge persoanele care au acces în diferite locuri sau sectoare în care sînt gestionate informații atribuite la secret de stat, acestea pot purta însemne sau echipamente specifice.

783. În locurile și sectoarele în care sînt gestionate informații atribuite la secret de stat, însemnele și echipamentele distinctive se stabilesc prin regulamente de ordine interioară.

784. Evidența legitimațiilor, permiselor și a altor însemne și echipamente distinctive se ține de Subdiviziunea de protecție a autorității publice sau a altei persoane juridice.

785. Persoanele care pierd permisele de acces, însemnele sau echipamentele specifice sînt obligate să anunțe imediat șeful ierarhic superior și subdiviziunea de protecție. Concomitent, faptul

pierderii se aduce la cunoștința conducătorului autorității publice sau al altei persoane juridice.

786. În situațiile menționate în punctul 785 din prezentul Regulament, conducătorul autorității publice sau al altei persoane juridice va dispune investigarea împrejurărilor în care s-au produs și va informa Serviciul de Informații și Securitate.

787. Subdiviziunea de protecție trebuie să întreprindă măsurile ce se impun pentru a preveni folosirea permiselor de acces, însemnelor sau echipamentelor specifice de către persoane neautorizate.

788. Accesul fiecărui angajat al autorității publice sau al altei persoane juridice deținătoare de informații atribuite la secret de stat în zone de securitate clasa I sau clasa a II-a se realizează prin intrări anume stabilite, pe baza permisului de acces, semnat de conducătorul acesteia.

789. Permisele de acces vor fi individuale, prin aplicarea unor semne distinctive.

790. La încetarea activității, permisele de acces se retrag și se anulează.

791. În locurile în care sînt gestionate informații atribuite la secret de stat este interzis accesul altor persoane, în afara celor care dispun de permis de acces.

792. Accesul persoanelor din afara autorității publice sau al altei persoane juridice în zona administrativă sau în zonele de securitate este permis numai dacă sînt însoțite de persoane anume desemnate, cu bilet de intrare eliberat pe baza documentelor de legitimare, de către conducătorul autorității publice sau al altei persoane juridice.

793. Accesul angajaților persoanelor juridice care efectuează lucrări de construcții, reparații și întreținere a clădirilor, instalațiilor sau utilităților în zonele administrative ori în zonele de securitate se realizează cu documente de acces temporar, eliberate de conducătorii autorităților publice sau ai altor persoane juridice beneficiare, pe baza actelor de identitate, la solicitarea reprezentanților autorizați ai persoanelor juridice în cauză.

794. Locurile în care se efectuează lucrările menționate se supraveghează de către persoane anume desemnate din autoritatea publică sau altă persoană juridică beneficiară.

795. Documentul de acces temporar este valabil pe durata executării lucrărilor, iar la finisarea activităților se restituie emitentului.

796. Pierderea documentului de acces temporar va fi luată în evidența Subdiviziunii de protecție, care va dispune măsurile necesare de prevenire a folosirii lui de către persoane neautorizate.

797. Reprezentanții organului abilitat – Serviciul de Informații și Securitate, pot să efectueze controlul privind starea protecției secretului de stat în cadrul autorităților publice și al altor persoane juridice ce au acces la obiectivele, sectoarele și locurile în care sînt gestionate informații atribuite la secret de stat, pe baza legitimației de serviciu și a delegației speciale, semnate de conducătorul organului pe care-l reprezintă.

798. Persoanele aflate la practică, stagii de instruire sau schimb de experiență au acces numai în locurile stabilite de conducătorul autorității publice sau al altei persoane juridice, pe baza permiselor de acces eliberate în acest sens.

799. Persoanele care solicită angajări, audiențe ori care prezintă reclamații și sesizări vor fi primite în afara zonelor administrative sau în locuri special amenajate, cu aprobarea conducătorului autorității publice sau al altei persoane juridice.

800. În caz de necesitate, la decizia conducătorului autorității publice sau al altei persoane juridice respective, în afara orelor de program și în zilele nelucrătoare se vor organiza patrulări pe perimetrul autorității publice sau al altei persoane juridice, la intervale care vor fi stabilite prin instrucțiuni elaborate în baza planului de pază și apărare a obiectivului.

801. Sistemele de pază, supraveghere și control-acces trebuie să asigure prevenirea pătrunderii neautorizate în obiectivele, sectoarele și locurile unde sînt gestionate informații atribuite la secret de stat.

802. Timpul de reacție a personalului de pază și apărare va fi testat periodic, pentru a garanta intervenția operativă în situații de urgență.

803. Autoritățile publice sau alte persoane juridice trebuie să întocmească și să aprobe Programul propriu de prevenire a scurgerii de informații atribuite la secret de stat, conform formei nr.73, anexă la prezentul Regulament, și să asigure aplicarea acestuia. Programul de prevenire a scurgerii de informații atribuite la secret de stat se avizează de Serviciul de Informații și Securitate. De asemenea, autoritățile

publice sau alte persoane juridice care gestionează informații atribuite la secret de stat vor întocmi planul de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită pentru protecția informațiilor atribuite la secret de stat.

804. Planul de pază și apărare menționat va fi înregistrat potrivit celui mai înalt grad de secretizare a informațiilor protejate și va cuprinde totalitatea măsurilor de securitate luate pentru prevenirea accesului neautorizat la acestea.

805. Planul de pază și apărare va fi anexat Programului de prevenire a scurgerii de informații atribuite la secret de stat și va cuprinde:

1) date privind delimitarea și marcarea zonelor de securitate, dispunerea posturilor de pază și măsurile de supraveghere a perimetrului protejat;

2) sistemul de control al accesului în zonele de securitate;

3) măsurile de avertizare și alarmare pentru situații de urgență;

4) planul de evacuare a documentelor și modul de acțiune în caz de urgență;

5) procedura de raportare, investigare și evidență a încălcărilor reglementărilor privind protecția informațiilor atribuite la secret de stat.

806. Informațiile atribuite la secret de stat se păstrează în safeuri, dulapuri de metal, ambalaje și alți suportți speciali, clasificate conform următoarelor clase:

1) clasa A – autorizate la nivel național pentru păstrarea informațiilor secretizate cu parafa “Strict secret” în zona de securitate clasa I;

2) clasa B – autorizate la nivel național pentru păstrarea informațiilor având gradele de secretizare “Secret”, “Confidențial” și “Restricționat” în zone de securitate clasa I sau clasa a II-a;

3) clasa C – mobilier de birou adecvat numai pentru păstrarea informațiilor secretizate cu parafa “Restricționat”.

807. Evidența safeurilor, dulapurilor de metal, ambalajelor și altor suportți speciali, precum și a cheilor de la acestea se ține de către Subdiviziunea de protecție într-un registru special, potrivit formei nr.74, anexă la prezentul Regulament.

808. Safeurile, dulapurile de metal, ambalajele și alți suportți speciali din clasele A și B vor fi construite astfel încât să asigure protecția împotriva pătrunderii clandestine și deteriorării sub orice formă a informațiilor.

809. Cerințele la care trebuie să corespundă safeurile, dulapurile de metal, ambalajele și alți suportți speciali din clasele A și B se elaborează, în conformitate cu standardele naționale și internaționale în vigoare, de către Comisia interdepartamentală pentru protecția secretului de stat în colaborare cu autoritățile administrației publice competente.

810. Încăperile de securitate sînt încăperile special amenajate în zone de securitate clasa I sau clasa a II-a, în care informațiile atribuite la secret de stat pot fi păstrate pe rafturi deschise sau pot fi expuse pe hărți, planșe ori diagrame.

811. Pereții, podelele, plafoanele, ușile și încuietorile încăperilor de securitate vor asigura protecția echivalentă clasei safeurilor, dulapurilor de metal, ambalajelor și altor suportți de securitate aprobate pentru păstrarea informațiilor atribuite la secret de stat, corespunzător gradului de secretizare.

812. Ferestrele încăperilor de securitate dispuse la parter sau ultimul etaj vor fi protejate obligatoriu cu gratii fixate în beton sau asigurate antiefracție.

813. În afara programului de lucru, ușile încăperilor de securitate vor fi sigilate, iar sistemul de ventilare asigurat împotriva accesului neautorizat și introducerii materialelor incendiare.

814. În situații de urgență, dacă informațiile atribuite la secret de stat trebuie evacuate, se vor utiliza ambalaje speciale autorizate la nivel național, din clasa corespunzătoare gradului de secretizare a acestor informații.

815. Încuietorile folosite la safeurile, dulapurile de metal, ambalajele, alți suportți speciali și încăperile de securitate în care sînt păstrate informații atribuite la secret de stat se împart în trei grupe, astfel:

1) grupa A – încuietori autorizate pentru safeurile, dulapurile de metal, ambalajele, alți suportți speciali din clasa A;

2) grupa B – încuietori autorizate pentru safeurile, dulapurile de metal, ambalajele, alți suportți speciali din clasa B;

3) grupa C – încuietori pentru mobilierul de birou (clasa C).

816. Cerințele cărora trebuie să corespundă mecanismele de închidere, sistemele cu cifru și încuietorile, pe grupe de utilizare, se elaborează, în conformitate cu standardele naționale și internaționale în vigoare, de către Comisia interdepartamentală pentru protecția secretului de stat în colaborare cu autoritățile administrației publice competente.

817. Cheile safeurilor, dulapurilor de metal, ambalajelor, altor suportți speciali de securitate și încăperilor de securitate, conform listei aprobate de către conducătorul autorității publice sau al altei persoane juridice respective, nu vor fi scoase din zonele de securitate.

818. În afara orelor de program, cheile de la încăperile, safeurile, dulapurile de metal, ambalajele, alți suportți speciali de securitate, conform listei aprobate de către conducătorul autorității publice sau al altei persoane juridice respective, se păstrează în cutii sigilate de către personalul care asigură paza și apărarea.

819. Predarea și primirea cheilor de la încăperile, safeurile, dulapurile de metal, ambalajele, alți suportți speciali de securitate se face, pe bază de semnătură (recipisă), într-un borderou special destinat, conform formei nr.75, anexă la prezentul Regulament.

820. Pentru situațiile de urgență, un rînd de chei suplimentare sau, după caz, o evidență scrisă a combinațiilor încuietorilor vor fi păstrate în plicuri opace sigilate, în ambalaje separate, într-o subdiviziune stabilă de conducerea autorității publice sau a altei persoane juridice, sub control corespunzător.

821. Evidența fiecărei combinații se va păstra în plic separat.

822. Cheilor și plicurilor cu combinații trebuie să li se asigure gradul de protecție necesar, în baza deciziei conducătorului autorității publice sau al altei persoane juridice respective, același grad de protecție ca și informațiilor la care permit accesul.

823. Combinațiile încuietorilor de la încăperile, safeurile, dulapurile de metal, ambalajele și alți suportți de securitate vor fi cunoscute de un număr restrîns de persoane desemnate de conducerea autorității publice sau a altei persoane juridice.

824. Cheile și combinațiile încuietorilor vor fi schimbate:

- 1) ori de cîte ori are loc o schimbare de personal;
- 2) de fiecare dată cînd se constată că au intervenit situații de natură să le facă vulnerabile;
- 3) la intervale regulate, de preferință o dată la șase luni, fără a se depăși 12 luni.

Cheile și combinațiile încuietorilor vor fi schimbate de fiecare dată cînd se constată că au intervenit situații de natură să le facă vulnerabile. Combinațiile încuietorilor vor fi schimbate la intervale regulate, de preferință o dată la șase luni, fără a se depăși 12 luni, și în caz de schimbare a personalului.

825. Sistemele electronice de alarmare sau de supraveghere destinate protecției informațiilor atribuite la secret de stat vor fi prevăzute cu surse de alimentare de rezervă.

826. Orice defecțiune sau intervenție neautorizată asupra sistemelor de alarmă sau de supraveghere destinate protecției informațiilor atribuite la secret de stat trebuie să avertizeze personalul care le monitorizează.

827. Dispozitivele de alarmare trebuie să intre în funcțiune în cazul penetrării pereților, podelelor, tavanelor și deschizăturilor sau la mișcări în interiorul încăperilor de securitate.

828. Copiatoarele și dispozitivele telefax se vor instala în încăperi special destinate și se vor folosi numai de către persoanele autorizate, potrivit gradului de secretizare a informațiilor la care au acces.

829. Autoritățile publice sau alte persoane juridice deținătoare de informații atribuite la secret de stat au obligația de a asigura protecția acestora împotriva ascultărilor neautorizate, pasive sau active.

830. Protecția împotriva ascultării pasive a discuțiilor secrete se realizează prin izolarea fonică a încăperilor.

831. Protecția împotriva ascultărilor active, prin microfoane, radio-emisători și alte dispozitive implantate, se realizează pe baza inspecțiilor de securitate a încăperilor, accesoriilor, instalațiilor, sistemelor de comunicații, echipamentelor și mobilierului de birou, precum și prin efectuarea măsurilor speciale tehnice (inclusiv utilizarea aparatului special de protecție a convorbirilor), realizate de instituții

specializate, potrivit competențelor legale.

832. Lista încăperilor protejate împotriva ascultărilor trebuie să fie aprobată de către conducătorul autorității publice sau al altei persoane juridice respective. Accesul în încăperile protejate împotriva ascultărilor se va controla în mod special.

833. Periodic, personalul specializat în depistarea dispozitivelor de ascultare va efectua inspecții fizice și tehnice.

834. Inspecțiile fizice și tehnice se organizează, în mod obligatoriu, în urma oricărei intrări neautorizate sau suspiciuni privind accesul persoanelor neautorizate și după executarea lucrărilor de reparații, întreținere, zugrăvire sau redecorare.

835. Nici un obiect nu va fi introdus în încăperile protejate împotriva ascultării, fără a fi verificat în prealabil de către personalul specializat în depistarea dispozitivelor de ascultare.

836. În zonele în care se poartă discuții secrete și care sînt asigurate din punct de vedere tehnic nu se vor instala telefoane, iar dacă instalarea acestora este absolut necesară, acestea trebuie prevăzute cu un dispozitiv de deconectare pasiv. Inspecțiile de securitate tehnică în aceste zone trebuie efectuate, în mod obligatoriu, înaintea începerii convorbirilor, pentru identificarea fizică a dispozitivelor de ascultare și verificarea sistemelor telefonice, electrice sau de altă natură, care ar putea fi utilizate ca mediu de atac.

837. Echipamentele de comunicații și dotările din birouri, în principal cele electrice și electronice, trebuie verificate de specialiști ai organului competent pentru protecția secretului de stat, înainte de a fi folosite în zonele în care se lucrează ori se discută despre informații avînd gradele de secretizare "Strict secret" sau "Secret", pentru a preveni transmiterea sau interceptarea, în afara cadrului legal, a unor informații inteligibile. Pentru aceste zone, la decizia conducătorului autorității publice sau al altei persoane juridice respective, se va organiza o evidență a tipului și numerelor de inventar ale echipamentului și mobilei mutate în/din interiorul încăperilor, care va fi gestionată ca material secret de stat.

Capitolul X

MĂSURI DE PROTECȚIE TEHNICĂ ȘI CRIPTOGRAFICĂ A SECRETULUI DE STAT

Secțiunea 1

Dispoziții generale

838. Modalitățile și măsurile de protecție a informațiilor atribuite la secret de stat, care se prezintă în format electronic, sînt similare celor pe suport de hîrtie.

839. În sensul prezentului capitol se definesc următoarele noțiuni și abrevieri:

1) *INFOSEC* – ansamblul măsurilor și structurilor de protecție a informațiilor atribuite la secret de stat, care sînt prelucrate, păstrate sau transmise prin intermediul sistemelor de comunicații electronice, împotriva amenințărilor și a oricăror acțiuni care pot aduce atingere confidențialității, integrității, disponibilității, autenticității și nerepudierii informațiilor atribuite la secret de stat, precum și afectarea funcționării sistemelor electronice, indiferent dacă acestea apar accidental sau intenționat. Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum și depistarea și prevenirea amenințărilor la care sînt expuse informațiile și sistemele;

2) *informații în format electronic* – texte, date, imagini, sunete, înregistrate pe dispozitive de stocare sau pe suporturi magnetici, optici, electrice ori transmise sub formă de curenți, tensiuni sau cîmp electromagnetic, în eter sau în rețele de comunicații;

3) *sistem de prelucrare automată a datelor (SPAD)* – ansamblul de elemente interdependente în care se includ: echipamentele de calcul, produsele software de bază și aplicative, metodele, procedeele și, dacă este cazul, personalul, organizate astfel încît să asigure îndeplinirea funcțiilor de stocare, prelucrare automată și transmitere a informațiilor în format electronic și care se află sub coordonarea și controlul unei singure autorități. Un SPAD poate să cuprindă subsisteme, iar unele dintre acestea pot fi ele însele SPAD;

4) *componente specifice de securitate ale unui SPAD* – ansamblul de elemente necesare asigurării unui nivel corespunzător de protecție pentru informațiile atribuite la secret de stat, care urmează a fi stocate sau procesate într-un SPAD. Acestea sînt:

- a) funcții și caracteristici hardware/firmware/software;
- b) proceduri de operare și moduri de operare;
- c) proceduri de evidență;
- d) controlul accesului;
- e) definirea zonei de operare a SPAD;
- f) definirea zonei de operare a posturilor de lucru/a terminalelor la distanță;
- g) restricții impuse de politica de management;
- h) structuri fizice și dispozitive;
- i) mijloace de control pentru personal și comunicații;
- j) rețele de transmisii de date (RTD);

5) *rețele de transmisii de date (RTD)* – ansamblul de elemente interdependente în care se includ: echipamente, programe și dispozitive de comunicație, tehnică de calcul hardware și software, metode și proceduri pentru transmisie și recepție de date și controlul rețelei, precum și, dacă este cazul, personalul aferent. Toate acestea sînt organizate astfel încît să asigure îndeplinirea funcțiilor de transmisie a informațiilor în format electronic între două sau mai multe SPAD sau să permită interconectarea cu alte RTD-uri. O RTD poate utiliza serviciile unuia sau mai multor sisteme de comunicații; mai multe RTD pot utiliza serviciile unuia și aceluiași sistem de comunicații. Caracteristicile de securitate ale unei RTD cuprind: caracteristicile de securitate ale sistemelor SPAD individuale conectate, împreună cu toate componentele și facilitățile asociate rețelei – facilități de comunicații ale rețelei, mecanisme și proceduri de identificare și etichetare, controlul accesului, programe și proceduri de control și revizie, necesare pentru asigurarea unui nivel corespunzător de protecție a informațiilor atribuite la secret de stat, care sînt transmise prin intermediul RTD;

6) *RTD locală* – rețea de transmisii de date care interconectează mai multe computere sau echipamente de rețea, situate în același perimetru;

7) *sistem informatic și de comunicații (SIC)* – ansamblu informatic prin intermediul căruia se stochează, se procesează și se transmit informații în format electronic, alcătuit din cel puțin un SPAD, izolat sau conectat la o RTD. SIC poate avea o configurație complexă, formată din mai multe SPAD-uri și/sau RTD-uri interconectate;

8) *securitatea SPAD, RTD și SIC* – aplicarea măsurilor de securitate la SPAD, RTD și SIC cu scopul de a preveni sau împiedica extragerea sau modificarea informațiilor atribuite la secret de stat stocate, procesate, transmise prin intermediul acestora – prin interceptare, alterare, distrugere, accesare neautorizată cu mijloace electronice, precum și invalidarea de servicii sau funcții, prin mijloace specifice;

9) *confidențialitate* – proprietatea informației din cadrul sistemului care caracterizează protecția ei de la accesul neautorizat (asigurarea accesului la informații atribuite la secret de stat a persoanei numai în baza autorizației de acces de forma corespunzătoare gradului de secretizare a informației accesate și în baza principiului necesității de a lucra cu asemenea informații);

10) *integritate* – proprietatea informației din cadrul sistemului, care caracterizează veridicitatea, concordanța și invariabilitatea acesteia, inclusiv în condițiile de acțiune intenționată sau neintenționată cu scopul modificării sau distrugerii acesteia, precum și interdicția modificării prin ștergere sau adăugare ori a distrugerii în mod neautorizat a informațiilor atribuite la secret de stat;

11) *accesibilitate* – proprietatea informației din cadrul sistemului, care caracterizează posibilitatea accesării libere a informației pentru efectuarea operațiunilor sancționate, precum și asigurarea condițiilor necesare regăsirii și utilizării cu ușurință, ori de cîte ori este nevoie, cu respectarea strictă a condițiilor de confidențialitate și integritate a informațiilor atribuite la secret de stat;

12) *autenticitate* – asigurarea posibilității de verificare a identității pe care un utilizator de SPAD sau RTD pretinde că o are;

13) *nerepudiare* – măsură prin care se asigură faptul că, după emiterea/recepționarea unei informații într-un sistem de comunicații securizat, expeditorul/destinatarul nu poate nega, în mod fals, că

a expediat/primit informații;

14) *risc de securitate* – probabilitatea ca o amenințare sau o vulnerabilitate a SPAD sau RTD – SIC să se materializeze în mod efectiv;

15) *management de risc* – activitatea de identificare, control și minimizare a riscurilor de securitate, fiind una continuă de stabilire și menținere a unui nivel de securitate în domeniul tehnologiei informației și comunicațiilor – într-o autoritate publică sau altă persoană juridică, în sensul că, pornind de la analiza de risc, identifică și evaluează amenințările și vulnerabilitățile și propune aplicarea măsurilor adecvate de contracarare, proiectate la un preț de cost corelat cu consecințele care ar decurge din divulgarea, modificarea sau ștergerea informațiilor care trebuie protejate;

16) *regula celor doi* – obligativitatea colaborării a două persoane pentru îndeplinirea unei activități specifice;

17) *produs informatic de securitate* – componentă de securitate care se încorporează într-un SPAD sau RTD – SIC și care servește la sporirea sau asigurarea confidențialității, integrității, accesibilității, autenticității și nerepudierii informațiilor stocate, procesate sau transmise;

18) *securitatea calculatoarelor (COMPUSEC)* – aplicarea la nivelul fiecărui calculator a facilităților de securitate hardware, software și firmware, pentru a preveni divulgarea, utilizarea, modificarea sau ștergerea neautorizată a informațiilor atribuite la secret de stat ori invalidarea neautorizată a unor funcții;

19) *securitatea comunicațiilor (COMSEC)* – aplicarea măsurilor de securitate în telecomunicații, cu scopul de a proteja mesajele dintr-un sistem de telecomunicații, care ar putea fi interceptate, studiate, analizate și, prin reconstituire, pot conduce la divulgarea informațiilor atribuite la secret de stat. COMSEC reprezintă ansamblul de proceduri, incluzând:

- a) măsuri de securitate a transmisiilor;
- b) măsuri de securitate împotriva radiațiilor – TEMPEST;
- c) măsuri de acoperire criptologică;
- d) măsuri de securitate fizică, procedurală, de personal și a documentelor;
- e) măsuri COMPUSEC;

20) *TEMPEST* – ansamblul măsurilor de testare și de realizare a securității împotriva scurgerii de informații, prin intermediul emisiilor electromagnetice parazite;

21) *evaluare* – examinarea detaliată, din punct de vedere tehnic și funcțional, a aspectelor de securitate ale SPAD și RTD – SIC sau a produselor de securitate, de către organul abilitat în acest sens. În procesul de evaluare se verifică:

- a) prezența facilităților/funțiilor de securitate cerute;
- b) absența efectelor secundare compromițătoare care ar putea decurge din implementarea facilităților de securitate;
- c) funcționalitatea globală a sistemului de securitate;
- d) satisfacerea cerințelor de securitate specifice pentru un SPAD și RTD – SIC;
- e) stabilirea nivelului de încredere al SPAD sau RTD – SIC ori al produselor informatice de securitate implementate;
- f) existența performanțelor de securitate ale produselor informatice de securitate instalate în SPAD sau RTD – SIC;

22) *certificare* – emiterea unui document în baza unei evaluări care atestă nivelul de corespundere a mijloacelor de protejare a informațiilor atribuite la secret de stat cu cerințele de protecție a informațiilor având gradul corespunzător de secretizare (măsura în care SPAD și RTD – SIC satisfac cerințele de securitate, precum și măsura în care produsele informatice de securitate corespund exigențelor referitoare la protecția informațiilor atribuite la secret de stat);

23) *zona SPAD* – zona de lucru în care se găsesc și operează unul sau mai multe calculatoare, unități periferice locale și de stocare, mijloace de control și echipament specific de rețea și de comunicații. Zona SPAD nu include zona în care sînt amplasate terminale, echipamente periferice sau stații de lucru la distanță, chiar dacă aceste echipamente sînt conectate la echipamentul central de calcul din zona SPAD;

24) *zona terminal/stație de lucru la distanță* – zona separată de zona SPAD în care se găsesc:

- a) elemente de tehnică de calcul;
- b) echipamentele periferice locale, terminale sau stații de lucru la distanță, conectate la echipamentele din zona SPAD;
- c) echipamente de comunicații;

25) *amenințare* – posibilitatea de compromitere accidentală sau deliberată a securității SPAD sau RTD – SIC, prin pierderea confidențialității, a integrității sau disponibilității informațiilor în format electronic sau prin afectarea funcțiilor care asigură autenticitatea și nerepudierea informațiilor;

26) *vulnerabilitate* – slăbiciune sau lipsă de control care ar putea permite sau facilita o manevră tehnică, procedurală sau operațională, prin care se amenință o valoare sau țintă specifică;

27) *TIC* – tehnologia informației și comunicațiilor.

840. Informațiile care se prezintă în format electronic pot fi:

- 1) stocate și procesate în cadrul SPAD sau transmise prin intermediul RTD;
- 2) stocate și transportate prin intermediul suporturilor de memorie, dispozitivelor electronice – cipuri de memorie, hârtie perforată sau alți suporturi specifici.

841. Încărcarea informațiilor pe mediile prevăzute în punctul 840 subpunctul 2), precum și interpretarea lor pentru a deveni inteligibile se face cu ajutorul echipamentelor electronice specializate.

842. Sistemele SPAD și RTD – SIC au dreptul să stocheze, să proceseze sau să transmită informații atribuite la secret de stat, numai dacă sînt autorizate, conform prezentului Regulament.

843. În vederea autorizării SPAD și RTD – SIC, autoritățile publice și alte persoane juridice vor întocmi, cu aprobarea organelor lor de conducere, strategia proprie de securitate, în baza căreia vor implementa sisteme proprii de securitate, care vor include utilizarea de produse specifice tehnologiei informației și comunicațiilor, personal instruit și măsuri de protecție a informației, incluzînd controlul accesului la sistemele și serviciile informatice și de comunicații, pe baza principiului necesității de a lucra cu informații atribuite la secret de stat și al gradului de secretizare atribuit.

844. SPAD și RTD – SIC vor fi supuse procesului de certificare, urmat de evaluări periodice.

845. Aplicarea reglementărilor în vigoare cu privire la protecția informațiilor atribuite la secret de stat în format electronic funcționează unitar la nivel național. Sistemul de emisie și implementare a măsurilor de securitate adresate protecției informațiilor atribuite la secret de stat, care sînt stocate, procesate sau transmise de SPAD sau RTD – SIC, precum și controlul modului de implementare a măsurilor de securitate se realizează de către organul desemnat la nivel național pentru protecția secretului de stat.

846. Măsurile de protecție a informațiilor atribuite la secret de stat în format electronic trebuie reactualizate permanent, prin depistare, documentare și gestionare a amenințărilor și vulnerabilităților la adresa informațiilor atribuite la secret de stat și a sistemelor care le prelucrează, le stochează și le transmit.

847. Măsurile de securitate INFOSEC sînt structurate după gradul de secretizare a informațiilor pe care le protejează și în conformitate cu conținutul acestora.

848. Conducătorul autorității publice sau al altei persoane juridice deținătoare de informații atribuite la secret de stat răspunde de securitatea propriilor informații care sînt stocate, procesate sau transmise în SPAD sau RTD – SIC.

849. În fiecare autoritate publică sau altă persoană juridică care administrează SPAD și RTD – SIC în care se stochează, se procesează sau se transmit informații atribuite la secret de stat se va institui o structură de securitate pentru tehnologia informației și a comunicațiilor – *SSTIC*, în subordinea Subdiviziunii de protecție.

850. În funcție de volumul de activitate și în cazul în care cerințele de securitate permit, atribuțiile *SSTIC* pot fi îndeplinite numai de către un angajat de securitate TIC sau pot fi preluate, în totalitate, de către Subdiviziunea de protecție.

851. *SSTIC* îndeplinește atribuții privind:

- 1) implementarea metodelor, mijloacelor și măsurilor necesare protecției informațiilor în format electronic;
- 2) exploatarea operațională a SPAD și RTD – SIC în condiții de securitate;

3) coordonarea cooperării dintre autoritatea publică sau altă persoană juridică deținătoare a SPAD sau RTD – SIC și organul competent pentru protecția secretului de stat;

4) implementarea măsurilor de securitate și protecție criptografică ale SPAD sau RTD – SIC.

852. SSTIC reprezintă punctul de contact între organul competent pentru protecția secretului de stat și autoritățile publice sau alte persoane juridice care dețin în administrare SPAD sau RTD – SIC și, după caz, poate fi investită, temporar, de către acesta, cu unele dintre atribuțiile sale.

853. Propunerile pe linie de securitate înaintate de către SSTIC devin aplicabile numai după ce sînt aprobate de către conducerea autorității publice sau al altei persoane juridice care deține în administrare respectivul SPAD sau RTD – SIC.

854. SSTIC se instituie la nivelul fiecărei SPAD și RTD – SIC și reprezintă persoana sau subdiviziunea cu atribuții de implementare a metodelor, mijloacelor și măsurilor de securitate și de exploatare a SPAD și RTD – SIC în condiții de securitate.

855. SSTIC este formată din administratori de securitate, după caz, alți specialiști privind SPAD sau RTD – SIC și condusă de către funcționarul de securitate TIC. Toată structura SSTIC face parte din personalul autorității publice sau al altei persoane juridice care administrează SPAD sau RTD – SIC.

856. Exercițarea atribuțiilor SSTIC trebuie să cuprindă întregul ciclu de viață al SPAD sau RTD – SIC, începînd cu proiectarea, continuînd cu elaborarea pașapoartelor tehnice (specificațiilor, sarcinilor tehnice), testarea instalării, certificarea, testarea periodică, exploatarea operațională, modificarea și încheind cu scoaterea din uz. În anumite situații, rolul SSTIC poate fi preluat de către alte subdiviziuni ale autorității publice sau al altei persoane juridice, în decursul ciclului de viață.

857. SSTIC mijlocește cooperarea dintre conducerea autorității publice sau al altei persoane juridice căreia îi aparține SPAD sau RTD – SIC și organul competent pentru protecția secretului de stat, atunci cînd autoritatea publică sau altă persoană juridică:

1) planifică dezvoltarea sau achiziția de SPAD sau RTD;

2) propune schimbări ale unei configurații de sistem existente;

3) propune conectarea unui SPAD sau a unei RTD – SIC cu un alt SPAD sau RTD – SIC;

4) propune schimbări ale modului de operare de securitate al SPAD sau RTD – SIC;

5) propune schimbări în programele existente sau utilizarea de noi programe, pentru optimizarea securității SPAD sau RTD – SIC;

6) inițiază proceduri de modificare a gradului de secretizare a SPAD și RTD – SIC care au fost deja certificate;

7) planifică sau propune întreprinderea oricărei alte activități referitoare la îmbunătățirea securității SPAD sau RTD – SIC deja certificate.

858. SSTIC, cu aprobarea organului competent pentru protecția secretului de stat, stabilește standardele și procedurile de securitate care trebuie respectate de către furnizorii de echipamente, pe parcursul dezvoltării, instalării și testării SPAD și RTD – SIC și răspunde pentru justificarea, selectarea, implementarea și controlul componentelor de securitate, care fac parte din SPAD și RTD – SIC.

859. SSTIC stabilește, pentru structurile de securitate și management ale SPAD și RTD – SIC, încă de la înființare, responsabilitățile pe care le vor exercita pe tot ciclul de viață al SPAD și RTD – SIC respective.

860. Activitatea INFOSEC din SPAD și RTD – SIC, desfășurată de către SSTIC, trebuie condusă și coordonată de persoane care dețin autorizație de acces la secretul de stat de forma corespunzătoare, cu pregătire de specialitate în domeniul sistemelor TIC și al securității acestora, precum și experiență de cel puțin 2 ani în domeniu.

861. Protecția SPAD și RTD – SIC din componența sistemelor de armament și de detecție se definește în contextul general al sistemelor din care acestea fac parte și se realizează prin aplicarea prevederilor prezentului Regulament.

Secțiunea a 2-a

Măsuri, cerințe și moduri de operare

862. Măsurile de protecție a informațiilor atribuite la secret de stat în format electronic se aplică

sistemelor SPAD și RTD – SIC, care stochează, procesează sau transmit asemenea informații.

863. Autoritățile publice sau alte persoane juridice deținătoare de informații atribuite la secret de stat au obligația să stabilească și să implementeze un ansamblu de măsuri de securitate a sistemelor SPAD și RTD – SIC – fizice, de personal, administrative, de tip TEMPEST și criptografic.

864. Măsurile de securitate destinate protecției SPAD și RTD – SIC trebuie să asigure controlul accesului pentru prevenirea sau detectarea divulgării neautorizate a informațiilor. În procesul de certificare va stabili dacă aceste măsuri sînt corespunzătoare.

865. Cerințele de securitate specifice (CSS) se stabilesc într-un document încheiat între organul competent pentru protecția secretului de stat și SSTIC, ce cuprinde principii și măsuri de securitate care trebuie să stea la baza procesului de certificare a SPAD sau RTD – SIC.

866. CSS se elaborează pentru fiecare SPAD și RTD – SIC care stochează, procesează sau transmite informații atribuite la secret de stat. Acestea sînt stabilite de către SSTIC și aprobate de către organul competent pentru protecția secretului de stat.

867. CSS se formulează încă din faza de proiectare a SPAD sau RTD – SIC și se dezvoltă pe tot ciclul de viață al sistemului.

868. CSS au la bază standardele naționale de protecție, parametrii esențiali ai mediului operațional, nivelul minim de autorizare a personalului, gradul de secretizare a informațiilor gestionate și modul de operare a sistemului care urmează să fie supus certificării.

869. SPAD și RTD – SIC care stochează, procesează sau transmit informații atribuite la secret de stat vor fi certificate și autorizate să opereze, pe anumite perioade de timp, în unul dintre următoarele moduri de operare:

- 1) specializat;
- 2) de nivel înalt;
- 3) multinivel.

870. În modul de operare *specializat*, toate persoanele cu drept de acces la SPAD sau la RTD trebuie să aibă autorizație de acces la secret de stat de forma corespunzătoare celui mai înalt grad de secretizare a informațiilor stocate, procesate sau transmise prin aceste sisteme, iar necesitatea de a lucra cu informații atribuite la secret de stat pentru aceste persoane se stabilește cu privire la toate informațiile stocate, procesate sau transmise în cadrul SPAD sau RTD – SIC.

871. În acest mod de operare, principiul necesității de a lucra cu informații atribuite la secret de stat nu impune o separare a informațiilor în cadrul SPAD sau RTD, ca mijloc de securitate a SIC. Celelalte măsuri de protecție prevăzute trebuie să asigure îndeplinirea cerințelor impuse de cel mai înalt grad de secretizare a informațiilor stocate, procesate sau transmise în cadrul SPAD sau RTD.

872. În modul de operare *de nivel înalt*, toate persoanele cu drept de acces la SPAD sau la RTD – SIC trebuie să aibă autorizație de acces la secret de stat de forma corespunzătoare celui mai înalt grad de secretizare a informațiilor stocate, procesate sau transmise în cadrul SPAD sau RTD – SIC, iar accesul la informații se face diferențiat, conform principiului necesității de a lucra cu informații atribuite la secret de stat.

873. Pentru a asigura accesul diferențiat la informații, conform principiului necesității de a lucra cu informații atribuite la secret de stat, se instituie facilități de securitate care să asigure un acces selectiv și separarea informațiilor în cadrul SPAD sau RTD – SIC. Celelalte măsuri de protecție trebuie să satisfacă cerințele pentru cel mai înalt grad de secretizare a informațiilor stocate, procesate, transmise în cadrul SPAD sau RTD – SIC.

874. Toate informațiile stocate, procesate sau vehiculate în cadrul unui SPAD sau RTD – SIC în acest mod de operare vor fi protejate ca informații, avînd cel mai înalt grad de secretizare care a fost constatat în mulțimea informațiilor stocate, procesate sau vehiculate prin sistem.

875. În modul de operare *multinivel*, accesul la informațiile atribuite la secret de stat se face diferențiat, potrivit principiului necesității de a lucra cu informații atribuite la secret de stat, conform următoarelor reguli:

1) nu toate persoanele cu drept de acces la SPAD sau RTD – SIC au autorizație de acces de forma corespunzătoare celui mai înalt grad de secretizare a informațiilor care sînt stocate, procesate sau

transmise prin aceste sisteme;

2) nu toate persoanele cu acces la SPAD sau RTD – SIC au acces la toate informațiile stocate, procesate sau transmise prin aceste sisteme, accesul acordându-se diferențiat, conform principiului necesității de a lucra cu informații atribuite la secret de stat.

876. Aplicarea regulilor prevăzute în punctul 875 din prezentul Regulament impune instituirea unor facilități de securitate care să asigure un mod selectiv și individual de acces la informațiile atribuite la secret de stat din cadrul SPAD sau RTD –SIC.

877. Securitatea SPAD, a rețelei și a obiectivului SIC se asigură prin funcțiile de administrator de securitate.

878. Administratorii de securitate sînt:

- 1) administratorul de securitate al SPAD;
- 2) administratorul de securitate al rețelei;
- 3) administratorul de securitate al obiectivului SIC.

879. Funcțiile de administratori de securitate trebuie să asigure îndeplinirea atribuțiilor SSTIC. Dacă este cazul, aceste funcții pot fi cumulate de către un singur specialist.

880. SSTIC desemnează un administrator de securitate al SPAD responsabil de supervizarea dezvoltării, implementării și administrării măsurilor de securitate dintr-un SPAD, inclusiv participarea la elaborarea procedurilor operaționale de securitate.

881. La recomandarea organului competent pentru protecția secretului de stat, SSTIC poate desemna structuri de administrare ale SPAD, care îndeplinesc aceleași atribuții.

882. Administratorul de securitate al rețelei este desemnat de SSTIC pentru un SIC de mari dimensiuni sau în cazul interconectării mai multor SPAD și îndeplinește atribuții privind managementul securității comunicațiilor.

883. Administratorul de securitate al obiectivului SIC este desemnat de SSTIC sau de organul competent pentru protecția secretului de stat și răspunde de asigurarea implementării și menținerea măsurilor de securitate aplicabile obiectivului SIC respectiv.

884. Responsabilitățile unui administrator de securitate al obiectivului SIC pot fi îndeplinite de către Subdiviziunea de protecție a autorității publice sau al altei persoane juridice, ca parte a atribuțiilor sale de serviciu.

885. Obiectivul SIC reprezintă un amplasament specific sau un grup de amplasamente în care funcționează un SPAD și/sau RTD. Responsabilitățile și măsurile de securitate pentru fiecare zonă de amplasare a unui terminal/stație de lucru care funcționează la distanță trebuie să fie clar determinate.

886. Toți utilizatorii de SPAD sau RTD – SIC poartă responsabilitatea în ceea ce privește securitatea acestor sisteme raportate, în principal, la drepturile acordate și sînt îndrumați de către administratorii de securitate.

887. Utilizatorii trebuie să dețină autorizație de acces la secretul de stat de forma corespunzătoare gradului de secretizare a informațiilor stocate, procesate sau transmise în SPAD sau RTD – SIC. La acordarea dreptului de acces la informații, se stabilește, individual, necesitatea de a lucra cu informațiile atribuite la secret de stat.

888. Informarea utilizatorilor cu îndatoririle lor de securitate trebuie să asigure o eficacitate sporită a sistemului de securitate.

889. Vizitatorii trebuie să aibă autorizație de acces de gradul corespunzător și să îndeplinească principiul necesității de a lucra cu informații atribuite la secret de stat. În situația în care accesul unui vizitator fără drept de acces este considerat necesar, vor fi luate măsuri de securitate suplimentare pentru ca acesta să nu poată avea acces la informațiile atribuite la secret de stat.

Secțiunea a 3-a

Condiții de securitate

890. Utilizatorilor SPAD și RTD – SIC li se acordă dreptul de acces la secretul de stat, în funcție de necesitatea acestora de a lucra cu informații atribuite la secret de stat și corespunzător gradului de secretizare a informațiilor stocate, procesate sau transmise prin aceste sisteme

891. Autoritățile publice sau alte persoane juridice deținătoare de informații atribuite la secret de stat în format electronic au obligația să instituie măsuri speciale pentru instruirea și supravegherea personalului, inclusiv a personalului de proiectare de sistem care are acces la SPAD și RTD, în vederea prevenirii și înlăturării vulnerabilităților față de accesarea neautorizată.

892. În proiectarea SPAD și RTD – SIC trebuie să se aibă în vedere ca atribuirea sarcinilor și responsabilităților personalului să se facă în așa fel încât să nu existe o persoană care să aibă cunoștințe sau acces la toate programele și cheile de securitate – parole, mijloace de identificare personală.

893. Procedurile de lucru ale personalului din SPAD și RTD – SIC trebuie să asigure separarea operațiunilor de programare și a celor de exploatare a sistemului sau rețelei. Nu se admite, cu excepția unor situații speciale, ca personalul să facă atât programarea, cât și operarea sistemelor sau rețelelor și trebuie instituite proceduri speciale pentru depistarea acestor situații.

894. Pentru orice fel de modificare aplicată unui sistem SPAD sau RTD – SIC este obligatorie colaborarea a cel puțin două persoane – “regula celor doi”. Procedurile de securitate trebuie să stabilească explicit situațiile în care “regula celor doi” trebuie aplicată.

895. Pentru a asigura implementarea corectă a măsurilor de securitate, personalul SPAD și RTD – SIC și personalul care răspunde de securitatea acestora trebuie să fie instruit și informat astfel încât să-și cunoască reciproc atribuțiile.

896. Zonele în care sînt amplasate SPAD și/sau RTD – SIC și cele cu terminale la distanță, în care sînt prezentate, stocate, procesate sau transmise informații atribuite la secret de stat ori în care este posibil accesul potențial la astfel de informații, se declară zone de securitate clasa I sau clasa a II-a ale obiectivului și se supun măsurilor de protecție fizică stabilite de prezentul Regulament.

897. În zonele în care sînt amplasate sisteme SPAD și terminale la distanță – stații de lucru, unde se procesează și/sau pot fi accesate informații atribuite la secret de stat, se aplică următoarele măsuri generale de securitate:

1) intrarea personalului (introducerea materialelor), precum și plecarea în/din aceste zone sînt controlate prin mijloace bine stabilite;

2) zonele și locurile în care securitatea SPAD sau RTD – SIC sau a terminalelor la distanță poate fi modificată nu trebuie să fie niciodată ocupate de o singură persoană autorizată;

3) persoanelor care solicită acces temporar sau cu intermitențe în aceste zone trebuie să li se autorizeze accesul, ca vizitatori. Vizitatorii vor fi însoțiți permanent, pentru a avea garanția că nu pot avea acces la informațiile atribuite la secret de stat și nici la echipamentele utilizate.

898. În funcție de riscul de securitate și de gradul de secretizare a informațiilor stocate, procesate și transmise, se impune cerința de aplicare a regulii de lucru cu două persoane și în alte zone, care vor fi stabilite în stadiul inițial al proiectului și prezentate în cadrul CSS.

899. Cînd un SPAD este exploatat în mod autonom, deconectat în mod permanent de alte SPAD, ținînd cont de condițiile specifice, de alte măsuri de securitate, tehnice sau procedurale și de rolul pe care îl are respectivul SPAD în funcționarea de ansamblu a sistemului, organul competent pentru protecția secretului de stat va stabili măsuri specifice de protecție, adaptate la structura acestui SPAD, conform gradului de secretizare a informațiilor gestionate.

900. Toate informațiile și materialele care privesc accesul la un SPAD sau RTD – SIC sînt controlate și protejate prin reglementări corespunzătoare gradului cel mai înalt de secretizare și specificului informațiilor la care respectivul SPAD sau RTD – SIC permite accesul.

901. Cînd nu mai sînt utilizate, informațiile și materialele specificate în punctul 900 la prezentul Regulament trebuie să fie distruse, conform prevederilor prezentului Regulament.

902. Informațiile atribuite la secret de stat în format electronic trebuie să fie controlate conform regulilor INFOSEC, înainte de a fi transmise din zonele SPAD și RTD – SIC sau din cele cu terminale la distanță.

903. Modul în care este prezentată informația în clar, chiar dacă se utilizează codul prescurtat de transmisie sau reprezentarea binară ori alte forme de transmitere la distanță, nu trebuie să influențeze gradul de secretizare acordat informațiilor respective.

904. Cînd informațiile sînt transferate între diverse SPAD sau RTD – SIC, ele trebuie să fie

protejate atât în timpul transferului, cât și la nivelul sistemelor informatice ale beneficiarului, corespunzător gradului de secretizare a informațiilor transmise.

905. Toate mediile de stocare, purtătorii materiali ai informațiilor se păstrează într-o modalitate care să corespundă celui mai înalt grad de secretizare a informațiilor stocate.

906. Copierea informațiilor atribuite la secret de stat, situate pe medii de stocare specifice TIC, se execută în conformitate cu prevederile din procedurile operaționale de securitate.

907. Mediile reutilizabile de stocare a informațiilor, folosite pentru înregistrarea informațiilor atribuite la secret de stat, își mențin cel mai înalt grad de secretizare pentru care au fost utilizate anterior, pînă cînd respectivelor informații li se reduce gradul de secretizare sau sînt desecretizate, moment în care parafa de secretizare, aplicată mediilor sus-menționate, se modifică în mod corespunzător sau aceste medii sînt distruse.

908. Evidența automată a accesului la informațiile atribuite la secret de stat în format electronic se ține în registrele de acces și trebuie realizată necondiționat prin software.

909. Registrele de acces se păstrează pe o perioadă stabilită de comun acord între organul competent pentru protecția secretului de stat și SSTIC.

910. Perioada minimă de păstrare a registrelor de acces la informațiile secretizate cu parafa "Strict secret" este de 10 ani, iar a registrelor de acces la informațiile avînd gradele de secretizare "Secret", "Confidențial" și "Restricționat" – de cel puțin 3 ani.

911. Mediile de stocare care conțin informații atribuite la secret de stat, utilizate în interiorul unei zone SPAD, pot fi manipulate ca material unic secret, cu condiția ca materialul să fie identificat, marcat cu parafa sa de secretizare și controlat în interiorul zonei SPAD, pînă la momentul în care este distrus sau transmis pentru păstrare.

912. Evidențele acestora vor fi menținute în cadrul zonei SPAD pînă în momentul în care vor fi supuse controlului sau distruse.

913. În cazul în care un mediu de stocare este generat într-un SPAD sau RTD – SIC, iar apoi este transmis într-o zonă cu terminal/stație de lucru la distanță, se stabilesc proceduri adecvate de securitate, aprobate de către organul competent pentru protecția secretului de stat. Procedurile trebuie să cuprindă și instrucțiuni specifice privind evidența informațiilor în format electronic.

914. Toate mediile de stocare secrete se verifică periodic, cel puțin anual, corespunzător gradului de secretizare.

915. Controlul periodic al mediilor de stocare se efectuează de către o comisie specială creată în modul stabilit de capitolul III, secțiunea a 11-a din prezentul Regulament, care trebuie să verifice prezența fizică a mediilor de stocare, precum și conținutul acestora în vederea corespunderii gradului de secretizare atribuit anterior.

916. Informațiile atribuite la secret de stat, înregistrate pe medii de stocare reutilizabile, se șterg doar în conformitate cu procedurile operaționale de securitate.

917. Cînd un mediu de stocare urmează să iasă din uz, trebuie să fie desecretizat, suprimîndu-se orice marcaje de secretizare, ulterior putînd fi utilizat ca mediu de stocare nesecret. Dacă acesta nu poate fi desecretizat, trebuie distrus în modul stabilit de prezentul Regulament.

918. Sînt interzise desecretizarea și reutilizarea mediilor de stocare care conțin informații avînd gradul de secretizare "Strict secret", acestea putînd fi numai distruse.

919. Informațiile atribuite la secret de stat în format electronic, stocate pe un mediu de unică folosință – cartele, benzi perforate, trebuie distruse.

Secțiunea a 4-a

Reguli generale de securitate TIC

920. Toate mijloacele folosite pentru transmiterea electromagnetică a informațiilor atribuite la secret de stat se supun instrucțiunilor de securitate a comunicațiilor, emise de către organul competent pentru protecția secretului de stat.

921. Într-un SPAD – SIC trebuie să se dispună mijloace de interzicere a accesului la informațiile atribuite la secret de stat de la toate terminalele/stațiile de lucru la distanță, atunci cînd se solicită acest

lucru, prin deconectare fizică sau prin proceduri software speciale, aprobate de organul competent pentru protecția secretului de stat.

922. Instalarea inițială a SPAD sau RTD – SIC sau orice modificare majoră adusă acestora vor fi executate de persoane autorizate, în condițiile prezentului Regulament. Lucrările vor fi permanent supravegheate de personal tehnic calificat, care are drept de acces la secretul de stat de forma corespunzătoare celui mai înalt grad de secretizare a informațiilor pe care respectivul SPAD sau RTD – SIC le va stoca, procesa sau transmite.

923. Toate echipamentele SPAD și RTD – SIC vor fi instalate în conformitate cu reglementările specifice în vigoare, emise de către organul competent pentru protecția secretului de stat și standardele tehnice corespunzătoare.

924. Sistemele SPAD și RTD – SIC, care stochează, procesează sau transmit informații secrete de stat, vor fi protejate corespunzător față de vulnerabilitățile de securitate cauzate de radiațiile compromițătoare – TEMPEST.

925. Procesarea informațiilor se realizează în conformitate cu procedurile operaționale de securitate, prevăzute de prezentul Regulament.

926. Transmiterea informațiilor atribuite la secret de stat către instalații automate, a căror funcționare nu necesită prezența unui operator uman, este interzisă, cu excepția cazului în care se aplică reglementări speciale aprobate de organul competent pentru protecția secretului de stat, iar acestea au fost specificate în procedurile operaționale de securitate.

927. Procedurile operaționale de securitate reprezintă descrierea implementării strategiei de securitate ce urmează să fie adoptată, a procedurilor operaționale de urmat și a responsabilităților personalului.

928. Procedurile operaționale de securitate sînt elaborate de către SSTIC în colaborare cu organul competent pentru protecția secretului de stat, precum și cu alte autorități cu atribuții în domeniu. Organul competent pentru protecția secretului de stat va aproba procedurile de operare înainte de a autoriza stocarea, procesarea sau transmiterea informațiilor secrete de stat prin SPAD – RTD – SIC.

929. SSTIC are obligația să efectueze controale periodice, prin care să stabilească dacă toate produsele software originale – sisteme de operare generale, subsisteme și pachete soft, aflate în folosință, sînt protejate în condiții corespunzătoare gradului de secretizare a informațiilor pe care acestea trebuie să le proceseze. Protecția aplicațiilor software se stabilește pe baza evaluării gradului de secretizare a acestora, ținînd cont de gradul de secretizare a informațiilor pe care urmează să le proceseze.

930. Este interzisă utilizarea de software necertificate de către organul competent pentru protecția secretului de stat.

931. Conservarea exemplarelor originale, a copiilor – backup sau off-site, precum și salvările periodice ale datelor obținute prin procesare vor fi executate în conformitate cu prevederile procedurilor operaționale de securitate.

932. Versiunile software care sînt în uz trebuie să fie verificate la intervale regulate, pentru a garanta integritatea și funcționarea lor corectă.

933. Versiunile noi sau modificate ale software-ului nu vor fi folosite pentru procesarea informațiilor atribuite la secret de stat, pînă cînd procedurile de securitate ale acestora nu sînt testate și aprobate conform CSS.

934. Un software care îmbunătățește posibilitățile sistemului și care nu are nici o procedură de securitate nu poate fi folosit înainte de a fi verificat de către SSTIC.

935. Verificarea prezenței virușilor și software-ului nociv se face în conformitate cu cerințele stabilite de către organul competent pentru protecția secretului de stat.

936. Versiunile de software noi sau modificate – sisteme de operare, subsisteme, pachete de software și aplicații de software, stocate pe diferite medii, care se introduc într-o autoritate publică sau altă persoană juridică, trebuie verificate obligatoriu pe sisteme de calcul izolate, în vederea depistării software-ului nociv sau a virușilor de calculator, înainte de a fi folosite în SPAD sau RTD – SIC. Periodic se va proceda la verificarea software-ului instalat.

937. Verificările trebuie făcute mai frecvent dacă SPAD sau RTD – SIC sînt conectate la alt SPAD sau RTD – SIC sau la o rețea publică de comunicații.

938. În contractele de întreținere a SPAD și RTD – SIC care stochează, procesează sau transmit informații atribuite la secret de stat se vor specifica cerințele care trebuie îndeplinite pentru ca personalul de întreținere și aparatura specifică a acestuia să poată fi introduse în zona de operare a sistemelor respective.

939. Personalul de întreținere trebuie să dețină autorizație de acces la secret de stat de forma corespunzătoare gradului de secretizare a informațiilor la care au acces.

940. Scoaterea echipamentelor sau a componentelor hardware din zona SPAD sau RTD – SIC se execută în conformitate cu prevederile procedurilor operaționale de securitate.

941. Cerințele menționate în punctul 938 și punctul 939 din prezentul Regulament trebuie stipulate în CSS, iar procedurile de desfășurare a activității respective trebuie stabilite în procedurile operaționale de securitate. Nu se acceptă tipurile de întreținere care constau în aplicarea unor proceduri de diagnosticare ce implică accesul de la distanță la sistem, decît în cazul în care activitatea respectivă se desfășoară sub control strict și numai cu aprobarea organului competent pentru protecția secretului de stat.

942. Componentele sistemelor de securitate implementate în SPAD sau RTD – SIC trebuie certificate sau autorizate pe baza unei documentații tehnice amănunțite privind proiectarea, realizarea și modul de distribuire al acestora.

943. SPAD sau RTD – SIC care stochează, procesează sau transmit informații atribuite la secret de stat sau componentele lor de bază – sisteme de operare de scop general, produse de limitare a funcționării pentru realizarea securității și produse pentru comunicare în rețea, se pot achiziționa numai dacă au fost evaluate și autorizate sau evaluate și certificate de către organul competent pentru protecția secretului de stat.

944. La închirierea unor componente hardware sau software, în special a unor medii de stocare, se va ține cont că astfel de echipamente, odată utilizate în SPAD sau RTD – SIC ce procesează, stochează sau transmit informații atribuite la secret de stat, vor fi supuse măsurilor de protecție reglementate prin prezentul Regulament. La secretizare, componentele respective nu vor putea fi scoase din zonele SPAD sau RTD – SIC decît după desecretizare.

945. Toate SPAD și RTD – SIC, înainte de a fi utilizate pentru stocarea, procesarea sau transmiterea informațiilor atribuite la secret de stat, trebuie certificate sau autorizate de către organul competent pentru protecția secretului de stat, pe baza datelor stabilite în CSS, procedurilor operaționale de securitate și altor documentații relevante.

946. Subsistemele SPAD și RTD – SIC și stațiile de lucru cu acces la distanță sau terminalele sînt certificate sau autorizate ca parte integrantă a sistemelor SPAD și RTD – SIC la care sînt conectate.

947. În situațiile referitoare la modul de operare de securitate multinivel, SPAD sau RTD – SIC, hardware-ul, firmware-ul și software-ul, organul competent pentru protecția secretului de stat stabilește, în vederea evaluării și certificării, criterii diferențiate pentru fiecare grad de secretizare a informațiilor vehiculate de SPAD sau RTD – SIC.

948. Cerințele de evaluare și certificare se includ în planificarea sistemului SPAD și RTD – SIC și sînt stipulate explicit în CSS, imediat după ce modul de operare de securitate a fost stabilit.

949. Evaluarea și certificarea de securitate în modul de operare de securitate multinivel se impune:

1) pentru SPAD sau RTD – SIC care stochează, procesează sau transmite informații secretizate cu parafa “Strict secret”;

2) pentru SPAD sau RTD – SIC care stochează, procesează sau transmite informații secretizate cu parafa “Secret”, în cazurile în care:

a) SPAD sau RTD – SIC este interconectat cu un alt SPAD sau RTD – SIC, de exemplu, aparținînd altui SSTIC;

b) SPAD sau RTD – SIC are un număr de utilizatori posibili care nu poate fi definit exact.

950. Procesele de evaluare și certificare se efectuează de către experți (specialiști cu pregătire tehnică adecvată), selecționați de către organul competent pentru protecția secretului de stat, care

dispun de drept de acces la secret de stat de forma corespunzătoare.

951. În procesele de evaluare și certificare se va stabili în ce măsură un SPAD sau RTD – SIC îndeplinește condițiile de securitate specificate prin CSS, avându-se în vedere că, după încheierea procesului de evaluare și certificare, anumite secțiuni – paragrafe sau capitole, din CSS trebuie să fie modificate sau actualizate.

952. Procesele de evaluare și certificare trebuie să înceapă din stadiul de definire a SPAD sau RTD – SIC și să continue pe parcursul fazelor de dezvoltare.

953. Pentru toate SPAD și RTD – SIC care stochează, procesează sau transmit informații atribuite la secret de stat, SSTIC stabilește proceduri de control prin care să se poată stabili dacă schimbările intervenite în SIC sînt de natură a le compromite securitatea.

954. Modificările care implică o certificare repetată sau pentru care se solicită aprobarea anterioară a organului competent pentru protecția secretului de stat trebuie să fie identificate cu claritate și expuse în CSS.

955. După orice modificare, reparare sau eroare care ar fi putut afecta dispozitivele de securitate ale SPAD sau RTD – SIC, SSTIC trebuie să efectueze o verificare privind funcționarea corectă a dispozitivelor de securitate.

956. Certificarea sau autorizarea SPAD sau RTD – SIC trebuie să corespundă nivelului de satisfacere a criteriilor de verificare.

957. Toate SPAD și RTD – SIC care stochează, procesează sau transmit informații atribuite la secret de stat sînt inspectate și reexamineate periodic de către organul competent pentru protecția secretului de stat.

958. Pentru SPAD sau RTD – SIC care stochează, procesează sau transmit informații secretizate cu parafa "Strict secret", inspectia se va face cel puțin o dată pe an.

959. Microcalculatoarele sau calculatoarele personale care au discuri fixe sau alte medii nevolatile de stocare a informației, ce operează autonom sau ca parte a unei rețele, precum și calculatoarele portabile cu discuri fixe sînt considerate medii de stocare a informațiilor, în același sens ca și celelalte medii amovibile de stocare a informațiilor.

960. În măsura în care microcalculatoarele sau calculatoarele personale stochează informații atribuite la secret de stat, acestea trebuie supuse cerințelor prezentului Regulament.

961. Echipamentelor prevăzute în punctul 959 din prezentul Regulament trebuie să li se acorde gradul de protecție pentru acces, manipulare, stocare și transport, corespunzător celui mai înalt grad de secretizare a informațiilor care au fost vreodată stocate sau procesate pe ele, pînă la trecerea la un alt grad de secretizare sau desecretizarea lor, în conformitate cu procedurile legale.

962. Este interzisă utilizarea mediilor de stocare amovibile, a software-ului și a hardware-ului, aflate în proprietate privată, pentru stocarea, procesarea și transmiterea informațiilor secrete de stat.

963. Este interzisă introducerea mediilor de stocare amovibile, a software-ului și hardware-ului, aflate în proprietate privată, în zonele în care se stochează, se procesează sau se transmit informații atribuite la secret de stat, fără aprobarea conducătorului autorității publice sau al altei persoane juridice.

964. Utilizarea într-un obiectiv a echipamentelor și a software-ului contractanților pentru stocarea, procesarea sau transmiterea informațiilor atribuite la secret de stat este permisă numai cu avizul SSTIC și aprobarea conducătorului autorității publice sau al altei persoane juridice.

965. Utilizarea într-un obiectiv a echipamentelor și software-ului puse la dispoziție de către alte instituții poate fi permisă numai cu avizul SSTIC. În acest caz, echipamentele sînt evidențiate în inventarul autorității publice sau al altei persoane juridice.

Capitolul XI

MĂSURI DE PROTECȚIE A SECRETULUI DE STAT LA EFECTUAREA UNOR LUCRĂRI COMUNE ȘI ALTOR LUCRĂRI

966. Autoritățile publice, alte persoane juridice, cetățenii pot efectua lucrări comune sau alte lucrări cu utilizarea informațiilor atribuite la secret de stat, în baza contractelor secretizate în modul stabilit de prezentul Regulament.

967. Pentru participarea la încheierea și derularea contractelor cu utilizarea informațiilor atribuite la secret de stat, persoanele juridice trebuie să dispună de certificat de securitate pentru efectuarea lucrărilor cu utilizarea informațiilor avînd un anumit grad de secretizare, iar cetățenii – să dispună de drept de acces la informațiile atribuite la secret de stat de forma corespunzătoare.

968. Clauzele și procedurile de protecție a informațiilor atribuite la secret de stat, devenite sau care pot deveni cunoscute în procesul încheierii și derulării contractelor în legătură cu efectuarea unor lucrări comune sau altor lucrări, vor fi stipulate în anexa de securitate a fiecărui contract, care presupune acces la astfel de informații.

969. Anexa de securitate se întocmește de beneficiar și include toate măsurile, drepturile și obligațiile reciproce ale părților de asigurare a integrității și protecției informațiilor atribuite la secret de stat, atît în procesul derulării contractului, cît și după încetarea acestuia.

970. Clauzele și procedurile de protecție vor fi supuse, periodic, inspecțiilor și verificărilor de către organul competent pentru protecția secretului de stat.

971. Beneficiarul este responsabil pentru secretizarea și definirea tuturor componentelor acestuia, în conformitate cu normele în vigoare.

972. La secretizarea contractelor se vor aplica următoarele reguli generale:

1) în toate stadiile de planificare și executare, gradul de secretizare a contractului se determină în funcție de conținutul informațiilor utilizate;

2) secretizarea se aplică numai acelor părți ale contractului care trebuie protejate;

3) dacă în derularea unui contract se folosesc informații din mai multe surse, cu grade de secretizare diferite, contractul va fi secretizat în funcție de gradul cel mai înalt al informațiilor, iar măsurile de protecție vor fi stabilite în modul corespunzător;

4) desecretizarea sau modificarea gradului de secretizare a unei informații din cadrul contractului se aprobă de conducătorul autorității publice sau al altei persoane juridice care a aprobat secretizarea inițială.

973. În cazul în care apare necesitatea protejării informațiilor dintr-un contract care, anterior, nu a fost necesar a fi secretizat, beneficiarul are obligația declanșării procedurilor de secretizare și protejare, conform reglementărilor în vigoare.

974. Contractantul poate ceda unui subcontractant realizarea unei părți din contractul secretizat, doar cu acordul beneficiarului sau, dacă acest drept este prevăzut în contract, cu informarea obligatorie a beneficiarului. Subcontractantul trebuie să dispună de certificat de securitate.

975. Contractantul (executantul) și subcontractanții sînt obligați să implementeze și să respecte toate măsurile de protecție a informațiilor atribuite la secret de stat puse la dispoziție sau care au fost generate pe timpul derulării contractelor.

976. Transmiterea informațiilor atribuite la secret de stat contractanților (executanților), în legătură cu efectuarea acestor lucrări, se face de către beneficiarul acestor lucrări, cu permisiunea autorității publice cu împuterniciri de dispoziție asupra acestor informații și numai în volumul necesar pentru efectuarea lucrărilor respective.

977. Toate informațiile atribuite la secret de stat, necesare derulării contractelor, se transmit prin intermediul Subdiviziunilor de protecție, în modul stabilit de prezentul Regulament.

978. În timpul efectuării lucrărilor comune, a altor lucrări și a apariției, în legătură cu aceasta, a necesității de a utiliza informații atribuite la secret de stat, persoanele juridice, inclusiv cele cu capital privat, pot încheia cu alte persoane juridice, care dispun de certificat de securitate, contracte de folosire a serviciilor prestate de către subdiviziunile lor de protecție, fapt ce se notifică în certificatul de securitate pentru efectuarea lucrărilor cu utilizarea informațiilor atribuite la secret de stat.

979. Dacă în timpul derulării contractului, executantul încalcă obligațiile de protecție a secretului de stat, beneficiarul are dreptul să suspende executarea comenzii pînă la lichidarea încălcărilor, iar în cazul încălcărilor repetate – să solicite anularea comenzii și a certificatului de securitate pentru efectuarea lucrărilor cu utilizarea informațiilor atribuite la secret de stat și tragerea la răspundere a persoanelor vinovate.

980. Prejudiciul material cauzat de către executant statului, în persoana beneficiarului, se repară

conform legislației.

Capitolul XII

CONTROLUL PRIVIND STAREA PROTECȚIEI SECRETULUI DE STAT

Secțiunea 1

Dispoziții generale

981. Controlul privind asigurarea protecției secretului de stat se efectuează de:

- 1) conducătorii autorităților publice și ai altor persoane juridice, precum și de Subdiviziunile de protecție ale acestora;
- 2) Serviciul de Informații și Securitate.

982. Conducătorii autorităților publice și ai altor persoane juridice, Subdiviziunile de protecție ale acestora exercită controlul privind asigurarea protecției secretului de stat referitor la informațiile deținute de acestea sau de persoanele juridice din subordine, precum și cu privire la informațiile transmise antreprenorilor în legătură cu executarea comenzilor.

983. Controlul privind asigurarea protecției secretului de stat în aparatele Parlamentului, Președintelui Republicii Moldova și Guvernului este organizat de către conducătorii acestor organe.

984. Serviciul de Informații și Securitate este abilitat cu exercitarea controlului privind starea protecției secretului de stat în cadrul autorităților publice (control interdepartamental) și în cadrul altor persoane juridice.

985. Controlul are ca scop:

- 1) evaluarea eficienței măsurilor concrete de protecție adoptate la nivelul deținătorilor de informații atribuite la secret de stat, în conformitate cu [Legea](#), cu prevederile prezentului Regulament și ale altor norme în materie, precum și cu programele de prevenire a scurgerii de informații atribuite la secret de stat;

- 2) identificarea neajunsurilor existente în sistemul de protecție a informațiilor atribuite la secret de stat, care ar putea conduce la divulgarea sau pierderea acestor informații, în vederea luării măsurilor de prevenire și lichidare ce se impun;

- 3) constatarea cauzelor apariției acestor neajunsuri;

- 4) luarea măsurilor de remediere a deficiențelor și elaborarea propunerilor de perfecționare a cadrului organizatoric și funcțional la nivelul autorității publice sau al altei persoane juridice controlate;

- 5) constatarea cazurilor de încălcare a normelor de protecție a secretului de stat și întreprinderea măsurilor necesare în vederea tragerii la răspundere a persoanelor vinovate de aceste încălcări.

986. Fiecare acțiune de control se încheie printr-un document de constatare, întocmit de persoana/persoanele care l-au efectuat.

987. Concluziile formulate de către Serviciul de Informații și Securitate în urma controlului sînt executorii pentru persoanele cu funcții de răspundere ale autorităților publice sau ale altor persoane juridice controlate, acestea urmînd să adopte măsuri imediate de remediere a deficiențelor constatate.

988. În funcție de obiectivele urmărite, controalele pot fi:

- 1) controale de fond (totale), care urmăresc verificarea întregului sistem organizatoric, structural și funcțional de protecție a informațiilor atribuite la secret de stat;

- 2) controale tematice, care vizează anumite domenii ale activității de protecție a informațiilor atribuite la secret de stat;

- 3) controale în situații de urgență (operative), care au ca scop verificarea anumitor aspecte, stabilite ca urmare a identificării unui risc de securitate.

989. În funcție de modul în care sînt stabilite și organizate, controalele pot fi:

- 1) planificate;

- 2) inopinate.

990. Conducătorii autorităților publice sau ai altor persoane juridice care fac obiectul controlului au obligația să pună la dispoziția reprezentanților Serviciului de Informații și Securitate, care efectuează controlul, toate informațiile solicitate privind modul de aplicare a măsurilor prevăzute de lege pentru

protecția secretului de stat.

991. Conducătorii autorităților publice sau ai altor persoane juridice deținătoare de informații atribuite la secret de stat au obligația să organizeze, anual și ori de câte ori este nevoie, controale interne privind gestionarea acestora.

Secțiunea a 2-a

Investigații de serviciu

992. Faptele de divulgare a informațiilor atribuite la secret de stat, pierdere a documentelor și altor purtători materiali de informații atribuite la secret de stat sau a articolelor care conțin asemenea informații se comunică neîntârziat Subdiviziunii de protecție, conducătorului autorității publice sau al altei persoane juridice (autorității cu împuterniciri de dispoziție asupra acestor informații) și Serviciului de Informații și Securitate.

993. Totodată, în cazul încălcărilor menționate în punctul 992 din prezentul Regulament se iau măsuri cu privire la organizarea unei investigații de serviciu pentru clarificarea circumstanțelor divulgării informațiilor atribuite la secret de stat, pierderii documentelor, altor purtători materiali sau articolelor care conțin informații atribuite la secret de stat și căutarea acestora. Măsurile necesare privind căutarea documentelor, altor purtători materiali de informații atribuite la secret de stat și articolelor secrete, clarificarea circumstanțelor divulgării informațiilor secrete și depistarea persoanelor vinovate în cadrul autorităților publice sau altor persoane juridice se îndeplinesc în comun cu Serviciul de Informații și Securitate.

994. Pentru efectuarea investigațiilor de serviciu, conducătorul autorității publice sau al altei persoane juridice, cel târziu a doua zi după descoperirea încălcării, instituie prin ordin o comisie formată din cel puțin 3 persoane competente și imparțiale, inclusiv din cadrul Subdiviziunii de protecție, care au acces de forma corespunzătoare gradului de secretizare a informațiilor respective. În activitatea comisiei pot fi atrași și reprezentanți ai autorităților publice sau altor persoane juridice ierarhic superioare.

995. Comisia care efectuează investigația de serviciu este obligată:

1) să stabilească circumstanțele divulgării informațiilor atribuite la secret de stat, pierderii documentelor, altor purtători materiali sau articolelor care conțin asemenea informații (cum ar fi: timpul, locul, modul);

2) să caute documentul, alt purtător material de informații, articolul secret;

3) să stabilească persoanele care au comis încălcările respective;

4) să stabilească cauza și condițiile care au contribuit la divulgarea informațiilor atribuite la secret de stat, pierderea, furtul documentelor, altor purtători materiali sau articolelor secrete și să elaboreze recomandări pentru înlăturarea acestora.

996. Membrii comisiei care efectuează investigația de serviciu au dreptul:

1) să examineze încăperile autorității publice sau al altei persoane juridice, teritoriul adiacent, safeurile, dulapurile de metal, ambalajele, alți suportți speciali, mobilierul, valizele speciale, unde ar putea să se afle documentele, alți purtători materiali de informații, articolele secrete pierdute;

2) să verifice, filă cu filă, documentația secretă și registrele de evidență;

3) să chestioneze angajații autorității publice sau al altei persoane juridice care ar putea acorda un sprijin la elucidarea circumstanțelor cazului și să obțină de la ei explicații (mărturii) în scris;

4) să atragă, cu permisiunea conducătorului autorității publice sau al altei persoane juridice respective, alți angajați ai acesteia pentru organizarea unor măsuri de investigație aparte, cu asigurarea condiției de imparțialitate.

997. Investigația de serviciu trebuie să se efectueze în termen de cel mult o lună din ziua descoperirii faptului încălcării. În acest termen, conducătorul autorității publice sau al altei persoane juridice trebuie să soluționeze, în modul stabilit, chestiunea privind tragerea la răspundere a persoanelor vinovate.

998. În cazul în care faptele săvârșite constituie infracțiuni, autoritatea publică sau altă persoană juridică are obligația de a sesiza organele de urmărire penală și de a pune la dispoziția acestora datele și materialele necesare probării acestora.

999. În cazul în care documentele, alți purtători materiali sau articolele secrete pierdute nu au fost descoperite și toate măsurile posibile de căutare s-au epuizat, au fost clarificate circumstanțele pierderii lor și identificării persoanelor vinovate de aceasta, căutarea poate fi încetată. În legătură cu încetarea căutării se întocmește o concluzie motivată, care se aprobă de conducătorul autorității publice sau al altei persoane juridice și, după caz, de către conducătorul autorității publice sau al altei persoane juridice ierarhic superioare.

1000. Rezultatele tuturor acțiunilor (măsurilor) întreprinse în procesul investigației de serviciu se documentează.

1001. La finalizarea investigației de serviciu, comisia este obligată să prezinte spre examinare conducătorului autorității publice sau al altei persoane juridice următoarele documente:

- 1) concluzia cu privire la rezultatele investigației de serviciu;
- 2) explicațiile scrise ale persoanelor chestionate de către membrii comisiei;
- 3) procesele-verbale privind verificarea documentelor, articolelor, încăperilor, safeurilor, altor suporturi speciali, mobilierului, valizelor speciale;
- 4) alte documente care se referă la investigația de serviciu.

1002. În procesul investigației de serviciu comisia va determina inclusiv gradul de secretizare a informațiilor divulgate, documentelor, altor purtători materiali de informații sau articolelor pierdute.

1003. Rezultatele activității cu privire la aprecierea gradului de secretizare a informațiilor divulgate sau pierdute se reflectă, în termen de cel mult 10 zile de la data instituirii comisiei, într-o concluzie care se prezintă spre aprobare conducătorului autorității publice sau al altei persoane juridice.

1004. Dacă comisia stabilește că gradul de secretizare a informațiilor divulgate sau pierdute nu corespunde conținutului acestora, atunci concluzia comisiei se aprobă de către conducătorul autorității publice sau al altei persoane juridice ierarhic superioare.

1005. Gradul de secretizare a informațiilor divulgate sau pierdute, primite de la alte autorități publice sau persoane juridice se apreciază de către comisia formată din specialiști ai autorităților publice sau persoanelor juridice respective sau de către comisia instituției ierarhic superioare.

1006. Concluzia comisiei privind aprecierea gradului de secretizare a informațiilor divulgate sau pierdute, cu anexarea, în caz de necesitate, a copiilor materialelor investigației de serviciu se prezintă Subdiviziunii de protecție, conducătorului autorității publice sau al altei persoane juridice, conducătorului autorității publice sau al altei persoane juridice ierarhic superioare, Serviciului de Informații și Securitate.

1007. Un exemplar al concluziei și materialele investigației de serviciu se păstrează în Subdiviziunea de protecție a autorității publice sau a altei persoane juridice.

1008. Subdiviziunea de protecție are obligația de a ține evidența cazurilor de încălcare a reglementărilor cu privire la secretul de stat, a documentelor de investigație și a măsurilor luate în acest sens. Documentele menționate se păstrează timp de cinci ani.

Anexă
la Regulamentul cu privire la asigurarea
regimului secret în cadrul autorităților
publice și al altor persoane juridice

FORMELE
documentelor de evidență și asigurare
a protecției secretului de stat

Forma nr
(punctul 9)

Aprobat

Avizat

(numele, prenumele, funcția)

(numele, prenumele, funcția)

(ziua, luna, anul)

(ziua, luna, anul)

**Nomenclatorul
funcțiilor care necesită acces la secretul de stat**

(denumirea autorității publice sau a altei persoane juridice)

Nr. crt.	Subdiviziunea	Numărul total de angajați	Funcția	Argumentarea necesității de perfectare a dreptului de acces	Numărul total de angajați care necesită perfectarea dreptului de acces				Numărul de angajați pentru care se perfectează dreptul de acces				Meritaj
					Strict secret	Secret	Confidențial	Restricționat	Strict secret	Secret	Confidențial	Restricționat	
1	2	3	4	5	6	7	8	9	10	11	12	13	14

(numele, prenumele, semnătura șefului Subdiviziunii de protecție)

Forma nr.2

(punctul 98)

(secret după completare)

Locul
pentru fotografie

Nr. _____ din _____

CHESTIONAR DE BAZĂ

Instituția solicitantă

Forma de acces solicitată

Motivul solicitării

DATE GENERALE DESPRE SOLICITANT

NUME

NUME ANTERIOARE

PRENUME

PRENUMELE TATĂLUI

DATA NAȘTERII

LOCUL NAȘTERII

CETĂȚENIA actuală

BULETIN DE IDENTITATE (PAȘAPORT)

Seria _____ nr. _____ eliberat de _____ la data

Număr de identificare _____

CETĂȚENIA deținută anterior

(țara, data dobândirii și renunțării la cetățenie)

CETĂȚENIE multiplă

(țara, data dobândirii și renunțării la cetățenie)

PAȘAPORTUL STATULUI RESPECTIV

Seria _____ nr. _____ eliberat de _____ la data

DOMICILIUL PERMANENT

Localitatea

Strada _____ numărul (bloc) _____ apartamentul

Telefon fix _____ telefon mobil

Fax _____ e-mail

DOMICILIUL TEMPORAR

Localitatea

Strada _____ numărul (bloc) _____ apartamentul

Telefon fix _____ telefon mobil

Fax _____ e-mail

DOMICILII PERMANENTE ȘI TEMPORARE ÎN ULTIMII CINCI ANI

Tipul de domiciliu permanent temporar

Localitatea

Strada _____ numărul (bloc) _____ apartamentul

Tipul de domiciliu permanent temporar

Localitatea

Strada _____ numărul (bloc) _____ apartamentul

ADRESE ȘI REȘEDINȚE ÎN STRĂINĂTATE ÎN ULTIMII CINCI ANI

(pentru perioade ce depășesc 6 luni)

Perioada _____ țara _____ localitatea _____

Strada _____ numărul (bloc) _____ apartamentul _____

Perioada _____ țara _____ localitatea _____

Strada _____ numărul (bloc) _____ apartamentul _____

STUDII CIVILE ȘI MILITARE

Nr. crt.	Perioada	Instituția	Felul studiilor

LIMBI STRĂINE CUNOSCUTE

Nr. crt.	Limba	Nivelul

(În cazul atestatelor, se vor indica instituția și data încheierii studiilor)

SITUAȚIA MILITARĂ

Fără serviciul militar satisfăcut Militar în termen În rezervă

Seria livretului militar _____ Numărul livretului militar _____

Eliberat de centrul militar _____ la data _____

PAȘAPOARTE

Pașaportul cetățeanului Republicii Moldova

Seria _____ numărul _____ eliberat de _____ la data _____

De serviciu

Seria _____ numărul _____ eliberat de _____ la data _____

Diplomatic

Seria _____ numărul _____ eliberat de _____ la data _____

CĂLĂTORII ÎN STRĂINĂTATE ÎN ULTIMII CINCI ANI

Nr. crt.	Țara	Localitatea	Perioada	Scopul

SITUAȚIA PROFESIONALĂ
LOCURI DE MUNCĂ ÎN ULTIMII CINCI ANI

Nr. crt.	Profesia (ocupația)	Gradul militar	Instituția (Unitatea)	Perioada	Funcții deținute

SITUAȚIA FAMILIALĂ ACTUALĂ

Celibatar(ă) Căsătorit(ă) Concubinaj

Despărțit(ă) în fapt Divorțat(ă) Văduv(ă)

Recăsătorit(ă)

Alte situații _____

Informații referitoare la data și locul încheierii căsătoriei sau legate de situația actuală

DATE DESPRE PARTENERUL DE VIAȚĂ
(SOȚ/SOȚIE, CONCUBIN/CONCUBINĂ)

NUME _____

NUME ANTERIOARE _____

PRENUME _____

PRENUMELE TATĂLUI _____

NUMĂR DE IDENTIFICARE _____
DATA NAȘTERII _____
LOCUL NAȘTERII _____
CETĂȚENIA la naștere _____ actuală _____
PROFESIA _____
LOCUL DE MUNCĂ _____

DOMICILIUL PERMANENT

Localitatea _____
Strada _____ numărul (bloc) _____ apartamentul _____
Telefon fix _____ telefon mobil _____
Fax _____ e-mail _____

DOMICILIUL TEMPORAR

Localitatea _____
Strada _____ numărul (bloc) _____ apartamentul _____
Telefon fix _____ telefon mobil _____

DOMICILII PERMANENTE ȘI TEMPORARE ÎN ULTIMII CINCI ANI

Tipul de domiciliu permanent temporar
Localitatea _____
Strada _____ numărul (bloc) _____ apartamentul _____
Tipul de domiciliu permanent temporar
Localitatea _____
Strada _____ numărul (bloc) _____ apartamentul _____

COPII

(care au împlinit vârsta de 16 ani, inclusiv cei din alte căsătorii)

Nume, prenume	Data nașterii	Localitatea	Domiciliul	Locul de muncă	Funcția

DATE DESPRE PĂRINȚI

TATĂL

NATURA RELĂȚIEI tată natural tată adoptiv tată vitreg

NUME _____

NUME ANTERIOARE _____

PRENUME _____

PRENUMELE TATĂLUI _____

NUMĂR DE IDENTIFICARE

DATA NAȘTERII

LOCUL NAȘTERII

PROFESIA, LOCUL DE MUNCĂ

CETĂȚENIA la naștere _____ actuală

DOMICILIUL PERMANENT

Localitatea

Strada _____ numărul (bloc) _____ apartamentul

Telefon fix _____ telefon mobil

Fax _____ e-mail

DOMICILIUL TEMPORAR

Localitatea

Strada _____ numărul (bloc) _____ apartamentul

Telefon fix _____ telefon mobil

Fax _____ e-mail

MAMA

NATURA RELAȚIEI mamă naturală mamă adoptivă mamă vitregă

NUME

NUME ANTERIOARE

PRENUME

PRENUMELE TATĂLUI

NUMĂR DE IDENTIFICARE

DATA NAȘTERII

LOCUL NAȘTERII

PROFESIA, LOCUL DE MUNCĂ

CETĂȚENIA la naștere _____ actuală

DOMICILIUL PERMANENT

Localitatea _____

Strada _____ numărul (bloc) _____ apartamentul _____

Telefon fix _____ telefon mobil _____

Fax _____ e-mail _____

DOMICILIUL TEMPORAR

Localitatea _____

Strada _____ numărul (bloc) _____ apartamentul _____

Telefon fix _____ telefon mobil _____

Fax _____ e-mail _____

DATE DESPRE FRAȚI/SURORI

NUME _____

NUME ANTERIOARE _____

PRENUME _____

PRENUMELE TATĂLUI _____

NUMĂR DE IDENTIFICARE _____

DATA ȘI LOCUL NAȘTERII _____

DOMICILIUL _____

PROFESIA, LOCUL DE MUNCĂ _____

NUME _____

NUME ANTERIOARE _____

PRENUME _____

PRENUMELE TATĂLUI _____

NUMĂR DE IDENTIFICARE _____

DATA ȘI LOCUL NAȘTERII _____

DOMICILIUL

PROFESIA, LOCUL DE MUNCĂ

NUME

NUME ANTERIOARE

PRENUME

PRENUMELE TATĂLUI

NUMĂR DE IDENTIFICARE

DATA ȘI LOCUL NAȘTERII

DOMICILIUL

PROFESIA, LOCUL DE MUNCĂ

NUME

NUME ANTERIOARE

PRENUME

PRENUMELE TATĂLUI

NUMĂR DE IDENTIFICARE

DATA ȘI LOCUL NAȘTERII

DOMICILIUL

PROFESIA, LOCUL DE MUNCĂ

NUME

NUME ANTERIOARE

PRENUME

PRENUMELE TATĂLUI

NUMĂR DE IDENTIFICARE

DATA ȘI LOCUL NAȘTERII

DOMICILIUL

PROFESIA, LOCUL DE MUNCĂ

ANTECEDENTE PENALE

Ați fost vreodată urmărit penal, condamnat pentru infracțiuni săvârșite cu intenție?

DA NU

Dacă ați răspuns cu da, detaliați în spațiul de mai jos, inclusiv perioadele și instituțiile care au sancționat faptele dvs., numărul și data ultimei hotărâri emise în cauza penală.

Nr. crt.	FAPTA SĂVÎRȘITĂ	PERIOADA	INSTITUȚIA	NUMĂRUL, DATA HOTĂRÎRII

DATE DE SECURITATE

Ați fost vreodată implicat în acțiuni de: spionaj, terorism, tentative de subminare a ordinii constituționale prin m violente?

Solicitantul DA NU .

Partenerul de viață DA NU .

Ați fost vreodată membru sau simpatizant al unei grupări implicate în acțiuni menționate mai sus?

Solicitantul DA NU .

Partenerul de viață DA NU .

Ați fost vreodată în relații apropiate cu o persoană care a activat sau a simpatizat cu astfel de grupări?

Solicitantul DA NU .

Partenerul de viață DA NU .

Ați participat/participați la acțiunile partidelor și asociațiilor obștești a căror activitate a fost suspendată, limita interzisă?

Solicitantul DA NU .

Partenerul de viață DA NU .

Ați fost implicat sau ați acordat sprijin activității unui stat străin, a unei organizații străine sau a reprezen acestora, precum și a cetățenilor străini și apatrizilor ce cauzează prejudicii intereselor și/sau securității Republicii Mol

Solicitantul DA NU .

Partenerul de viață DA NU .

Dacă ați răspuns cu da la vreuna dintre întrebări, detaliați mai jos.

Ați colaborat cu fostele organe de securitate care au desfășurat activități de represiune politică?

Solicitantul DA NU .

Partenerul de viață DA NU .

Considerați că ați atras atenția vreunui serviciu de informații sau de securitate străin?

Solicitantul DA NU .

Partenerul de viață DA NU .

Considerați că au fost făcute presiuni asupra dumneavoastră sau asupra membrilor familiei dumneavoaș urmare a unui incident survenit pe teritoriul altei țări?

Solicitantul DA NU .

Partenerul de viață DA NU .

Sînteți în relații permanente de natură profesională sau personală cu cetățeni străini?

Solicitantul DA NU .

Partenerul de viață DA NU .

Considerați că vi s-a solicitat vreodată să furnizați informații clasificate în afara atribuțiilor de serviciu?

Solicitantul DA NU .

Partenerul de viață DA NU .

Intenționați să vă stabiliți domiciliul permanent într-o altă țară?

Solicitantul DA NU .

Partenerul de viață DA NU .

Dacă ați răspuns cu da la vreuna dintre întrebări, detaliați mai jos.

Aveți rude apropiate, din cele menționate mai sus, care locuiesc în străinătate sau care au locuit mai mult de 6 luni în străinătate?

Solicitantul DA NU .

Partenerul de viață DA NU .

Dacă ați răspuns cu da, detaliați mai jos:

Nr. crt.	NUMELE, PRENUMELE, PRENUMELE TATĂLUI	GRADUL DE RUDENIE	ȚARA	PERIOADA

DECLARAȚIE

Subsemnatul, _____, declar că toate datele furnizate mai sus sînt autentice.

Declar că am luat cunoștință de cerințele procedurii de verificare în legătură cu perfectarea (reperfectarea) dreptului de acces la secretul de stat și le accept.

Consimt ca toate datele pe care le furnizez să fie verificate, conștient fiind de consecințele legale ale declarațiilor neautentice sau incomplete.

Mă angajez să furnizez orice date suplimentare care îmi vor fi solicitate în eventualitatea unor neclarități, precum și să informez, din proprie inițiativă, asupra oricărei modificări apărute în cele declarate mai sus.

Data _____

Semnătura _____

Numele, prenumele funcționarului
subdiviziunii resurse umane _____

Semnătura _____

Forma:
(punct
(secret după compl

Nr. _____ din _____

CHESTIONAR SUPLIMENTAR

(se completează pentru gradul de secretizare "Strict secret" și "Secret")

Instituția solicitantă _____
Forma de acces solicitată _____
Motivul solicitării _____

DATE PERSONALE ALE SOLICITANTULUI

NUME	
PRENUME	
PRENUMELE TATĂLUI	
NUMĂR DE IDENTIFICARE	
DATA NAȘTERII	
LOCUL NAȘTERII	
CETĂȚENIA actuală	
Data completării formularului de bază	

DATE SUPLIMENTARE DESPRE SOLICITANT

În afara domiciliilor, adreselor și reședințelor indicate în formularul de bază, în ultimii zece ani ați mai avut și alte
ÎN REPUBLICA MOLDOVA

Perioada _____ localitatea _____
Strada _____ numărul (bloc) _____ apartamentul _____
Perioada _____ localitatea _____
Strada _____ numărul (bloc) _____ apartamentul _____

ÎN STRĂINĂTATE

Perioada _____ țara _____ localitatea _____
Strada _____ numărul (bloc) _____ apartamentul _____
Perioada _____ țara _____ localitatea _____
Strada _____ numărul (bloc) _____ apartamentul _____

RUDE

Cumnați/cumnate

GRAD DE RUDENIE				
NUMELE ACTUAL				
NUMELE LA NAȘTERE				
NUME ANTERIOARE				
PRENUMELE				
PRENUMELE TATĂLUI				
NUMĂR DE IDENTIFICARE				
DATA NAȘTERII				
LOCUL NAȘTERII				
CETĂȚENIA ACTUALĂ				
DOMICILIUL PERMANENT				
OCUPAȚIA ACTUALĂ				

Părinții partenerului de viață (naturali, vitregi sau adoptivi):

	TATĂL		MAMA	
GRADUL DE RUDENIE				
NUMELE ACTUAL				
NUMELE LA NAȘTERE				
NUME ANTERIOARE				
PRENUMELE				
PRENUMELE TATĂLUI				
NUMĂR DE IDENTIFICARE				
DATA NAȘTERII				
LOCUL NAȘTERII				
CETĂȚENIA ACTUALĂ				
DOMICILIUL PERMANENT				
OCUPAȚIA ACTUALĂ				

STARE DE SĂNĂTATE

Ați fost vreodată diagnosticat cu boală ce prezintă contraindicații medicale pentru lucrul cu informațiile atribuite secret de stat, conform nomenclatorului aprobat de Ministerul Sănătății?

Dacă răspunsul este afirmativ, detaliați:

MĂSURI DE SIGURANȚĂ

Ați avut sau aveți probleme legate de consumul de alcool?

Dacă răspunsul este afirmativ, detaliați:

Ați consumat sau consumați substanțe care creează dependență sau droguri?

Dacă răspunsul este afirmativ, detaliați:

DECLARAȚIE

Subsemnatul, _____, declar că toate datele furnizate mai sus sînt autentice

Declar că am luat cunoștință de cerințele procedurii de verificare în legătură cu perfectarea (reperfectarea) drept de acces la secretul de stat și le accept.

Consimt ca toate datele pe care le furnizez să fie verificate, conștient fiind de consecințele legale ale declarațiilor neautentice sau incomplete.

Mă angajez să furnizez orice date suplimentare care îmi vor fi solicitate în eventualitatea unor neclarități, precum să informez, din proprie inițiativă, asupra oricărei modificări apărute în cele declarate mai sus.

Data _____

Semnătura _____

Numele, prenumele funcționarului
subdiviziunii resurse umane _____

Semnătura _____

ANGAJAMENT DE CONFIDENȚIALITATE

Subsemnatul, _____, născut la data de _____
_____ (numele, prenumele)

în localitatea _____, angajat al (angajându-mă în)

în funcția de _____, cu domiciliul în localitatea

strada _____ numărul (bloc) _____

apartamentul _____,

titular al autorizației de acces nr. _____ din

_____ *

* (se completează doar în cazul în care persoana dispune/a dispus de acces la secret de stat)

declar că am luat cunoștință de dispozițiile legale cu privire la protecția secretului de stat și **mă angajez** să le respect întocmai, să păstrez cu strictețe secretul de stat și modalitatea de asigurare a regimului secret, să nu divulg/pierd informațiile ce constituie secret de stat care mi-au fost încredințate sau îmi vor deveni cunoscute în procesul activității, inclusiv după încetarea activităților care presupun accesul la aceste informații.

Declar că am luat cunoștință de cerințele cu privire la limitarea unor drepturi în legătură cu accesul la secretul de stat, stabilite de [Legea nr.245-XVI din 27 noiembrie 2008](#) cu privire la secretul de stat și le accept.

Sînt conștient că, în cazul în care voi încălca prevederile normative privind protecția informațiilor atribuite la secret de stat, voi purta răspundere penală, civilă, administrativă sau disciplinară, conform legislației.

Data _____

Semnătura _____

Numele, prenumele

angajatului Subdiviziunii de protecție _____

Semnătura _____

Forma nr.5
(punctul 104)

(Antetul autorității publice sau al altei persoane juridice)

Nr. _____ din _____

Serviciul de Informații și Securitate
al Republicii Moldova

În vederea perfectării (reperfectării) dreptului de acces la secret de stat, forma
_____,
pentru

_____,
(numele, prenumele cetățeanului)

angajat al

_____,
(denumirea completă a instituției)

în funcția de _____, vă rugăm să inițiați măsurile de verificare necesare, în conformitate cu prevederile art.26 din [Legea nr.245-XVI din 27 noiembrie 2008](#) cu privire la secretul de stat.

Menționăm că în prezent cetățeanul deține/ nu deține autorizație de acces la secret de stat de forma _____ numărul de ordine în Nomenclatorul funcțiilor care necesită acces la secretul de stat _____ data coordonării cu SIS _____, inclusiv numărul nomenclatorului respectiv _____.

Anexăm chestionarul de bază (după caz, chestionarul suplimentar), corespunzător formei de acces solicitate, lista rudelor și persoanelor apropiate.

(Conducătorul autorității publice
sau al altei persoane juridice)

(semnătura)

Forma nr.6
(punctul 104)

Model

Lista
rudelor și persoanelor apropiate ale dlui Moraru Dumitru Ion

Nr. crt.	Gradul de rudenie	Numele, prenumele, prenumele tatălui	Ziua, luna, anul și locul nașterii	Domiciliul	Locul de muncă, funcția
1.	Angajatul	Moraru Dumitru Ion	10.03.1952, or.Cahul	or.Chișinău, str.Ismail nr.108, bloc 3, ap.20	or.Chișinău, Ministerul Agriculturii, specialist
2.	Mama	Moraru Eugenia Vasile	01.02.1926, or.Cahul	or.Chișinău, șos.Hîncești nr.15, ap.10	Pensionară
3.	Tata	Moraru Ion Teodor	15.11.1920, or.Cahul	—	Decedat în 1996
4.	Fratele	Moraru Oleg Ion	06.06.1958, or.Cahul	or.Orhei, str.Eminescu nr.24	or.Orhei, Fabrica de conserve
5.	Sora	Moraru Stela Ion	10.01.1956, or.Cahul	or.Bălți, str.Gagarin nr.30, ap.3	or.Bălți, școala nr.25, profesoară

Notă:

1. Lista trebuie să aibă formatul unei file standard: 210 mm – orizontal și 297 mm – vertical.
2. Pentru persoanele care au același nume de familie, lista se întocmește în ordine alfabetică, inclusiv după prenume și prenumele tatălui. De exemplu, pentru angajatul Moraru D.I., mama – Moraru E.V., tata – Moraru I.T., fratele – Moraru O.I., sora – Moraru S.I. Totodată, numele de fată al mamei se introduce într-o listă aparte. Sora dacă după căsătorie și-a luat numele de familie al soțului, la fel, se introduce într-o listă aparte. Dacă persoana supusă măsurilor de verificare (angajatul) este căsătorită, trebuie să se întocmească o listă aparte pentru soție, specificînd numele ei de fată.
3. Pentru persoanele cu nume dublu se întocmesc liste conform modelului de mai sus, pentru fiecare nume aparte.
4. Listele menționate nu se legalizează prin semnătura conducătorului autorității publice sau altei persoane juridice.

(Antetul Serviciului de Informații și Securitate al Republicii Moldova)

Nr. _____ din _____

(Autoritatea publică sau altă persoană juridică)

La solicitarea dumneavoastră nr. _____ din _____ vă informăm cu privire la posibilitatea/
imposibilitatea de acordare cetățeanului

_____ ,

(numele, prenumele)

angajat al

_____ ,

(denumirea completă a instituției)

în funcția de

_____ ,

dreptul de acces la secret de stat de forma

_____ ,

în temeiul art.25 alin.(1) lit. _____ din [Legea nr.245-XVI din 27 noiembrie 2008](#) cu privire la secretul de
stat, ținând cont de următoarele motive: _____ .

(se completează doar în cazul imposibilității de a acorda dreptul de acces la secret de stat)

(Conducătorul Serviciului de Informații
și Securitate al Republicii Moldova)

(semnătura)

[Forma nr.7 modificată prin Hot.Guv. nr.770 din 13.11.2024, în vigoare 14.11.2024]

Forn
(punct

(Antetul autorității publice sau al altei persoane juridice)

Nr. _____ din _____

Locu
pentru fot
(4,5 × 6

**AUTORIZAȚIE DE ACCES LA SECRET DE STAT
DE FORMA _____**

gradul (gradele) de secretizare

Prin prezenta se autorizează accesul la secret de stat pentru dl/dna _____

(numele, prenumele)

angajat în funcția de _____

Data, locul nașterii _____

Domiciliul _____

Mențiuni _____

(schimbarea numelui)

(schimbarea domiciliului)

Autorizația este valabilă pe un termen de _____

Prelungit: pînă la _____

pînă la _____.

Suspendat: de la _____ pînă la _____

de la _____ pînă la _____.

Șeful Subdiviziunii de protecție _____

(nume, prenume și semnătură)

Titular _____

(nume, prenume și semnătură)

(Conducătorul autorității publice
sau al altei persoane juridice)

(semnătura, ștampila)

Form
(punct)

Autoritatea publică sau altă persoană juridică
care a acordat dreptul de acces

Supus re:

CERTIFICAT DE ACCES LA SECRET DE STAT

de forma _____

Nr. _____ din _____

Prin prezentul se confirmă dreptul cetățeanului _____

(numele, prenumele)

de a avea acces la informații _____

(gradul de secretizare)

			concluziei Serviciului de Informații și Securitate				27.11.2008 cu privire la secretul de stat	cu privire la secretul de stat		
1	2	3	4	5	6	7	8	9	10	11

Forma nr.12
(punctele 116, 135)

(Antetul autorității publice sau al altei persoane juridice)

Nr. _____ din _____

**Serviciul de Informații și Securitate
al Republicii Moldova**

Prin prezenta vă comunicăm eliberarea (prelungirea, suspendarea, încetarea valabilității) autorizației de acces la secret de stat de forma _____, nr. _____ din _____
pentru dl/dna

(numele, prenumele)

angajat al instituției noastre în funcția de

Autorizația este valabilă (prelungită, suspendată) pe un termen de /termenul de valabilitate al autorizației a încetat la data de _____.

(Conducătorul autorității publice
sau al altei persoane juridice)

(semnătura, ștampila)

Forma
(punct

Fișa de evidență nr. _____

Numele _____

Prenumele _____

Prenumele tatălui _____

Cetățenia _____

Data și anul nașterii _____ Locul nașterii _____

Locul de muncă și funcția _____

Notă:

formatul fișei – 140 × 100 mm.

Forma nr.14
 (punctul 124)

FIȘĂ INDIVIDUALĂ DE INSTRUIRE

NUME _____

PRENUME _____

FUNCȚIA _____

SUBDIVIZIUNEA _____

FORMA DE ACCES LA SECRET DE STAT _____

Nr. crt.	Tema	Forma de instruire	Locul	Perioada	Semnătura titularului de fișă	Mențiuni

Forma
 (punct

(Antetul persoanei juridice)

Nr. _____ din _____

Comisia interdepartam
pentru protecția secretului c

CERERE
pentru eliberarea certificatului de securitate

Prin prezenta rugăm să eliberați certificatul de securitate pentru _____

(denumirea completă, forma organizatorico-juridică a persoanei juridice)

cu sediul în _____

(adresa completă)

numărul de identificare de stat _____ în vederea desfășurării activității ce ține de utilizarea inform
atribuite la secret de stat/ crearea mijloacelor de protejare a informației/ realizarea măsurilor și/sau prestarea servici
protecție a secretului de stat.

La cerere anexăm:

- formularul completat al chestionarului de securitate;
- documentele ce confirmă datele indicate în formular.

(Conducătorul persoanei juridice)

(semnătura, ștampila)

Forma
(punct

CHESTIONAR DE SECURITATE

PERSOANA JURIDICĂ SOLICITANTĂ

Denumire completă _____

Data și numărul certificatului de înregistrare de stat _____

Numărul de identificare _____

Sediul: str. _____ nr. _____ localitatea _____

Nr. telefon _____ fax _____

Telex _____ e-mail _____

Adresă Internet _____

Forma juridică de organizare _____

Capital _____

(autohton, mixt, străin)

Filiale/ reprezentanțe

Denumirea completă _____

Numărul de identificare _____

Sediul str. _____ nr. _____ localitatea _____

Nr. telefon _____ fax _____

Telex _____ e-mail _____

Adresă Internet _____

CONDUCĂTORUL PERSOANEI JURIDICE

Nume și prenume _____

Data numirii în funcție _____

Pregătire profesională _____

Data nașterii _____ localitatea _____ țara _____

SUBDIVIZIUNEA DE PROTECȚIE

Nume și prenume _____

Funcția _____

Pregătire profesională _____

Data nașterii _____ localitatea _____ țara _____

(Datele se completează pentru toate persoanele din Subdiviziunea de protecție)

DATE DESPRE UTILIZAREA SERVICIILOR PRESTATE DE SUBDIVIZIUNEA DE PROTECȚIE A ALTEI PERSOAN

JURIDICE

Denumirea completă a prestatorului _____

Data și numărul certificatului de înregistrare de stat _____

Numărul de identificare _____

Sediul: str. _____ nr. _____ localitatea _____

Nr. telefon _____ fax _____

Telex _____ e-mail _____

Adresă Internet _____

Numărul, data contractului de prestări servicii _____

Numele, prenumele, funcția persoanei care a semnat contractul în numele prestatorului _____

(Se completează în cazul în care persoana juridică nu dispune de subdiviziune de protecție proprie)

DATE DESPRE ACTIVITATEA DESFĂȘURATĂ

Genul (genurile) de activitate

Activitate licențiată (genul de activitate, seria, numărul și data eliberării licenței)

INFORMAȚII DE SECURITATE

	DA	NU
Considerați că instituția dumneavoastră a atras atenția unui serviciu de informații sau de securitate străin?		
Au existat cazuri când au fost solicitate informații cu caracter sensibil în afara atribuțiilor de serviciu?		
Instituția sau vreunul dintre angajați a fost implicat(ă) sau a sprijinit activități de:		
- spionaj		
- terorism		
Ați avut vreodată angajați care au sprijinit sau au fost implicați în una dintre activitățile de mai sus?		
Cunoașteți despre orice alte împrejurări, condiții (factori de risc) nedeclarate în răspunsurile precedente, care au putut influența activitatea dvs. sau a personalului din subordine, cum ar fi: obișnuința utilizării unor substanțe psihotrope, dependența de alcool, dificultăți financiare deosebite?		

DATE REFERITOARE LA SISTEMUL DE PROTECȚIE A INFORMAȚIILOR ATRIBUITE LA SECRET DE STAT**PROTECȚIA INFORMAȚIILOR:**Gradul de secretizare al informațiilor gestionate: **CONFIDENȚIAL, RESTRICTIONAT**LOCUL/LOCURILE UNDE SE STOCHEAZĂ DATE ȘI INFORMAȚII
ATRIBUITE LA SECRET DE STAT

	DA	NU
încăpere destinată numai protecției informațiilor		
încăpere destinată numai sistemului/subsistemului de		

calcul destinat preluării, prelucrării, stocării și transmiterii datelor și informațiilor atribuite la secret de stat		
încăperile sînt prevăzute cu: - pereți antifonați		
- uși și încuietori speciale		
- podele și tavane speciale pentru zone sensibile		
alte locuri unde se stochează date și informații sau se desfășoară activități cu caracter secret de stat		

În legătură cu acestea se vor face precizări privind poziția față de punctul de acces și control, împrejurimile, garanțiile prezintă în asigurarea protecției datelor și informațiilor ori activităților atribuite la secret de stat _____

**MĂSURI DE PROTECȚIE FIZICĂ A ÎNCĂPERILOR SAU LOCURILOR UNDE SE PĂSTREAZĂ
SAU SE STOCHEAZĂ DATE ȘI INFORMAȚII ATRIBUITE LA SECRET DE STAT
ORI ACTIVITĂȚI CU CARACTER SECRET DE STAT**

	DA	NU
Zone de securitate existente:		
Zonă de securitate clasa II (pentru gestionarea informațiilor secrete de stat cu gradul de secretizare "Confidențial", "Restricționat")		
perimetrul este clar definit și protejat, avînd toate intrările și ieșirile controlate		
accesul persoanelor neautorizate este permis conform prevederilor interne, cu însoțitori sau prin controale specifice		
Zonă administrativă (pentru manipularea și depozitarea informațiilor cu gradul de secretizare "Restricționat")		
perimetrul oferă posibilitatea de control al personalului și/sau vehiculelor		
sînt utilizate:		
- registre și jurnale speciale pentru corespondență, evidență, transport etc.		
- mape speciale de păstrare		
- sigillii		
- fișe de predare-primire		
- ecusoane de acces		
- mobilă de birou adecvată zonei administrative		
PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ȘI DE TELECOMUNICAȚII DESTINAT PRELUĂRII, PRELUCRĂRII, STOCĂRII ȘI TRANSMITERII DE DATE ȘI INFORMAȚII ATRIBUITE LA SECRET DE STAT		
Echipament de comunicație și de birotică existent (telefoane, fax, telex, xerox)		
- în zona de securitate clasa a II-a		
Echipament informatic		

- aveți acces la Internet		
- este utilizat un sistem de protecție (securizare)		
pe server-ul principal		
la nivel de utilizator		
MĂSURI PROCEDURALE DE PROTECȚIE A INFORMAȚIILOR ATRIBUITE LA SECRET DE STAT SAU A ACTIVITĂȚILOR CU CARACTER SECRET DE STAT		
Aveți elaborate proceduri privind:		
- clasificarea informațiilor după gradul de secretizare		
- accesul pentru personalul propriu		
- accesul pentru personalul din afară, inclusiv străini și reprezentanți ai mass-media		
- multiplicarea, transportul și circulația documentelor în interiorul și în afara instituției, atât în timpul, cât și în afara programului de lucru		
- protecția sistemului/subsistemului informatic și de telecomunicații		
- controlul intern, activitatea de analiză și evaluare a modului în care se respectă prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le execută, documentele ce se întocmesc și cum se execută, responsabilitățile și sancțiunile		
- instruirea personalului cu drept de acces		

PROTECȚIA PERSONALULUI

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA SECRET DE STAT						
Nr. crt.	NUME, PRENUME	DATA, LOCUL NAȘTERII	FUNCȚIA	DOMICILIU, TELEFON	FORMA DE ACCES	NOTE*

* Se va înscrie ca mențiune dacă are/urmează să aibă drept de acces la secret de stat și orice alte observații considerate necesare.

PROTECȚIA INFORMAȚIILOR:

Gradul de secretizare al informațiilor gestionate: **STRICT SECRET, SECRET**

LOCUL/LOCURILE UNDE SE STOCHEAZĂ DATE ȘI INFORMAȚII ATRIBUITE LA SECRET DE STAT	DA	NU
- încăpere destinată numai protecției informațiilor atribuite la secret de stat		
- încăpere destinată numai sistemului/subsistemului de calcul destinat preluării, prelucrării, stocării și		

transmiterii datelor și informațiilor atribuite la secret de stat		
- încăperile sînt prevăzute cu: - pereți antifonați		
- uși și încuietori speciale		
- podele și tavane speciale pentru zone sensibile		
- alte locuri unde se stochează date și informații atribuite la secret de stat sau se desfășoară activități cu caracter secret de stat		

În legătură cu acestea se vor face precizări privind poziția față de punctul de acces și control, împrejurimile, garanțiile ce le prezintă în asigurarea protecției datelor și informațiilor atribuite la secret de stat ori activităților cu caracter secret de

MĂSURI DE PROTECȚIE FIZICĂ A ÎNCĂPERILOR SAU LOCURILOR UNDE SE PĂSTREAZĂ SAU SE STOCHEAZĂ DATE ȘI INFORMAȚII ATRIBUITE LA SECRET DE STAT ORI ACTIVITĂȚI CU CARACTER SECRET DE STAT

	DA	NU
Zone de securitate existente:		
Zonă de securitate clasa I (pentru gestionarea informațiilor, inclusiv cu gradul de secretizare "Strict secret", "Secret", cu acces autorizat)		
- perimetrul este clar definit și protejat, avînd toate intrările și ieșirile controlate		
- este marcată zona, este specificată restricția și este menționată zona de securitate		
- există controlul sistemului de intrare, care permite doar accesul persoanelor autorizate pentru intrarea în zonă		
(Dacă DA, descrieți sistemul(ele) de protecție mecanică, electrică, electronică, informațională, optică, acustică etc.)		
Zonă de securitate clasa a II-a (pentru gestionarea informațiilor cu gradul de secretizare "Confidențial", "Restricționat")		
- perimetrul este clar definit și protejat, avînd toate intrările și ieșirile controlate		
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu însoțitori sau prin controale specifice		
Zonă administrativă (pentru manipularea și depozitarea informațiilor cu gradul de secretizare "Restricționat")		
- perimetrul oferă posibilitatea de control al personalului și/sau vehiculelor		
- sînt utilizate:		
registre și jurnale speciale pentru corespondență,		

evidență, transport etc.		
mape speciale de păstrare		
sigilii		
fișe de predare-primire		
ecusoane de acces		
mobilă de birou adecvată zonei administrative		

**PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ȘI DE TELECOMUNICAȚII
DESTINAT PRELUĂRII, PRELUCRĂRII, STOCĂRII ȘI TRANSMITERII DE DATE
ȘI INFORMAȚII ATRIBUITE LA SECRET DE STAT**

Echipament de comunicații și de birotică existent (telefoane, fax, telex, xerox)

- în zona de securitate clasa I

- în zona de securitate clasa a II-a

Echipament informatic		
- număr de calculatoare _____		
- utilizați calculatoarele în rețeaua Intranet		
- aveți acces la Internet		
- este utilizat un sistem de protecție (securizare)		
pe server-ul principal		
la nivel de utilizator		

** Menționați tipul server-ului principal și distribuitorul, administratorul (în cazul în care este o persoană juridică specializată care prestează servicii), precum și locul/locurile unde sînt plasate calculatoarele conectate în rețeaua la server-ul care stochează informații atribuite la secret de stat

**MĂSURI PROCEDURALE DE PROTECȚIE A INFORMAȚIILOR ATRIBUITE LA SECRET
DE STAT SAU A ACTIVITĂȚILOR CU CARACTER SECRET DE STAT**

Aveți elaborate proceduri privind:		
- clasificarea informațiilor după gradul de secretizare		
- accesul pentru personalul propriu		
- accesul pentru personalul din afară, inclusiv străini și reprezentanți ai mass-media		
- multiplicarea, transportul și circulația documentelor în interiorul și în afara întreprinderii, atît în timpul, cît și în afara programului de lucru		
- protecția sistemului/subsistemului informatic și de telecomunicații		
- controlul intern, activitatea de analiză și evaluare a modului în care se respectă prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le execută, documentele ce se întocmesc și cum se execută, responsabilitățile și sancțiunile		
- instruirea personalului cu drept de acces		

** Se va completa pentru gradul de secretizare "Strict secret".

PROTECȚIA PERSONALULUI

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII ATRIBUITE LA SECRET DE STAT

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII ATRIBUITE LA SECRET DE STAT						
Nr. ctr.	NUME, PRENUME	DATA, LOCUL NAȘTERII	FUNCȚIA	DOMICILIU, TELEFON	FORMA DE ACCES	MENȚIUNI*

* Se va înscrie ca mențiune dacă are/urmează să aibă acces și orice alte observații considerate necesare.

LISTA PERSOANELOR AUTORIZATE SĂ ADMINISTREZE SISTEMUL/ SUBSISTEMUL INFORMATIC ȘI DE TELECOMUNICAȚII, PRECUM ȘI CEI CARE LUCREAZĂ ÎN REȚEAUA INTRANET CU ACCES LA INFORMAȚIILE ATRIBUITE LA SECRET DE STAT

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SA AIBĂ ACCES LA INFORMAȚIILE ATRIBUITE LA SECRET DE STAT						
Nr. crt.	NUME, PRENUME	DATA, LOCUL NAȘTERII	FUNCȚIA	DOMICILIU, TELEFON	FORMA DE ACCES	MENȚIUNI*

* Se va înscrie echipamentul pe care-l administrează sau faptul că are acces Intranet.

DATE CU PRIVIRE LA ÎNCĂLCĂRILE LEGISLAȚIEI

	DA	NU
În ultimii 10 ani a fost intentat un proces penal împotriva întreprinderii dvs.?		
În caz de răspuns afirmativ, precizați când, de ce, denumirea instanței judecătorești, sentința, pedeapsa, perioada de executare.		
În ultimii 5 ani întreprinderea pe care o conduceți a fost acuzată de încălcarea legii?		
În caz de răspuns afirmativ, precizați când, cum, de ce, autoritatea care a constatat fapta, sancțiunea aplicată.		

Orice schimbare referitoare la datele cuprinse în chestionar se transmite imediat sub formă de completare la chestionar

Localitatea și data completării chestionarului

Funcția, numele, prenumele
conducătorului persoanei juridice

(semnătura, ștampila)

ANGAJAMENT

Subsemnatul(a),

(numele, prenumele - cu majuscule)

în calitate de

(funcția)

la

(denumirea completă a persoanei juridice)

cu sediul în localitatea

str. _____ nr.

certific pe propria-mi răspundere că informațiile declarate în prezentul chestionar sînt autentice.

Declar că personalul angajat care are/va avea acces la informații secrete de stat a luat cunoștință de prevederile legale referitoare la protecția secretului de stat și mă angajez că le voi respecta.

Am cunoștință de faptul că divulgarea/pierderea, prin orice metodă, a informațiilor încredințate care constituie secret de stat atrage răspunderea penală, civilă, administrativă sau disciplinară, conform legislației în vigoare.

Forma nr.
(punctul 1)

(Antetul Serviciului de Informații și Securitate al Republicii Moldova)

Nr. _____ din _____

**Comisia interdepartamentară
pentru protecția secretului de stat**

La solicitarea dumneavoastră nr. _____ din _____ vă informăm cu privire la îndeplinirea/

neîndeplinirea condițiilor stipulate în art.32 alin.(3) lit. __ din [Legea nr.245-XVI din 27 noiembrie 2008](#) cu privire la secretul de stat și/sau pct. _____ subpct. _____ din Regulamentul cu privire la asigurarea regimului secret în cadrul autorităților publice și al altor persoane juridice, necesare pentru desfășurarea activității legate de secretul de stat, utilizarea informațiilor avînd gradul de secretiz

la

(denumirea completă a persoanei juridice)

cu sediul în

(adresa completă)

număr de identificare de stat _____.

(Directorul Serviciului de Informații și
Securitate al Republicii Moldova)

(semnătura)

Forma nr.18
(punctul 149)

Fișa de atestare

Data atestării _____

Interviul de atestare

Întrebări	Răspunsuri

Votarea membrilor Comisiei interdepartamentale

Prezenți	Pro	Contra

Decizia _____

(atestat / neatestat)

Opinii separate

Nume, prenume	Opinie separată	Semnătura

Semnăturile membrilor Comisiei interdepartamentale

Președinte			
Vicepreședinte(ți)			
Secretar			
Membri			

--	--	--	--

Întocmit la _____
(data)

Am luat cunoștință:

(numele, prenumele conducătorului persoanei juridice, denumirea persoanei juridice)

Data _____

Semnătura _____

Forma
(punct)

**COMISIA INTERDEPARTAMENTALĂ
PENTRU PROTECȚIA SECRETULUI DE STAT**
(antetul)

Nr. _____ din _____

**CERTIFICAT
de securitate**

(gradul de secretizare al informațiilor)

Se autorizează _____

(denumirea completă a persoanei juridice)

cu sediul în _____

(adresa completă)

numărul de identificare de stat _____, în vederea desfășurării activității ce ține de utilizarea inform
atribuite la secret de stat / crearea mijloacelor de protejare a informației / realizarea măsurilor și/sau prestarea servic
protecție a secretului de stat.

Note: _____

(modificarea denumirii)

(schimbarea sediului)

(mențiuni privind contractul de folosire a serviciilor prestate de către Subdiviziunea de protecție a altei persoane juridice)

Valabil pe un termen de _____

Prelungit: pînă la _____

pînă la _____.

Suspendat: de la _____ pînă la _____

de la _____ pînă la _____.

(Președintele Comisiei interdepartamentale
pentru protecția secretului de stat)

(semnătura, ștampila)

Forma
(punctu

**COMISIA INTERDEPARTAMENTALĂ
PENTRU PROTECȚIA SECRETULUI DE STAT**

Registrul de evidență a certificatelor de securitate

Nr. crt.	Data eliberării certificatului de securitate	Denumirea completă și numărul de identificare de stat (IDNO)	Sediul persoanei juridice	Numărul și data solicitării de efectuare a expertizei speciale/ numărul și data concluziei Serviciului de Informații și Securitate	Gradul de secretizare al informațiilor utilizate	Seria și numărul de certificate de securitate	Numărul, data eliberării copiei (copiilor)	Termenul de valabilitate/ termenul prelungirii	Termenul de suspendare (de la – până la) și temeiul	Data încetării valabilității și temeiul	Numărul și data procesului-verbal de distrugere
1		2	3	4	5	6		7	8	9	10

(denumirea completă a autorității publice sau a altei persoane juridice)

Registrul de evidență a documentelor de intrare, de ieșire și a celor

Numărul de ordine și evidență	Data înregistrării	Numărul, data documentului,	Emitentul/destinatarul	Conținutul pe scurt	Numele executorului și	Numărul				Numărul carnetului de notițe, al	Mențiuni cu privire	Cui este eliberat documentul
						de exemplare	de file ale exemplare	de file ale documentelor	de file în anexă			

a docu- mentelor		gradul de secre- tizare			subdivi- ziunea		plarelor	mentului de bază		ciornelor	la dis- trugerea ciornelor	ment
1	2	3	4	5	6	7	8	9	10	11	12	13

(denumirea completă a autorității publice sau a altei persoane juridice)

**REGISTRUL UNIC
de evidență a registrelor și dosarelor finalizate**

Numărul de ordine și evidență	Gradul de secretizare	Numărul de file(fișe)	Denumirea registrlui (fișei), dosarului	Numărul volumului registrlui, dosarului	Data încheierii	Data înscrierii	Numele, prenumele persoanei responsabile de păstrarea registrlui (fișei), dosarului	Data și semnătura	Termenul de păstrare	Men Numă de inven de pr
1	2	3	4	5	6	7	8	9	10	11

Forma nr.23
(punctul 228)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

**REGISTRUL
de evidență și control**

1	2	3	4	5	6	7	8	9	10	11

Forma nr.26
(punctul 237)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

REGISTRUL
de evidență a actelor normative primite pentru informare/executare

Nr. crt.	Numărul și data actului normativ	Emitentul	Titlul	Numărul de file	Cine a luat cunoștință de actul normativ	Date privind executarea actului normativ	Restituirea actului normativ
1	2	3	4	5	6	7	8

Forma nr.27
(punctele 246, 252)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

REGISTRUL
de evidență a caietelor de lucru

Numărul de ordine și evidență	Data înregistrării	Denumirea înscrierilor efectuate	Gradul de secretizare	Numărul de caiete	Cui a fost eliberat (subdiviziunea, numele, prenumele)	Recipisa de primire a executantului, data	Recipisa de restituire a angajatului Subdiviziunii de protecție, data	Mențiuni
1	2	3	4	5	6	7	8	9

Forma nr.28
(punctele 250, 379)

(parafa de secretizare)

FIȘA DE EVIDENȚĂ
a documentelor (dosarelor) eliberate

tipul documentului (dosarului), conținutul succint

numărul de evidență, data, gradul de secretizare

numărul exemplarului (volumului), numărul de foi

Data eliberării	Cui a fost eliberat (subdiviziunea, numele, prenumele executantului)	Numărul de file ale documentului (dosarului) aduse la cunoștința executantului	Recipisa de primire sau de informare, data	Recipisa de restituire, data
1	2	3	4	5

Forme nr.29
(punctele 252, 639)

(parafa de secretizare)

CONTUL PERSONAL nr. _____

Executantul

(numele, prenumele)

Subdiviziunea

funcția

Data	Denumirea documentului sau denumirea/ semnul convențional al articolului	Numărul de exemplare (unități) eliberate	Numărul de inventar sau alt număr de evidență al articolului	Recipisa de primire, data	Semnătura persoanei care a predat documentul/ articolul	Recipisa de restituire, data
1	2	3	4	5	6	7

Forma nr.30
(punctul 255)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

**REGISTRUL
de evidență a ștampilelor**

Numărul de ordine și evidență	Data de înregistrare	Numărul de fabricație	Cui este eliberat (subdiviziunea, numele, prenumele)	Recipisa de primire de către executant, data primirii	Recipisa de restituire de către angajatul Subdiviziunii de protecție, data restituirii	Mențiuni
1	2	3	4	5	6	7

(denumirea completă a autorității publice sau a altei persoane juridice)

**REGISTRUL
de evidență a documentelor întocmite**

Numărul de evidență	Data de înregistrare	Gradul de secretizare	Tipul și conținutul succint al documentului	Subdiviziunea, numele, prenumele executantului	Numărul carnetului special de notițe și al ciornelor	Numărul de exemplare întocmite	Numărul de file în exemplar	Recipisa de primire a documentului și ciornelor de la executant, data	Mențiuni cu privire la distrugerea ciornelor	Transmisi	
										Unde/cui a fost transmis documentul	Numărul de exemplare
1	2	3	4	5	6	7	8	9	10	11	12

Notă:

1. La înregistrarea scrisorii de însoțire, în rubrica 4 se indică numărul de evidență a anexelor (în cazul în care are anexa).
2. La expedierea anexelor, în rubrica 13 se indică numărul scrisorii de însoțire.

Forma nr.32
(punctul 267, 365)

(parafa de secretizare)

de evidență a documentelor întocmite

Numărul de evidență	Data înregistrării	Gradul de secretizare	Tipul și conținutul succint al documentului	Subdiviziunea, numele, prenumele executantului	Numărul carnetului special de notițe și al ciornelor
1	2	3	4	5	6

Unde/cui a fost transmis documentul	Numărul de exemplare	Numărul de file în exemplar	Numărul de ieșire și data	Documentul este clasat		Mențiuni cu privire la controlul disponibilului de documente, data
				Numărul dosarului, volumului	Numărul de file	
1	2	3	4	5	6	7

Numărul de exemplare întocmite	Numărul de file în exemplar	Recipisa de primire a documentului și ciornelor de la executant, data	Mențiuni cu privire la distrugerea ciornelor	Mențiuni cu privire la distrugerea documentului			
				Numărul de exemplare și numerele acestora	Numărul de file în exemplar	Numărul total de file	Numărul și data procesului-verbal de distrugere
1	2	3	4	5	6	7	8

Forma nr.33
(punctul 285)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

REGISTRUL
de evidență a plicurilor

Numărul și data registrului (borderoului, inventarului etc.) de distribuire	Numărul de plicuri	Numărul de ordine a plicurilor și parafa de secretizare aplicată pe acestea	Numerele documentelor indicate pe plic	Semnătura curierului care a distribuit corespondența, data și ora	Semnătura angajatului Subdiviziunii de protecție, data și ora primirii plicului
1	2	3	4	5	6

Forma
(punctele 29:

(parafa de secretiz

FIȘA nr. _____
de evidență a documentelor recepționate

Numărul și data de intrare	Numărul și data documentului recepționat	Gradul de secretizare	Numărul de file și numărul de exemplare		Numărul dosarului, volumului în care este clasat documentul și numărul de file. Numărul și data procesului-verbal cu privire la distrugerea		Mențiu privire contro disponibili document
			documentul de bază	anexa	documentului de bază	anexei	
1	2	3	4	5	6	7	8

De unde a parvenit: _____

Tipul și conținutul succint (informații secrete nu se includ):

Circulația documentului (semnătura, data):

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Forma nr.37
(punctul 302)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

REGISTRUL
de evidență a documentelor

Numărul de ordine și evidență	Data de intrare	De la cine a fost recepționat (numele, prenumele, subdiviziunea)	Numărul de evidență și data documentului recepționat	Nu-mărul de exemplare	Nu-mărul total de file	Tipul și conținutul succint	Cine l-a semnat	Unde și cui este transmis	Data trans-miterii	Numărul de inventar sau al recipisei	În care dosar este clasată copia	Men-țiuni
1	2	3	4	5	6	7	8	9	10	11	12	13

Forma nr.38
(punctul 313)

_____ (parafa de secretizare)

FOAIE DE COMANDĂ nr. _____
privind multiplicarea documentelor secrete

Subdiviziunea _____

Forma multiplicare _____

Numărul de ordine și evidență a originalului	Gradul de secretizare	Numărul de file ale originalului	Numărul necesar de exemplare	Numărul de exemplare multiplicare	Numărul de file în exemplar	Numărul de file rebutate	Mențiuni cu privire la distrugerea rebutului
1	2	3	4	5	6	7	8

Șeful Subdiviziunii de protecție

_____ (numele, prenumele, funcția persoanei care a aprobat multiplicarea)

_____ semnătura, data

_____ semnătura, data

Forma nr.39
(punctul 318)

_____ (parafa de secretizare)

_____ (denumirea completă a autorității publice sau a altei persoane juridice)

REGISTRUL
de evidență a foilor de comandă

						exe- cutant	corec- tare, tipărire, broșare etc.)	imprimări de de corectură etc.)				rialului)	
1	2	3	4	5	6	7	8	9	10	11	12	13	14

REGISTRUL
de evidență a edițiilor secrete

Numărul de ordine	Denumirea ediției	Numărul ediției	Gradul de secreti- zare	Au fost editate sau primite				La distribuire		La res
				De unde a parvenit/ de cine a fost editat	Numărul de intrare a scrisorii de însoțire (foii de comandă), data	Numărul de exem- plare	Numererele exem- plarelor	Unde și cui a fost transmis	Numărul și data documentului de ieșire, data (numărul dosarului în care este clasată scrisoarea de distribuie)	Numărul de exemplare numerele acestora
1	2	3	4	5	6	7	8	9	10	11

APROBAT

NOMENCLATORUL DOSARELOR

(denumirea completă a autorității publice sau a altei persoane juridice)

pentru anul _____

Numărul de ordine și evidență	Indicele subdiviziunii	Denumirea dosarului	Gradul de secretizare	Numele executantului căruia i s-a acordat dreptul de a utiliza dosarul	Numărul volumului	Data		Numărul de file	Termenul de păstrare și articolul conform listei	Mențiuni cu privire la circulație	
						deschiderii	încheierii			Unde se păstrează, numele responsabilului pentru păstrare	F
1	2	3	4	5	6	7	8	9	10	11	

Șeful Subdiviziunii de protecție

(semnătura)

Forma nr.44
(punctele 380, 384)

(parafa de secretizare)

Inventarul interior al dosarului
nr. _____ nr. volum _____ anul _____

Nr. crt.	Numărul documentului		Numărul exemplarului	Tipul (denumirea) documentului, de unde a parvenit	Numărul de file în dosar	Date cu privire la executarea documentului din dosar și locul aflării acestuia
	de intrare	pregătit (de ieșire)				
1	2	3	4	5	6	7

În inventar sînt incluse în total

(numărul în cifre și litere)

documente pe

_____ file.

(numărul în cifre și litere)

Din dosar au fost extrase

_____ file,

(numărul în cifre și litere)

în schimb au fost incluse _____ adevărîțe de substituire.

(numărul în cifre și litere)

Inventarul a fost întocmit de

(numele, prenumele, funcția angajatului Subdiviziunii de protecție care a întocmit inventarul, semnătura, data)

Notă:

Pe o foaie separată, cusută la sfârșitul dosarului, se face o înscriere cu următorul conținut:

“În total în dosar (volum) au fost numerotate, cusute și sigilate
_____ file.

(numărul în cifre și litere)

Inventar intern al documentelor pe

_____ file,

(numărul în cifre și litere)

întocmit de

(numele, prenumele, funcția angajatului Subdiviziunii de protecție care a întocmit inventarul, semnătura, data)

Forma

(punctu

(parafa de secretiza

ADEVERINȚĂ DE SUBSTITUIRE

Documentul(ele) _____

(denumirea)

cu gradul de secretizare _____, cusut(e) la dosarul nr. _____ volumul nr. _____ pe file _____
luat(e) în evidență cu nr. _____ din _____, avînd _____ file, inclusiv anexa(e) pe _____
fost retras(e) din prezentul dosar și:

1) cusut(e) la dosarul nr. _____, volumul nr. _____, filele _____, pentru anul _____

2) transmis(e) _____ la data _____

(cui)

cu numărul de ieșire _____, copia căruia este cusută la dosarul nr. _____, volumul nr. _____, filele _____

3) eliberat(e) pentru utilizare provizorie _____

(cui și conform cărui număr de evidență)

4) distrus(e) _____

(numărul și data procesului-verbal)

Retragerea documentului(elor) a fost permisă de _____

(numele, prenumele, funcția, semnătura, data)

Documentul(ele) au fost retras(e) din dosar de _____

(numele, prenumele, funcția)

(data)

(semnătura)

Documentul(ele) a (au) fost primit(e) pentru _____

(expediere, cusut în alt dosar, transmis executantului)

(numele, prenumele, funcția)

(data)

(semnătura)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

REGISTRUL
de evidență a materialelor de broșate

Numărul de ordine și evidență	Data de înregistrare	Gradul de secretizare	Denumirea documentului	De unde a parvenit (de care subdiviziune este înțocmit)	Numărul de intrare, data scrisorii de însoțire sau numerele de inventar incluse în document	Numărul de exemplare	Numărul de file în document	Numele exemplarelor	Transmise		Mențiuni cu privire la distrugere (numărul și data procesului-verbal)	M
									Unde și cui	Numărul de ieșire și data scrisorii de însoțire		
1	2	3	4	5	6	7	8	9	10	11	12	

(parafa de secretizare)

APROBAT

(numele, prenumele, funcția)

(semnătura)

PROCES-VERBAL nr. _____ din _____
cu privire la distrugerea documentelor/dosarelor

Comisia în următoarea componență: _____

(numele, prenumele, funcția)

a selectat pentru distrugere următoarele documente (dosare), care și-au pierdut importanța practică și nu au valoare istorică sau altă valoare.

Nr. crt.	Tipul evidenței, numărul de evidență, data documentului (dosarului)	Gradul de secretizare	Denumirea documentului (dosarului)	Numărul de exemplare (volume)	Numărul exemplarelor	Numărul de file în exemplar (volum)	Numărul total c
1	2	3	4	5	6	7	8

Notă cu privire la documentele extrase:

tipul documentelor, din care dosare sînt extrase (numărul de înregistrare, denumirea

documentelor, numerele dosarelor și filelor), în care dosare noi și la care numere de

file sînt cusute documentele extrase sau înregistrate în registrele anului în curs.

În total urmează a fi distruse _____
(numărul în litere)

denumiri de documente, în _____
(numărul în litere)

exemplare, dosare în _____ VO
(numărul în litere)

Membrii comisiei: _____
(semnătura)

Avizat _____

(semnătura)

(semnătura)

Înscrierile efectuate în procesul-verbal au fost confruntate cu datele de evidență verificate de _____

(numele, prenumele, funcția, semnătura)

Înainte de a fi distruse, documentele (dosarele) au fost confruntate cu datele înscrise în procesul-verbal și au fost distruse pe cale _____.

Ziua, luna, anul _____

Membrii comisiei: _____
(semnătura)

(semnătura)

(semnătura)

Înscrierile în registrele de evidență cu privire la distrugerea documentelor (dosarelor) au fost efectuate de _____

(numele, prenumele, funcția, semnătura)

Ziua, luna, anul _____

(denumirea completă a autorității publice sau a altei persoane juridice)

REGISTRUL
de evidență preliminară a documentației tehnice secrete

Nu- mărul de ordine	Data de înregis- trare	Gradul de secre- tizare	Denu- mirea	Semnul distin- ctiv (mar- cajul)	Tipul docu- mentului (manu- cris, original, copie)	Numărul filelor luate în evidență	Cui sînt eliberate (recipisa de primire, data)	Resti- tuite (reci- pisa de restit- uire, data)	Multiplicat			Transmis	
									Nu- mărul foii de co- mandă	Nu- mărul de exem- plare	Numărul exem- plarelor	Numărul de ieșire și data expe- scrisorii de însoțire	Cui sînt expe- diate
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Forma nr.49
(punctul 506)

(parafa de secretizare)

FIȘA
de evidență preliminară a documentației tehnice secrete

Subdiviziunea	Denumirea	Semnul distinctiv (marcajul)	Gradul de secretizare	Numărul de evidență preliminară
1	2	3	4	5

Data înregistrării	Tipul documentului (manuscris, original)	Numărul de file luate în evidență	Cui sînt eliberate	Recipisa de primire, data	Recipisa de restituire, data	Date despre luarea în evidență de inventar	Numărul și data procesului-verbal de distrugere
1	2	3	4	5	6	7	8

--	--	--	--	--	--	--	--

Executarea copiilor și duplicatelor					Distrugerea				Luat în evidență preliminară
Data	Numărul foii de comandă	Tipul documentului (copie, duplicat)	Numărul de exemplare	Numărul de file în document	Data	Numărul procesului-verbal	Numărul exemplarului	Numărul de file în document	
1	2	3	4	5	6	7	8	9	10

Verso Fișei

Duplicatul sau numărul de ordine al exemplarului copiei	La transmitere				La restituire		
	Destinatarul	Numărul de ieșire a scrisorii de însoțire	Data	Emitentul	Numărul de intrare a scrisorii de însoțire	Data	Numărul de file în document
1	2	3	4	5	6	7	8

Forma nr.50
(punctul 525)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

**REGISTRUL
de evidență a circulației fișelor**

Numărul de ordine și evidență	Data de înregistrare	Gradul de secretizare	Denumirea subdiviziunii și numele executantului	Mențiuni cu privire la circulația fișelor	Mențiuni cu privire la verificare	Mențiuni
1	2	3	4	5	6	7

(denumirea completă a autorității publice sau a altei persoane juridice)

(denumirea completă a autorității publice sau altei persoane juridice)

REGISTRUL
de evidență a articolelor secrete

Numărul de ordine și evidență	Data de înregistrare	Denumirea sau semnul convențional	Numărul de fabricație (individual)	Gradul de secretizare	Numărul de intrare și data scrisorii de însoțire	De unde a parvenit/ în care subdiviziune este luat în evidență	Recipisa reprezentantului Subdiviziunii de protecție pentru primirea fișei de evidență a articolului	În care subdiviziune es transmis articol secret					
1	2	3	4	5	6	7	8	9	10	11	12	13	

Forma nr.59
(punctul 637)

(parafa de secretizare)

REGISTRUL (FIȘA)
de evidență numerică a articolelor secrete

Denumirea sau semnul convențional al articolului _____marcajul

Unitatea _____ de _____ măsură

Numărul de ordine și evidență	Data	De unde a parvenit/ unde este transmis	Numărul foi de însoțire, data	Recepționat	Transmis	Reziduuri	Mențiuni
1	2	3	4	5	6	7	8

Notă: Pentru fiecare denumire sau semn convențional de articol secret se rezervă spațiu suficient în registru (pagini, file) sau poate fi atribuit un registru aparte.

(parafa de secretizare)

FIȘA DE EVIDENȚĂ
pe articol

Denumirea sau semnul convențional al articolului

Numărul de fabricație

Data eliberării articolului	Subdiviziunea	Numele, prenumele recepționarului	Semnătura	Semnătura persoanei care l-a eliberat	Recipisa de restituire	Mențiuni
1	2	3	4	5	6	7

Distrus conform procesului-verbal nr. _____ din _____

Transmis cu foaia de însoțire nr. _____ din _____

(parafa de secretizare)

REGISTRUL
de evidență privind eliberarea articolelor

Secția

Sectorul

Data	Numele persoanei care a recepționat articolul	Denumirea sau semnul convențional al articolului	Numărul de unități eliberate	Numărul de fabricație sau de inventar al articolului	Recipisa de primire	Semnătura persoanei care a predat articolul	Recipisa de restituire, data
1	2	3	4	5	6	7	8

Cotorul registrului nr. _____
Registrul a fost primit _____
(data)

(parafa de secretizare)

(data)

Secția _____

Sectorul _____

Registrul nr. _____

de predare a articolului _____

prin _____

(cui)

(numele, prenumele persoanei care a recepționat articolul)

Denumirea sau semnul convențional al articolului	Numărul de fabricație	Mențiuni
1	2	3

Total articole _____

(numărul de bucăți cu litere)

A predat _____

A recepționat _____

Forma nr.6

(punctul 64:

(parafa de secretizare)

Secția _____

(data)

**FOAIE
de însoțire**

la predarea articolelor

(cui)

prin _____

(numele, prenumele beneficiarului)

Denumirea sau semnul convențional al articolului	Numărul de fabricație	Mențiuni
1	2	3

În total articole și fișe de evidență la ele

(numărul în litere)

A predat _____

(șeful subdiviziunii, numele, prenumele)

A recepționat _____

(șeful subdiviziunii, numele, prenumele)

(semnătura)

(semnătura)

Forma
(punct

(parafa de secretizare)

APROBAT

(numele, prenumele, funcția)

(semnătura)

(data)

PROCES-VERBAL

nr. _____ din _____

Subsemnații, _____

(numele, prenumele, funcția)

am montat următoarele elemente secrete de completare:

Nr. crt.	Denumirea sau semnul convențional al articolului	Gradul de secretizare	Numărul de evidență a articolului	Piese de completare montate în ar	
				Denumirea sau semnul convențional	Numărul fabricației
1	2	3	4	5	6

Semnăturile: _____

În registrul de evidență, mențiunea despre montare a fost efectuată de către

(numele, prenumele, funcția)

Forma
(punctu

(parafa de secretiza

APROBAT

(numele, prenumele, funcția)

(semnătura)

(data)

PROCES-VERBAL

nr. _____ din _____

Subsemnații, _____

(numele, prenumele, funcția)

am retras (înlocuit) următoarele elemente secrete de completare – montate anterior:

Nr. crt.	Elementele de completare retrase (înlocuite) din articolul:			Denumirea sau semnul convențional al elementului retras (înlocuit)	Gradul de secretizare	Numărul de evidență	Elementul retras (înlocuit) este supus distrugerii sau este luat în evidență	Num: proces verba privin distruș sau nu de evic
	denumirea sau semnul convențional al articolului	gradul de secretizare	numărul de fabricație					
1	2	3	4	5	6	7	8	9

Semnăturile: _____

În registrul de evidență, mențiunea despre retragerea (înlocuirea) piesei de completare a fost efectuată de către

(numele, prenumele, funcția)

(parafa de secretizare)

EXPEDITOR**DESTINATAR**

FOAIE
de însoțire nr. _____

Prin

(numele, prenumele însoțitorului)

În

Denumirea sau semnul convențional al articolului/ gradul de secretizare	Evidența contabilă	Numărul lotului	Tipul ambalajului	Numărul de locuri	Unitatea de măsură	Numărul		Prețul	Suma	
						transmis	recepționat de destinatar			
							în cifre			în litere
1	2	3	4	5	6	7	8	9	10	11

A predat:

A primit:

A recepționat: _____

(însoțitor)

V

Mențiuni speciale

Numărul locului	Numărul plumburilor	Plumburile			
		Numărul cleștelui de plumbuit	Textul ampretei	Numărul cleștelui de plumbuit	Textul ampre
1	2	3	4	5	6

Responsabil pentru expediere _____

(semnătura)

Data _____

Articolele menționate în foaia de însoțire, în număr de _____ locuri, plumbuite într-un ambalaj intact au fost recepționate

(data)

(semnătura)

Mențiunile Subdiviziunii de protecție:

Documentele au fost transmise la _____, numărul de ieșire _____
(data)

Articolele au fost transmise conform inventarului nr. _____ din _____

Forma nr.67
(punctul 668)

(parafa de secretizare)

Dispoziție de expediție nr. _____
pentru livrarea articolelor secrete _____

Șeful secției _____

COTORUL DISPOZIȚIEI nr. _____ ora _____
Primită la data de _____
Merceologul secției _____

Rugăm să livrați la

(denumirea întreprinderii)

Articolul

(denumirea sau semnul convențional)

Furnizorul _____ se află la adresa

Termenul de recepționare a articolului

Permisul se va comanda

la _____

Numărul de locuri _____, greutatea _____ kg, mărimea
locului:

lungimea _____, lățimea _____, înălțimea _____

Tipul ambalajului

Specificul transportării

Conducătorul

(data)

(semnătura)

Verso

Mențiuni
privind executarea dispoziției

1. Încărcătura a fost livrată de

2. Încărcătura a fost recepționată în întregime de

(numele, prenumele, semnătura, data)

3. Documentele de însoțire au fost primite de

(numele, prenumele, semnătura, data)

4. Încărcătura a fost livrată la data _____, la ora

Expeditorul _____
(semnătura)

A verificat merceologul _____
(semnătura)

Forma nr.68
(punctul 671)

(parafa de secretizare)

FOAIE DE AMBALAJ
pentru transmiterea articolelor secrete

(expeditorul)
în ambalajul nr. _____

(data)

Nr. crt.	Denumirea sau semnul convențional	Numărul de fabricație	Numărul de inventar	Gradul de secretizare	Numărul de inventar și data documentelor de însoțire (formular, pașaport etc.)	Mențiuni
1	2	3	4	5	6	7

Responsabil de ambalaj

Reprezentantul Subdiviziunii de control tehnic

Beneficiar

Forma
(punctu

APROB

(data)

PROCES-VERBAL
nr. _____ din _____
cu privire la distrugerea articolelor secrete

Comisia în următoarea componență _____
(numele, prenumele, funcția)

a verificat articolele secrete enumerate mai jos, rebutate în procesul producerii sau exploatării, și a stabilit necesitatea distrugerii acestora.

Nr. crt.	Denumirea sau semnul convențional	Numărul de fabricație	Numărul de inventar	Numărul de unități, greutatea	Gradul de secretizare	Numărul de inventar al pașaportului (formularului)	Menț
1	2	3	4	5	6	7	8

(data)

Semnăturile: _____

Articolele secrete sînt distruse prin _____

(data)

Semnăturile: _____

Înainte de a fi distruse, numerele de evidență ale articolelor secrete au fost verificate cu datele indicate în procesul verbal.

Angajatul (reprezentantul) Subdiviziunii de protecție _____

Înscrierile în registrele (fișele) de evidență cu privire la distrugerea articolelor secrete au fost efectuate

_____, la _____
(numele, prenumele, funcția, semnătura) (data)

(parafa de secretizare)

(autoritatea publică)

CARNETUL nr. _____
BLANCHETA nr. _____
MESAJ CIFRAT DE IEȘIRE nr. _____

Expeditor _____

(denumirea subdiviziunii)

Destinatar _____

Numărul de expediere _____

(data)

Executat _____

primit la ora _____, data _____

(numele, prenumele)

cifrat la ora _____, data _____

(subdiviziunea)

A cifrat _____

Tel. _____

(semnătura)

Forma nr.71

(punctul 735)

(parafa de secretizare)

REGISTRUL
de evidență a mesajelor cifrate transmise

Numărul de ordine și evidență	Gradul de secretizare	Data semnării	Cui este adresat	Conținutul succint	Numele, prenumele executantului, subdiviziunea	Numărul formularului	Numărul de inventar conform căruia mesajul a fost transmis organului de cifrare, data, cui a este transmis (recipisa de primire, data)
-------------------------------	-----------------------	---------------	------------------	--------------------	--	----------------------	--

1	2	3	4	5	6	7	8

Forma
(punctu

(parafa de secretiza

REGISTRUL
de evidență a mesajelor cifrate primite

Numărul de ordine și evidență	Data de înregistrare	Gradul de secretizare	Numărul de intrare al mesajului, data	De unde a parvenit și cine a semnat	Conținutul succint	Numărul de expediere al mesajului, data	Numărul exemplarului	Cui a fost transmis pentru executare, recipisa de primire, data	Recipisa de restituire, data	Nu inv cor că f trat me org, cif dat a trat (re pri d
1	2	3	4	5	6	7	8	9	10	

Forma nr.73
(punctul 803)

parafa de secretizare

(după completare, în funcție de gradul de secretizare a informațiilor pe care le cuprinde)

(antetul autorității publice sau al altei persoane juridice)

APROBAT

(funcția, numele și prenumele conducătorului autorității publice sau al altei persoane juridice)

(semnătura și ștampila)

PROGRAMUL DE PREVENIRE A SCURGERII DE INFORMAȚII ATRIBUITE LA SECRET DE STAT

(denumirea autorității publice sau a altei persoane juridice)

Capitolul I BAZA LEGALĂ

Se va menționa cadrul normativ care a stat la baza întocmirii Programului de prevenire a scurgerii de informații atribuite la secret de stat (în continuare – Program).

Capitolul II GENERALITĂȚI

Secțiunea 1

Prezentare generală

Se va face o scurtă prezentare a autorității publice sau a altei persoane juridice, a reprezentanțelor și filialelor. Vor fi prezentate elementele de concretizare a identității, statutul juridic, obiectul de activitate.

Secțiunea a 2-a

Obiective

Vor fi prezentate obiectivele urmărite prin măsurile prezentate în Program.

Vor fi vizate următoarele obiective minime:

- apărarea informațiilor atribuite la secret de stat împotriva acțiunilor de divulgare, pierdere, sustragere, distrugere neautorizată sau alterare;
- prevenirea accesului neautorizat la astfel de informații, a cunoașterii și răspândirii lor ilegale;
- înlăturarea riscurilor și vulnerabilităților ce pot pune în pericol protecția informațiilor atribuite la secret de stat;
- asigurarea cadrului procedural necesar protecției informațiilor atribuite la secret de stat.

Secțiunea a 3-a

Principii

Se precizează principiile care stau la baza măsurilor de prevenire a scurgerii de informații.

Măsurile de prevenire a scurgerii de informații se bazează pe:

- autorizarea accesului la informațiile atribuite la secret de stat absolut necesare activității (principiul “necesității de a lucra cu informații atribuite la secret de stat”);
- asigurarea aplicării măsurilor de protecție, în mod diferențiat, pe zone de securitate și în funcție de forma de acces la secret de stat;
- accesul la informațiile atribuite la secret de stat este permis numai în baza verificărilor corespunzătoare;
- aplicarea, în mod obligatoriu și unitar, a măsurilor de protecție atât în locurile în care se depozitează informațiile atribuite la secret de stat și în cazul sistemelor informatice care stochează, prelucrează sau transmit informații de acest fel, cât și a persoanelor care au acces la acestea și a utilizatorilor rețelelor respective;
- răspunderea personală privind aplicarea măsurilor de protecție stipulate prin programul de prevenire a scurgerii de informații atribuite la secret de stat.

Capitolul III INFORMAȚII ATRIBUITE LA SECRET DE STAT

Secțiunea 1

Elemente generale privind informațiile atribuite la secret de stat deținute de autoritatea publică sau altă persoană juridică

Se vor face precizări privind gradele de secretizare a informațiilor deținute de autoritatea publică sau altă persoană juridică (în cazul celor primite de la alți emitenți se va menționa baza juridică a deținerii, respectiv, tipul contractului și dacă s-au asumat obligații de protejare a secretului de stat prin încheierea de acorduri între părți).

Secțiunea a 2-a

Lista informațiilor atribuite la secret de stat

Autoritățile publice sau alte persoane juridice vor întocmi lista informațiilor atribuite la secret de stat în baza Nomenclatorului informațiilor atribuite la secret de stat, care va include categoriile informațiilor pe care le dețin și gradul de secretizare al acestora (documente, date, obiecte sau activități, indiferent de suportul material sau formă).

Lista va fi actualizată ori de câte ori situația o impune (secretizarea sau desecretizarea unor informații).

Secțiunea a 3-a

Locurile unde se stochează permanent sau temporar informații atribuite la secret de stat sau se desfășoară astfel de activități

(conform anexei nr.1 la Program)

Vor fi menționate:

- spațiile destinate păstrării documentelor secrete;
- spațiul destinat sistemului/rețelelor informatice de procesare automată a datelor care preiau, prelucrează, stochează și transmit date și informații atribuite la secret de stat;
- alte locuri unde se gestionează sau se utilizează informații atribuite la secret sau se desfășoară astfel de activități.

Capitolul IV

Accesul la secret de stat

Secțiunea 1

Lista funcțiilor care necesită acces la secret de stat

Vor fi precizate funcțiile care necesită accesul la informațiile atribuite la secret de stat, pe grade de secretizare. Se va face referință la Nomenclatorul funcțiilor care necesită acces la secretul de stat, aprobat de conducătorul autorității publice sau al altei persoane juridice respective.

Secțiunea a 2-a

Prezentarea Structurii de protecție a informațiilor atribuite la secret de stat

Pentru fiecare persoană în parte se vor preciza:

- numele, prenumele, numărul de identificare;
- nume anterioare;
- data și locul nașterii, profesia, funcția, domiciliul, telefonul);

Atribuțiile privind asigurarea protecției informațiilor atribuite la secret de stat.

Secțiunea a 3-a

Prezentarea persoanelor care au sau urmează să aibă acces la informații atribuite la secret de stat

Va fi întocmită lista cu persoanele care au sau urmează să aibă acces la informații atribuite la secret de stat pe grade de secretizare (inclusiv cele care lucrează în sistemul informatic și de telecomunicații, destinat preluării, prelucrării, stocării și transmiterii de informații atribuite la secret de

stat). Numărul persoanelor nominalizate în lista respectivă va fi cel mult egal cu cel al funcțiilor care necesită acces la informațiile atribuite la secret de stat.

Pentru fiecare persoană nominalizată vor fi precizate:

- numele, prenumele, numărul de identificare, alte date de identificare (nume anterioare, data și locul nașterii, profesia, funcția, domiciliul, telefonul);
- informațiile atribuite la secret de stat care îi sînt absolut necesare activității, cu precizarea gradului de secretizare a acestora.

Listele respective vor fi actualizate, cu îndeplinirea procedurilor legale de coordonare, în funcție de necesități (extinderea sau limitarea accesului unor persoane la informații atribuite la secret de stat, în funcție de modificarea atribuțiilor de serviciu).

Capitolul V PROTECȚIA FIZICĂ

Secțiunea 1

Măsurile de protecție fizică a clădirilor, spațiilor/locurilor unde se păstrează și se utilizează informații atribuite la secret de stat sau se desfășoară astfel de activități

(conform anexei nr.2 la Program)

Vor fi stipulate măsuri privind:

- securitatea clădirilor;
- controlul intrărilor și ieșirilor;
- paza;
- safeurile, dulapurile de metal, ambalajele, alți suportți speciali și încăperile de securitate;
- încuietorile;
- controlul cheilor și combinațiilor;
- dispozitivele de detectare a intrușilor;
- protecția fizică a copiatoarelor și dispozitivelor telefax;
- planurile de urgență.

Secțiunea a 2-a

Măsuri procedurale de protecție a informațiilor ori a activităților secrete

Vor fi prezentate:

- reguli de evidență, procesare, utilizare, accesare, multiplicare, transmitere, păstrare și stocare a informațiilor atribuite la secret de stat, indiferent de suportul material (aprobat de conducerea autorității publice sau altei persoane juridice);
- reguli de acces pentru personalul propriu;
- reguli de acces pentru personalul/persoanele din afara autorității publice sau altei persoane juridice.

Capitolul VI

PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ȘI DE TELECOMUNICAȚII DESTINAT PRELUĂRII, PRELUCRĂRII, STOCĂRII ȘI TRANSMITERII DE INFORMAȚII ATRIBUITE LA SECRET DE STAT

Vor fi prezentate echipamentele de comunicații și birotică (telefoane, fax, telex, copiatoare) prin care vor fi transmise/prelucrate informații atribuite la secret de stat.

Vor fi prezentate, de asemenea, echipamentul informatic existent, calculatoarele conectate la Internet, sistemele de protecție utilizate și instituția prestatoare de servicii pentru întreținerea sau instalarea programelor (conform anexei nr.3 la Program).

În situația în care unele dintre aceste echipamente nu sînt protejate corespunzător, se va face precizarea că folosirea acestora pentru prelucrarea informațiilor atribuite la secret de stat este interzisă.

Capitolul VII

MĂSURI DE PROTECȚIE ÎMPOTRIVA OBSERVĂRII ȘI ASCULTĂRII

Zonele în care se elaborează și/sau se discută informații atribuite la secret de stat trebuie protejate împotriva observării și ascultării pasive și/sau active. Responsabilitatea înlăturării riscurilor privind observarea și ascultarea revine autorității publice sau altei persoane juridice, care elaborează sau, după caz, gestionează informații atribuite la secret de stat (conform anexei nr.4 la Program).

Capitolul VIII

CONTROALE

Secțiunea 1

Controale, activități de analiză și evaluare a modului în care se respectă prevederile legale referitoare la protecția informațiilor atribuite la secret de stat

Vor fi prezentate tematica și periodicitatea controalelor (inopinate, periodice), cine le execută, documentele ce se întocmesc și forma răspunderii pentru încălcarea reglementărilor privind protecția informațiilor atribuite la secret de stat.

Se va întocmi planificarea activităților de evaluare și analiză a stării de protecție a informațiilor atribuite la secret de stat și se va prevedea ca anual, după încheierea operațiunii de verificare a disponibilului documentelor și altor purtători materiali de informații atribuite la secret de stat, să se analizeze și să se evalueze modul în care au fost respectate prevederile Programului, prevăzându-se măsurile care se impun și termenele de remediere a unor nereguli constatate.

Secțiunea a 2-a

Soluționarea cazurilor de încălcare a prevederilor legale referitoare la protecția informațiilor atribuite la secret de stat

(conform anexei nr.5 la Program)

Se vor face referiri la:

- măsurile ce vor fi luate în cazul constatării încălcării prevederilor legale referitoare la protecția informațiilor atribuite la secret de stat;
- evidența încălcărilor reglementărilor de securitate;
- comunicarea divulgării sau pierderii informațiilor atribuite la secret de stat;
- scoaterea de la evidență a documentelor secrete pierdute sau distruse.

Capitolul IX

MĂSURI DE INSTRUIRE A PERSOANELOR CARE AU ATRIBUȚII DE ASIGURARE A REGIMULUI SECRET ȘI A CELOR CARE AU ACCES LA INFORMAȚII ATRIBUITE LA SECRET DE STAT

(conform anexei nr.6 la Program)

Se vor preciza:

- situațiile care impun asemenea măsuri;
- responsabilitățile;
- mijloacele și metodele de instruire.

Planul specific de pregătire a personalului este elaborat la începutul fiecărui an. În conținutul acestuia vor fi menționate responsabilitățile, termenele, mijloacele și metodele de instruire și educație protectivă. Subdiviziunea de protecție va ține evidența instruirilor/activităților de educație protectivă și va asigura pregătirea tuturor persoanelor care au sau urmează să aibă acces la informațiile atribuite la secret de stat, care nu au participat la instruirile organizate.

Întocmit

(numele, prenumele și semnătura șefului Subdiviziunii de protecție)

Răspunderea pentru întocmirea, avizarea și aplicarea Programului de prevenire a scurgerii de

informații atribuite la secret de stat revine conducătorului autorității publice sau altei persoane juridice deținătoare de informații atribuite la secret de stat.

Programul de prevenire a scurgerii de informații atribuite la secret de stat se actualizează, anual sau ori de câte ori este necesar (identificarea unor noi riscuri și vulnerabilități, apariția unor noi situații sau acte normative etc.), modificările efectuate aducându-se de fiecare dată la cunoștință organului competent pentru protecția secretului de stat, căruia se transmite sub formă de completare pentru a fi avizat.

Programul se întocmește în 2 exemplare (un exemplar se păstrează la titular și unul la organul competent pentru protecția secretului de stat).

Anexa nr. 1
la Programul de prevenire a scurgerii
de informații atribuite la secret de stat

Locurile unde se stochează permanent sau temporar informații atribuite la secret de stat sau se desfășoară astfel de activități

De la caz la caz, pentru fiecare zonă administrativă, zonă de securitate sau încăpere în care se desfășoară activități, se lucrează cu/se gestionează informații atribuite la secret de stat vor fi menționate măsurile de securitate protectivă existente și garanțiile pe care le prezintă în protecția informațiilor și activităților secrete. De asemenea, se vor menționa sarcinile și atribuțiile ce trebuie îndeplinite, conform regulamentului de organizare și funcționare internă.

Măsurile de protecție fizică a încăperilor și locurilor unde se păstrează sau se utilizează informații atribuite la secret de stat sau se desfășoară astfel de activități se vor organiza și implementa în funcție de zonele de securitate. Accesul în zonele de securitate și încăperile în care se derulează activități ori se lucrează cu informații atribuite la secret de stat va fi permis exclusiv persoanelor care au drept de acces la secret de stat de forma corespunzătoare gradului de secretizare al informațiilor respective, cu respectarea principiului "necesității de a lucra cu informații atribuite la secret de stat".

Zonele în care sînt utilizate sau stocate informații atribuite la secret de stat trebuie organizate și administrate în așa fel încît să corespundă uneia dintre următoarele categorii:

a) zona de securitate clasa I, care presupune că orice persoană aflată în interiorul acesteia are acces la informații secrete de stat, de gradul "Strict secret" și "Secret". O asemenea zonă necesită:

- un perimetru clar delimitat și protejat, în care toate intrările și ieșirile sînt supravegheate;
- controlul sistemului de intrare, care să permită numai accesul persoanelor verificate corespunzător și autorizate în mod special;

- indicarea gradului de secretizare a informațiilor existente în zonă;

b) zona de securitate clasa a II-a, care presupune că gestionarea informațiilor cu gradul de secretizare "Confidențial" și "Restricționat" se realizează prin aplicarea unor măsuri specifice de protecție împotriva accesului persoanelor neautorizate.

O asemenea zonă necesită:

- perimetru clar delimitat și protejat, în care toate intrările și ieșirile sînt supravegheate;
- controlul sistemului de intrare, pentru a permite accesul neînsoțit numai persoanelor verificate și autorizate să pătrundă în această zonă. Pentru toate celelalte persoane trebuie să existe reguli de însoțire, supraveghere și prevenire a accesului neautorizat la informații atribuite la secret de stat sau în sectoare în care sînt gestionate și stocate astfel de informații.

Încăperile în care nu se lucrează zilnic 24 de ore vor fi inspectate după orele de program, pentru a verifica dacă informațiile atribuite la secret de stat sînt asigurate în mod corespunzător;

c) Zona administrativă

În jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilită o zonă administrativă cu perimetru vizibil definit, în interiorul căreia să existe posibilitatea de control al personalului și vehiculelor.

În zona administrativă sînt permise gestionarea și păstrarea numai a informațiilor restricționate.

Anexa nr.2
la Programul de prevenire a scurgerii
de informații atribuite la secret de stat

**Măsurile de protecție fizică a clădirilor, spațiilor/locurilor unde se păstrează
și se utilizează informații atribuite la secret de stat sau se desfășoară
astfel de activități**

Securitatea clădirilor

Clădirile, spațiile/locurile în care se află informații atribuite la secret de stat trebuie protejate împotriva accesului neautorizat.

Măsurile de protecție (grilaje la ferestre, încuietori la uși, pază la intrări, sisteme automate pentru controlul accesului, controale și patrule de securitate, sisteme de alarmă sau pentru detectarea intrușilor etc.) vor fi dimensionate în raport cu:

- a) gradul de secretizare al informațiilor, suportul, volumul și modul de depozitare a acestora în clădire;
- b) tipul safeurilor, dulapurilor de metal, ambalajelor și altor suporturi în care sînt păstrate (depozitate) informațiile;
- c) locul de amplasare a spațiilor/locurilor unde se păstrează sau se concentrează informații atribuite la secret de stat ori se desfășoară astfel de activități;
- d) caracteristicile clădirii.

Controlul intrărilor și ieșirilor

Intrările în zonele de securitate clasa I și clasa a II-a vor fi controlate prin permis de intrare sau printr-un sistem special de recunoaștere personală aplicat personalului permanent, în mod obligatoriu se va institui un sistem de control al vizitatorilor pentru prevenirea accesului neautorizat la informațiile atribuite la secret de stat.

Se recomandă ca permisul de intrare să nu arate, în clar, identitatea autorității publice sau altei persoane juridice emitente ori locul în care deținătorul are acces. Controlul intrărilor și ieșirilor poate fi însoțit de un sistem de identificare automată, care trebuie considerat suplimentar, fără a presupune o înlocuire totală a pazei.

Dacă se apreciază necesar, la intrarea sau la ieșirea din zonele de securitate clasa I sau clasa a II-a, se vor efectua controale pentru depistarea și/sau prevenirea tranzitării fără drept a informațiilor și materialelor atribuite la secret de stat.

Paza

Folosirea paznicilor pentru asigurarea zonelor de securitate și a informațiilor atribuite la secret de stat se va face numai după ce au fost verificați, li s-a acordat autorizația de acces corespunzător zonei și li s-a efectuat pregătirea de specialitate. Vor fi precizate inclusiv măsuri de control și supraveghere corespunzătoare a paznicilor.

Patrulările în zonele de securitate clasa I și clasa a II-a se vor realiza în afara orelor de program și în zilele nelucrătoare, la intervale care vor fi stabilite în funcție de amenințarea locală, pentru a exista garanția că informațiile atribuite la secret de stat sînt protejate în mod corespunzător.

Pentru eficientizarea sistemelor de pază, în special în zonele de securitate, unde, în interesul securității, paznicii nu pot avea intrare directă, trebuie asigurate măsuri menite să prevină accesul neautorizat și să detecteze eventualele încercări de pătrundere fără drept în aceste perimetre, prin folosirea unor modalități adecvate (televiziune cu circuit închis, sisteme de alarmă sau pentru inspecție vizuală). De la caz la caz, astfel de modalități pot fi folosite și ca substitute ale patrulelor.

Safeuri, dulapuri de metal, ambalaje, alți suportți speciali și încăperi de securitate

Safeurile, dulapurile de metal, ambalajele, alți suportți speciali folosite pentru păstrarea informațiilor atribuite la secret de stat se împart în trei clase:

- clasa A: autorizate la nivel național pentru depozitarea informațiilor cu gradul de secretizare "Strict secrete" în zone de securitate clasa I sau clasa a II-a;
- clasa B: autorizate la nivel național pentru păstrarea informațiilor cu gradul de secretizare "Secret", "Confidențial" și "Restricționat" în zone de securitate clasa I sau clasa a II-a;
- clasa C: mobilier de birou adecvat numai pentru păstrarea informațiilor secrete de serviciu.

Încăperile de securitate sînt construite (amenajate) în zone de securitate clasa I sau clasa a II-a, unde informațiile atribuite la secret de stat sînt păstrate pe rafturi deschise sau sînt expuse pe hărți, diagrame etc. Pereții, podelele, plafoanele, ușile și încuietorii acestor încăperi vor oferi o protecție echivalentă clasei safeului, dulapului de metal, ambalajului, altui suport special de securitate autorizat pentru păstrarea informațiilor respective.

Încuietori

Încuietorii folosite la safeurile, dulapurile de metal, ambalajele, alți suportți speciali și încăperile de securitate în care sînt păstrate informații atribuite la secret de stat se împart în trei grupe, astfel:

- grupa A: încuietori autorizate pentru safeurile, dulapurile de metal, ambalajele, alți suportți speciali din clasa A;
- grupa B: încuietori autorizate pentru safeurile, dulapurile de metal, ambalajele, alți suportți speciali din clasa B;
- grupa C: încuietori indicate pentru mobilierul de birou adecvat numai pentru păstrarea informațiilor cu gradul de secretizare "Restricționat" (pentru clasa C).

Controlul cheilor și combinațiilor

Cheile safeurilor, dulapurilor de metal, ambalajelor, altor suportți și încăperilor de securitate nu trebuie scoase din clădirea sau zona de securitate în care se află documentele secrete.

Combinațiile încuietorilor (safeurilor, dulapurilor de metal, ambalajelor, altor suportți de securitate) vor fi cunoscute numai de persoanele abilitate.

Pentru cazurile de urgență, un rînd de chei suplimentare (o evidență scrisă a fiecărei combinații) vor fi păstrate în plicuri opace sigilate într-o subdiviziune stabilită de conducerea autorității publice sau altei persoane juridice, sub control corespunzător, în ambalaje separate. Evidența fiecărei combinații trebuie păstrată în plic separat. Cheilor și plicurilor trebuie să li se asigure protecție corespunzător gradului de secretizare a informațiilor la care acestea permit accesul.

Cunoașterea combinațiilor încuietorilor de la containerele de securitate va fi restrînsă la un număr minim de persoane. Cheile și combinațiile vor fi schimbate:

- a) ori de cîte ori are loc o schimbare de personal;
- b) de fiecare dată cînd se constată că au intervenit situații de natură să le facă vulnerabile;
- c) la intervale regulate, de preferință o dată la șase luni (fără a se depăși 12 luni).

Dispozitive de detectare a intrușilor

Cînd se folosesc sisteme de alarmă, televiziune cu circuit închis sau alte dispozitive destinate supravegherii zonelor de securitate sau protecției informațiilor atribuite la secret de stat, sursa de alimentare trebuie să aibă atît conectare permanentă, cît și de rezervă (eventual, o baterie reîncărcabilă).

Orice defectare sau intervenție neautorizată asupra acestor sisteme trebuie să declanșeze o alarmă sau un alt sistem de avertizare pentru personalul care monitorizează instalația respectivă.

Protecția fizică a copiatoarelor și dispozitivelor telefax

Copiatoarele și dispozitivele telefax trebuie protejate fizic, în măsura în care este necesar să se

garanteze folosirea lor numai de către persoanele autorizate.

Planuri de urgență

Fiecare autoritate publică sau altă persoană juridică va pregăti planuri pentru protejarea informațiilor atribuite la secret de stat în cazuri de urgență, care să prevadă inclusiv evacuarea și distrugerea acestora atunci când este cazul.

Protecția, evacuarea și/sau distrugerea materialelor cu gradul de secretizare "Strict secret", în cazuri de urgență, vor avea totdeauna prioritate față de alte documente secrete.

Anexa nr.3

la Programul de prevenire a scurgerii
de informații atribuite la secret de stat

Protecția sistemelor/subsistemelor informatice destinate preluării, prelucrării, stocării și transmiterii de date și informații atribuite la secret de stat și a încăperilor în care acestea sînt plasate

- Administratorul și utilizatorii sistemului destinat preluării, prelucrării, stocării și transmisiei de date și informații atribuite la secret de stat sînt numiți de conducătorul autorității publice sau altei persoane juridice.

- Administratorul, utilizatorii și persoanele care au acces la date și informații atribuite la secret de stat, procesate prin sisteme de prelucrare automată a datelor, sînt supuși măsurilor de verificare și autorizare corespunzător gradelor de secretizare a informațiilor la care au acces.

- Încăperile unde sînt plasate sisteme/subsisteme informatice destinate preluării, prelucrării, stocării și transmisiei de date și informații atribuite la secret de stat vor fi asigurate cu sisteme de supraveghere și control al accesului potrivit reglementărilor în vigoare, corespunzător gradului de secretizare al informațiilor.

- Sistemul/subsistemul informatic destinat preluării, prelucrării, stocării și transmisiei de date și informații atribuite la secret de stat va fi prevăzut cu sistem de secretizare prin metode, mijloace și echipamente pentru asigurarea integrității, confidențialității și accesibilității acestora.

- Utilizarea sistemelor informatice care preiau, prelucrează, stochează și transmit informații atribuite la secret de stat se face pe bază de parole, coduri și chei de criptare care se păstrează în plicuri sigilate la dispoziția conducătorului autorității publice sau al altei persoane juridice.

- Accesul în sistemul/subsistemul informatic destinat preluării, prelucrării, stocării și transmiterii de date și informații atribuite la secret de stat se atribuie, individual și diferențiat, în conformitate cu activitatea fiecărui utilizator pentru pornirea, utilizarea și oprirea sistemului de calcul, introducerea, citirea, modificarea, ștergerea sau transferul de date în/din bazele de date ale sistemului informatic, gestionarea și utilizarea cheilor de criptare/decriptare.

- Consultarea, introducerea, modificarea sau ștergerea informațiilor din baza de date se efectuează numai cu aprobarea conducătorului autorității publice sau al altei persoane juridice, asigurîndu-se o evidență strictă, în scopul realizării eventualei examinări ulterioare a activității, a interacțiunii utilizatorilor cu sistemele de calcul, prin memorarea momentului, tipului operației, codului utilizatorului și datelor accesate de acesta.

- Elaborarea de lucrări din bazele de date ale sistemului/subsistemului destinat preluării, prelucrării, stocării și transmiterii de date și informații atribuite la secret de stat se efectuează numai pe baza dispozițiilor conducerii autorității publice sau a altei persoane juridice, emise pe adrese sau documente interne de lucru.

Suportii de memorie externă (discurile, discurile portabile, dischetele, benzile magnetice, casetele de bandă magnetică, compact-discurile, discurile optice sau magneto-optice), utilizați în sistemul/subsistemul destinat preluării, prelucrării, stocării și transmiterii de date și informații atribuite la

secret de stat, au regimul documentelor secrete și se păstrează la compartimentul de documente secrete, fiind supuși procedurilor restrictive identice acestora.

- Instalarea, depanarea sau modificarea configurației sistemului de calcul destinat preluării, prelucrării, stocării și transmiterii de date și informații atribuite la secret de stat se execută de personalul verificat și autorizat cu drept de acces la secret de stat.

- Săptămînal, administratorul sistemului informatic destinat preluării, prelucrării, stocării și transmiterii de date și informații atribuite la secret de stat va elimina fișierele temporare de lucru sau ieșite din uz și va verifica integritatea fișierelor stocate pe discuri.

- Intrarea și ieșirea atît a persoanelor, cît și a materialelor vor fi controlate.

- În încăperile în care sistemul/subsistemul poate fi modificat nu se va permite accesul unui singur angajat autorizat (se va institui "regula celor doi").

- Persoanele care solicită acces temporar sau intermitent în aceste încăperi vor obține aprobare de vizitator de la administratorul de sistem; vizitatorii trebuie supravegheați permanent pentru a preveni accesul în scopuri ilicite la echipamentele informatice.

Un pericol în domeniul protecției informațiilor atribuite la secret de stat procesate, stocate și transmise prin sistemul de prelucrare automată a datelor îl reprezintă orice acțiune, inacțiune sau împrejurare de natură să afecteze integritatea, accesibilitatea sau confidențialitatea datelor, precum și funcționalitatea programelor și echipamentelor aferente unui sistem informatic.

Constituie pericole:

- pierderea, sustragerea, înlocuirea, alterarea sau distrugerea neautorizată ori accidentală a datelor, programelor, suporturilor materiali ai acestora sau a echipamentelor aferente;

- operarea greșită în timpul preluării, prelucrării, transferului, stocării sau arhivării datelor;

- interceptarea și interpretarea transmisiilor efectuate în cadrul rețelei de calculatoare;

- forțarea accesului, accesul neautorizat sau întârzierea accesului autorizat la date, programe, suportii materiali ai acestora sau la echipamentele aferente;

- eludarea restricțiilor privind accesul la date, prin modificarea neautorizată a configurațiilor instalate, programelor sau a drepturilor de acces;

- copierea neautorizată a datelor;

- interceptarea și interpretarea radiațiilor electromagnetice sau acustice produse de echipamentele de calcul, dispozitivele de transmisiuni sau canalele de comunicație;

- interceptarea discuțiilor sau convorbirilor telefonice referitoare la sistemul informatic;

- exploatarea informativă a personalului implicat în dezvoltarea, întreținerea sau exploatarea sistemului informatic;

- introducerea în exploatare a produselor informatice fără o testare prealabilă care să ofere garanții de funcționare corectă și controlată;

- păstrarea, amplasarea, exploatarea, întreținerea sau depozitarea în condiții improprii a sistemelor de calcul, purtătorilor materiali de date sau a dispozitivelor și echipamentelor destinate asigurării protecției și securității datelor;

- nerespectarea reglementărilor referitoare la secretul de stat sau a regulilor de divizare a muncii;

- nerespectarea regulilor privind depozitarea, utilizarea sau distrugerea suporturilor de memorie externă și a dispozitivelor și echipamentelor scoase din uz;

- nerespectarea prevederilor, metodologiilor și a documentațiilor tehnice de întreținere și exploatare a sistemelor informatice;

- apariția de anomalii în funcționarea sistemelor de operare, pachetelor de programe sau programelor de aplicații;

- apariția de anomalii în funcționarea sistemelor informatice;

- apariția de deranjamente ale canalelor de comunicație;

- discutarea în condiții de insecuritate sau cu persoane neautorizate a unor aspecte privind sistemele de calcul, informațiile și datele înmagazinate;

- producerea de calamități naturale (cutremure, inundații, alunecări de teren etc.);

- producerea de evenimente cu efect distructiv (explozii, incendii, spargeri de conducte, acțiuni

teroriste, acte de vandalism, șocuri electromagnetice etc.);

- producerea pe orice cale de evenimente cu efecte similare.

Posibile pericole, amenințări ori atacuri la adresa securității sistemului/rețelelor informatice:

- ascultare pasivă (atac contra confidențialității): accesarea sistemului în scopul modificării informațiilor generate, transmise, stocate sau afișate pe componentele vulnerabile ale acestuia;

- intercepta: penetrarea neautorizată a sistemului în scopul modificării informațiilor transmise pe o cale de comunicație;

- deducerea prin interferență: acțiunea unui utilizator autorizat de a corela informațiile la care are acces, în scopul deducerii unor informații atribuite la secret de stat la care nu are dreptul de acces;

- deghizarea ("înșelarea" mecanismelor de autentificare): însușirea și folosirea identității unui utilizator autorizat pentru accesarea sistemului;

- crearea și utilizarea unor canale disimulate ("ocolirea" controalelor de acces) în scopul transmiterii de informații de la un utilizator autorizat către unul neautorizat;

- utilizarea "porții secrete" (trap-desk) pentru evitarea controalelor de acces.

Anexa nr.4

la Programul de prevenire a scurgerii
de informații atribuite la secret de stat

Măsuri de protecție împotriva observării și ascultării

Protecția împotriva ascultărilor pasive (posibile prin ascultare directă sau furnizate de comunicații nesigure) se realizează pe baza asistenței tehnice din partea instituțiilor abilitate, prin izolarea fonică a pereților, ușilor, podelelor și plafoanelor zonelor sensibile.

Protecția împotriva ascultărilor active (prin microfoane, emițători radio și alte dispozitive implantate) necesită inspecții de securitate tehnică și/sau fizică a structurii încăperii, accesoriilor, instalațiilor tehnico-sanitare, echipamentelor și mobilierului de birou, sistemelor de comunicații etc. Aceste inspecții vor fi realizate de instituții competente.

Zone sigure din punct de vedere tehnic

Accesul în zonele protejate împotriva ascultărilor se va controla în mod special.

Încăperile vor fi încuiate sau păzite corespunzător cerințelor de securitate fizică, inclusiv când nu sînt ocupate, iar cheile vor fi tratate ca materiale cu caracter secret. Periodic, se vor organiza inspecții fizice și/sau tehnice. De asemenea, astfel de inspecții se vor organiza, în mod obligatoriu, ca urmare a oricărei intrări neautorizate, a unei suspiciuni privind accesul personalului extern și după executarea lucrărilor de reparații, întreținere, zugrăvire, redecorare etc. Nici un obiect nu se va introduce în aceste zone, fără a fi verificat de către personalul specializat în depistarea dispozitivelor de ascultare.

În mod curent, în zonele asigurate din punct de vedere tehnic nu se vor instala telefoane. Totuși, când instalarea acestora este absolut necesară, trebuie prevăzute cu un dispozitiv de deconectare pasiv.

Inspecțiile de securitate tehnică în zonele unde se poartă discuții extrem de sensibile trebuie întreprinse, în mod obligatoriu, premurgător începerii convorbirilor, atît pentru identificarea fizică a dispozitivelor de ascultare, cît și pentru verificarea sistemelor telefonice, electrice sau de altă natură, care ar putea fi folosite ca mediu de atac.

Verificarea dotărilor electrice/electronice din birouri

Înainte de a fi folosite în zonele în care se lucrează ori se discută despre informații cu gradul de secretizare "Strict secrete" și "Secrete", echipamentele de comunicații și dotările de orice fel din birouri, în principal cele electrice și electronice, trebuie verificate de specialiști în securitatea comunicațiilor, pentru a preveni transmiterea ilicită sau din neglijență a unor informații inteligibile.

În aceste zone se va organiza o evidență a tipului și numărului de inventar ale fiecărei piese de

mobilier sau echipament introduse sau mutate din încăperi, care va fi păstrată sub cheie, iar cheile vor fi protejate corespunzător.

Anexa nr.5
la Programul de prevenire a scurgerii
de informații atribuite la secret de stat

Soluționarea cazurilor de încălcare a prevederilor legale referitoare la protecția informațiilor atribuite la secret de stat

Cazurile de încălcare a prevederilor legale referitoare la protecția informațiilor atribuite la secret de stat vor fi comunicate imediat conducătorului autorității publice sau altei persoane juridice și organului competent pentru protecția secretului de stat.

Orice încălcare a prevederilor legale referitoare la protecția informațiilor atribuite la secret de stat va fi cercetată de persoane special desemnate, cu experiență în activitatea de securitate, pentru a stabili:

- dacă și în ce mod au fost compromise informațiile atribuite la secret de stat;
- dacă persoanele neautorizate care au avut sau ar fi putut avea acces la informații atribuite la secret de stat prezintă suficientă încredere și loialitate, astfel încât rezultatul compromiterii să nu creeze prejudicii;
- măsurile de remediere, corective sau disciplinare (inclusiv juridice), care sînt recomandate.

În situația în care persoanele care au luat cunoștință de conținutul informațiilor atribuite la secret de stat prezintă încredere, vor fi instruite în mod corespunzător pentru a preveni răspîndirea acestor informații, în caz contrar se va proceda la evaluarea prejudiciului rezultat și vor fi întreprinse măsurile necesare diminuării acestuia.

Evidența încălcărilor prevederilor legale

În cadrul autorităților publice și altor persoane juridice, deținătoare de informații atribuite la secret de stat, se va organiza evidența cazurilor de încălcare a prevederilor legale, a rapoartelor de investigații și măsurilor corective întreprinse. Aceste evidențe vor fi păstrate timp de trei ani de către Subdiviziunea de protecție și vor fi puse la dispoziție în timpul controalelor efectuate de reprezentanții autorizați ai organului competent pentru protecția secretului de stat.

Comunicarea compromiterilor

Informațiile atribuite la secret de stat sînt compromise atunci cînd conținutul acestora (total sau parțial) este cunoscut de persoane neautorizate (care nu au autorizare valabilă de acces la acestea) ori cînd au fost supuse riscului acestei cunoașteri neautorizate (informațiile atribuite la secret de stat pierdute, chiar și temporar, în afara unei zone de securitate sînt considerate a fi compromise).

Organul competent pentru protecția secretului de stat va fi încunoscîntat prin cel mai operativ sistem de comunicare asupra circumstanțelor compromiterii unor astfel de informații.

Scopul principal al comunicării compromiterii este de a da posibilitatea recuperării informațiilor, evaluării prejudiciilor și întreprinderii acțiunilor necesare sau aplicabile pentru minimalizarea consecințelor.

Informarea preliminară trebuie să conțină:

- a) o descriere a informațiilor respective (gradul de secretizare, numărul de înregistrare, numărul de exemplare, conținutul, data, emitentul);
- b) o scurtă prezentare a circumstanțelor în care a avut loc compromiterea, inclusiv data constatării, perioada în care informațiile au fost expuse compromiterii și, dacă se cunoaște, persoanele neautorizate care au avut sau ar fi putut avea acces la acestea;
- c) precizări cu privire la eventuala informare a autorității publice cu împuterniciri de dispoziție asupra acestora.

La solicitarea organului competent pentru protecția secretului de stat, informările preliminare vor fi completate pe măsura derulării cercetărilor.

Evaluările proprii ale autorităților publice sau altor persoane juridice, referitoare la prejudiciile și acțiunile ce urmează a fi întreprinse pentru înlăturarea sau diminuarea acestora, vor fi prezentate în cel mai scurt timp organului competent pentru protecția secretului de stat.

Scoaterea din evidență a documentelor secrete pierdute sau distruse

Cînd există indicii certe, confirmate în scris de instituțiile abilitate cu atribuții de control și investigare a compromiterii informațiilor atribuite la secret de stat, că documentul dat în răspundere este iremediabil pierdut (și nu rătăcit), acesta va fi scos din evidență, numai după finalizarea cercetărilor, cu avizul instituțiilor abilitate.

Anexa nr.6
la Programul de prevenire a scurgerii
de informații atribuite la secret de stat

Măsurile de instruire a persoanelor care au atribuții de asigurare a regimului secret și a celor care au acces la informații atribuite la secret de stat (educație protectivă)

Educația protectivă are ca principal obiectiv instruirea persoanelor care au acces la informații atribuite la secret de stat în vederea aplicării măsurilor legale referitoare la protejarea secretului de stat.

Educația personalului se realizează prin derularea unor activități specifice în cadrul cărora persoanelor care au drept de acces la secret de stat le sînt prezentate:

- prevederile legislației în domeniul protecției informațiilor atribuite la secret de stat;
- conținutul Programului de prevenire a scurgerii de informații atribuite la secret de stat;
- competențele organului competent pentru protecția secretului de stat;
- aspectele semnificative privind protecția secretului de stat cu relevanță în domeniul specific de activitate;
- mijloacele și metodele utilizate de structurile specializate în culegerea de informații atribuite la secret de stat;
- consecințele nerespectării normelor legale în domeniu;
- alte elemente de interes pentru siguranța națională.

Ca mijloace frecvent utilizate în procesul de educație protectivă pot fi folosite documentare, filme de specialitate, diapozitive, materiale publicitare etc.

Forma nr.74
(punctul 807)

(parafa de secretizare)

(denumirea completă a autorității publice sau a altei persoane juridice)

REGISTRUL **de evidență a safeurilor, dulapurilor de metal, ambalajelor,** **altor suportți speciali și a cheilor de la acestea**

Numărul	Denumirea	Clasa	Numărul	Locul	Ce se	Numărul	Numele,	Recipisa	Recipisa	Men-
---------	-----------	-------	---------	-------	-------	---------	---------	----------	----------	------

