

VENDIM
Nr.690, datë 5.10.2011

PËR MIRATIMIN E RREGULLORES “PËR MBROJTJEN KRIPTOGRAFIKE TË INFORMACIONIT TË KLASIFIKUAR “SEKRET SHTETËROR””

Në mbështetje të nenit 100 të Kushtetutës dhe të neneve 25 e 31 të ligjit nr.8457, datë 11.2.1999 “Për informacionin e klasifikuar “Sekret shtetëror””, të ndryshuar, me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e rregullores “Për mbrojtjen kriptografike të informacionit të klasifikuar “Sekret shtetëror””, sipas tekstit që i bashkëlidhet këtij vendimi.

2. Vendimi nr.14, datë 28.1.2002 i Këshillit të Ministrave “Për miratimin e rregullores “Për shërbimin shifrar të Republikës së Shqipërisë””, shfuqizohet.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTRI
Sali Berisha

RREGULLORE
PËR MBROJTJEN KRIPTOGRAFIKE TË INFORMACIONIT TË KLASIFIKUAR
“SEKRET SHTETËROR”

KREU I
RREGULLA TË PËRGJITHSHME

Neni 1
Objekti

Objekti i këtij vendimi është përcaktimi i strukturave kriptografike, detyrat që ato kryejnë dhe rregullat që zbatohen për sigurimin kriptografik të informacionit të klasifikuar “sekret shtetëror” në institucionet shtetërore të Republikës së Shqipërisë.

Neni 2
Mbështetja ligjore

1. Ligji nr.8457, datë 11.2.1999 “Për informacionin e klasifikuar “sekret shtetëror””, i ndryshuar.

2. Vendimi i Këshillit të Ministrave nr.922, datë 17.12.2007 “Për sigurimin e informacionit të klasifikuar “sekret shtetëror” që prodhohet, ruhet, përpunohet apo transmetohet në sistemet e komunikimit”.

3. Vendimi i Këshillit të Ministrave nr.121, datë 15.3.2001 “Për rregullat e sigurimit fizik të informacionit të klasifikuar”, i ndryshuar.

4. Vendimi i Këshillit të Ministrave nr.122, datë 15.3.2001 “Për shqyrtimin e pastërtisë dhe për dhënien e “Certifikatës së sigurisë” personave që do të njihen me informacionin e klasifikuar “sekret shtetëror””, i ndryshuar.

5. Vendimi i Këshillit të Ministrave nr.81, datë 28.1.2008 "Për përcaktimin e kriterëve dhe të procedurave për asgjësimin e informacionit të klasifikuar "sekret shtetëror""

Neni 3

Elementet e sigurisë

1. “Siguria kriptografike” është aplikimi i masave të sigurisë ndaj informacionit të klasifikuar “sekret shtetëror”, që qarkullon në kanalet e komunikimit masiv dhe publik, me qëllim mbrojtjen nga persona të paautorizuar.

2. Parimi “Nevojë për njohje” është parimi, sipas të cilit njohja me sistemet kriptografike lejohet vetëm për personelin e autorizuar dhe të pajisur me certifikatë sigurie të përshtatshme.

3. “Përgjegjësi individuale” do të thotë që çdo përdorues përgjigjet për sigurimin dhe kontrollin e materialit kriptografik që ka në administrim. Përdoruesi që ka të drejtën e njohjes dhe përdorimit të materialit kriptografik trajnohet dhe praktikohet. Përdoruesit e autorizuar për njohjen e sistemeve kriptografike nuk duhet të shpërndajnë informacionin kriptografik te persona të tjerë të paautorizuar.

Neni 4

Përkufizime

Për efekt të kësaj rregulloreje, termat e mëposhtëm kanë këtë kuptim:

1. “Kriptografi” është praktika e sigurimit të konfidencialitetit, integritetit, autenticitetit, disponibilitetit të informacionit të klasifikuar nëpërmjet kriptimit dhe dekriptimit të tij.

2. “Material kriptografik” përfshin çelësat në të gjitha format e tyre, dokumentet, pajisjet që përmbajnë informacion kriptografik e që janë të rëndësishëm për kriptimin dhe dekriptimin e informacionit.

3. “Kriptim” është procesi i transformimit të informacionit në mënyrë të tillë që të fsheh përmbajtjen e tij.

4. “Dekriptim” është procesi i kundërt i kriptimit.

5. “Mbrojtja kriptografike” është aplikimi i metodave dhe mjeteve kriptografike për fshehjen e përmbajtjes së informacionit.

6. “Çelës kriptografik” është variabël transformimi, i cili përdoret gjatë kriptimit-dekriptimit të informacionit.

7. “Algoritëm kriptografik” është metodë që mundëson kriptimin dhe dekriptimin e informacionit.

8. “Pajisje kriptografike” nënkupton pajisje teknike ose software (program) që përdoren për mbrojtjen kriptografike të informacionit.

9. “Sisteme kriptografike” nënkupton tërësinë e pajisjeve kriptografike dhe materialeve kriptografike të përdorura si një njësi e vetme për të realizuar procesin kriptografik sipas rregullave përkatëse për administrimin e tyre.

10. “Incident kriptografik” konsiderohet çdo veprim ose mosveprim që cenon sigurinë e sistemeve kriptografike, komprometimin e procesit kriptografik dhe leximin e informacionit të klasifikuar.

11. “Komprometim i informacionit” nënkupton vënien në dispozicion në mënyrë të qëllimshme ose jo të materialit kriptografik, personave të paautorizuar, si rrjedhojë e humbjes, vjedhjes, spiunazhit, rikuperimit, defekteve të materialit kriptografik, shikimit, fotografimit etj., dhe që cenon konfidencialitetin, disponibilitetin dhe integritetin e informacionit të klasifikuar. Çdo rast komprometimi trajtohet si incident kriptografik.

12. “Përdorues të pajisjeve kriptografike” janë punonjësit që për kryerjen e detyrave të tyre kërkojnë akses në materialet kriptografike dhe kryejnë proceset kriptografike të

informacionit të klasifikuar “sekret shtetëror”.

KREU II STRUKTURAT KRIPTOGRAFIKE

Neni 5

Strukturat kriptografike të përcaktuara dhe të specializuara realizojnë sigurinë kriptografike.

Neni 6

Autoriteti i mbrojtjes kriptografike

Drejtoria e Shifrës, strukturë në varësi të Ministrisë së Mbrojtjes, është Autoritet Kombëtar për Sigurimin e Komunikimeve dhe Autoritet Kombëtar i Shpërndarjes.

Neni 7

Strukturat kriptografike qendrore

1. Strukturat kriptografike qendrore janë struktura bazë për mbrojtjen kriptografike të informacionit të klasifikuar “sekret shtetëror”, në çdo institucion qendror shtetëror.
2. Strukturat kriptografike qendrore ngrihen në Ministrinë e Mbrojtjes, në Ministrinë e Brendshme, në Ministrinë e Punëve të Jashtme dhe në Shërbimin Informativ të Shtetit.
3. Çdo institucion tjetër ngre strukturat e veta kriptografike për mbrojtjen e informacionit të klasifikuar “sekret shtetëror”, kur e gjykon të nevojshme.
4. Struktura kriptografike qendrore ka varësi funksionale nga titullari i institucionit.

Neni 8

Zyrat/sectorët kriptografikë

1. Zyra/sectori kriptografik përbën njësinë më të vogël kriptografike dhe kryen përpunimin kriptografik të informacionit të klasifikuar që njësia strukturore shkëmben me struktura të tjera shtetërore.
2. Zyra/sectori kriptografik i ngritur pranë njësive strukturore ka varësi administrative dhe profesionale:
 - a) Varësia administrative është nga drejtuesi i njësisë strukturore, në përbërje të të cilit vepron sectori kriptografik;
 - b) Varësia profesionale është nga titullari i strukturës qendrore kriptografike të institucionit dhe përfshin: mënyrën e kryerjes së procesit kriptografik, furnizimit me materiale kriptografike, shmangien e defekteve dhe raportimin e incidenteve, asgjësimin dhe shkatërrimin e materialit kriptografik.
3. Kur zyra/sectori kriptografik mbyllet, i gjithë dokumentacioni i krijuar gjatë dhe në funksion të aktivitetit të saj/tij asgjësohet dhe shkatërrohet sipas legjislacionit në fuqi.
4. Aktiviteti kriptografik i këtyre strukturave kriptografike qendrore, zyrave/sectorëve kriptografikë kryhet në përputhje me kërkesat e kësaj rregulloreje.

KREU III DETYRAT E STRUKTURAVE KRIPTOGRAFIKE

Neni 9

Drejtoria e Shifrës

Drejtoria e Shifrës, nëpërmjet strukturave të specializuara të saj, kryen këto detyra:

1. Prodhon, siguron dhe aplikon pajisje kriptografike, fortësia e të cilave të jetë në përputhje me nivelin e klasifikimit të informacionit.
2. Siguron që materiali çelës kriptografik të jetë në çdo kohë në kushte pune;
3. Kryen instalimin e pajisjeve kriptografike dhe kontrollon përdorimin e tyre për mbrojtjen e informacionit të klasifikuar “sekret shtetëror”, kur ky informacion transmetohet me mjete të komunikimit masiv e publik.
4. Përgatit dokumentacionin e nevojshëm për certifikimin e pajisjeve kriptografike, e paraqet atë në DSIK dhe e përditëson sa herë ka ndryshime të rëndësishme në sistemin kriptografik.
5. Koordinon dhe kontrollon aktivitetin e strukturave kriptografike në institucionet shtetërore.
6. Zbaton kushtet e sigurisë fizike për përdorimin e pajisjeve kriptografike dhe verifikon plotësimin e këtyre kushteve para instalimit të tyre.
7. Përgatit udhëzues të veçantë për përdorimin e çdo pajisjeje kriptografike dhe e vë atë në dispozicion të përdoruesve.
8. Prodhon, administron dhe shpërndan çelësat kriptografikë që përdoren për kriptimin/dekriptimin e informacionit nga strukturat kriptografike, në përputhje me kërkesat e kësaj rregulloreje.
9. Përcakton rregullat e shkatërrimit të materialit çelës kriptografik ose të pajisjeve kriptografike në zbatim të ligjit dhe akteve nënligjore në fuqi për shkatërrimin e informacionit të klasifikuar.
10. Kryen hapjen dhe mbylljen e zyrave/sectorëve kriptografikë, me kërkesë të institucionit të interesuar, në bashkëpunim me strukturën kriptografike qendrore.
11. Trajton përdoruesit e pajisjeve kriptografike, në fushën e operimit dhe të shfrytëzimit, në sistemet përkatëse, dhe veçanërisht për veprimet që cenojnë sigurinë e tyre.
12. Pajis me dëshmi aftësie personelin e strukturës kriptografike qendrore dhe të zyrave/sectorëve kriptografikë.
13. Inspekton mënyrën e përdorimit të pajisjeve kriptografike, në çdo institucion, jo më pak se një herë në vit.
14. Harton procedura që duhen ndjekur nga zyrat/sectorët kriptografikë dhe nga struktura kriptografike qendrore, për trajtimin e incidenteve dhe rastet emergjente.
15. Ngre grup pune për hetimin e shkaqeve e rrethanave në rast incidentesh kriptografike dhe merr masat përkatëse për shmangien e pasojave negative.
16. Administron pajisjet kriptografike të certifikuara më parë nga DSIK-ja.

Neni 10

Detyrat e Strukturës Kriptografike Qendrore

Struktura Kriptografike Qendrore ka këto detyra:

- I. Bashkëpunon me Drejtorinë e Shifrës dhe DSIK-në për projektimin dhe krijimin e infrastrukturës së nevojshme për ngritjen e sistemit/sistemeve kriptografike të institucionit.
2. Merr në dorëzim sistemin/sistemet kriptografik të ngritur dhe ndjek respektimin e standarteve të sigurisë gjatë përdorimit të tij.
3. Ndjek respektimin e procedurave kriptografike të informacionit të klasifikuar “sekret shtetëror” nga përdoruesit e strukturave kriptografike të institucionit.
4. Merr masa për pajisjen e përdoruesve me certifikatë sigurie të përshtatshme.
5. Merr masa për certifikimin e pajisjeve kriptografike që përdor institucioni.
6. Merr masa për respektimin e afateve të ndryshimit të çelësve kriptografikë të

përcaktuara në procedurat e operimit të sigurt.

7. Kontrollon mënyrën e marrjes, ruajtjes dhe përdorimit të çelësve kriptografikë, në strukturat kriptografike në varësi.

8. Kryen teste periodike të pajisjeve kriptografike në përdorim të institucionit ku operon.

9. Koordinon punën me Drejtorinë e Shifrës, për trajnimin e përdoruesve të sistemit/sistemeve kriptografike.

10. Ndjek detyrat në kuadrin e planit të evakuimit të informacionit të klasifikuar në rastet e gjendjes së luftës, gjendjes së jashtëzakonshme, fatkeqësive natyrore dhe emergjencave civile në lidhje me materialet kriptografike të strukturave kriptografike të institucionit.

11. Mbikëqyr punën e përdoruesve të pajisjeve kriptografike, evidenton dobësitë që shfaqen gjatë procesit kriptografik dhe rekomandon masat për korrigjimin e tyre.

12. Raporton incidentet menjëherë te titullari i institucionit, Drejtoria e Shifrës dhe DSIK-ja.

13. Mban një regjistër qendror për pajisjet kriptografike që institucioni ka në përdorim, kryen për çdo vit inventarin e tyre dhe njofton Drejtorinë e Shifrës mbi rezultatin e tij.

14. Mban aktdorëzimin e materialit kriptografik kur puna është e organizuar me turne, nga dorëzuesi te marrësi në dorëzim. Modeli i aktdorëzimit përcaktohet nga Drejtoria e Shifrës.

Neni 11

Përdoruesi i pajisjeve kriptografike

1. Përdoruesi i pajisjeve kriptografike të plotësojë këto kushte:

a) Të njohë legjislacionin në fuqi për informacionin e klasifikuar “sekret shtetëror”.

b) Të jetë pajisur me certifikatë sigurie të përshtatshme.

c) Të jetë instruktuar dhe pajisur me dëshmi aftësie të përshtatshme në fushën e kriptografisë, për njohjen e pajisjes kriptografike në përdorim.

2. Përdoruesi i pajisjeve kriptografike ka për detyrë:

a) Të përdorë pajisjet kriptografike sipas konfigurimit strukturor dhe në përputhje me nivelin e klasifikimit të informacionit.

b) Të kryejë sipas procedurave të përcaktuara, kriptimin, dekriptimin, transmetimin dhe evidentimin e informacionit të klasifikuar.

c) Të konfirmojë në çdo rast mbërritjen e informacionit të kriptuar tek i adresuari.

d) Të administrojë informacionin që kripton dhe dekripton, në përputhje me legjislacionin në fuqi.

e) Të informojë me shkrim eprorin për çdo rast komprometimi apo incidenti kriptografik.

f) Të dokumentojë kalimin e procesit kriptografik të përdoruesit pasardhës.

3. Përdoruesit të pajisjeve kriptografike i ndalohet:

a) Të ndryshojë konfigurimin e pajisjes kriptografike.

b) Të krijojë kopje të çelësve kriptografikë në përdorim.

c) Të njohë informacionin që nuk është përpunuar nga ai vetë.

d) Të japë personave të paautorizuar, të dhëna mbi procesin kriptografik dhe informacionet e klasifikuara.

e) Të zbatojë urdhra që bien në kundërshtim me këtë rregullore.

f) Të përdorë pajisje kriptografike të paakredituara më parë nga DSIK-ja.

4. Kur një përdorues i pajisjes kriptografike mungon për një periudhë kohe (leje, sëmundje), ai zëvendësohet nga një përdorues i një strukture apo sektori tjetër me

vendndodhje në të njëjtin rajon, i instruktuar dhe certifikuar përshtatshëm. Në këtë rast dorëzohen me procesverbal vetëm materialet që nevojiten për punë. Dorëzimi i këtyre materialeve bëhet në prani të eprorit të tij.

5. Kur punonjësi i strukturës kriptografike përgjegjëse transferohet, ai i dorëzon dokumentet pasardhësit.

KREU IV ADMINISTRIMI I SISTEMEVE KRIPTOGRAFIKE

Neni 12

Ngritja e sistemit kriptografik

1. Ngritja e sistemit kriptografik nis me kërkesën me shkrim të institucionit të interesuar në Drejtorinë e Shifrës.

2. Drejtoria e Shifrës, në bazë të kërkesës së bërë, vlerëson plotësimin e kushteve të nevojshme dhe kryen instalimin e sistemit kriptografik.

3. Pas instalimit të sistemit kriptografik, Drejtoria e Shifrës kryen testimin e tij.

4. Instalimi i pajisjes kriptografike shoqërohet me aktin e instalimit, i cili mbahet në dy kopje, një për strukturën qendrore dhe një për Drejtorinë e Shifrës. Në aktin e instalimit evidentohen:

a) sistemi i instaluar, vendi dhe koha e instalimit;

b) niveli i klasifikimit të informacionit që sistemi mbron;

c) përdoruesi i sistemit kriptografik dhe instruktimi i tij; ç) çelësat kriptografikë të instaluar.

5. Administrimi i sistemit kriptografik kryhet nga struktura kriptografike qendrore e institucionit.

6. Drejtuesi i strukturës kriptografike qendrore, sektorit/zyrës kriptografike është përgjegjës për sigurinë e sistemit kriptografik të institucionit dhe administrimin e dokumentacionit në përdorim.

Neni 13

Pajisjet kriptografike

1. Drejtoria e Shifrës vendos në përdorim pajisjet kriptografike, pasi të jenë certifikuar nga DSIK-ja.

2. Pajisjet kriptografike përdoren deri në nivelin e klasifikimit të informacionit, për të cilin janë certifikuar dhe sipas instruksioneve të përdorimit të tyre.

3. Pajisjet kriptografike ruhen, në mënyrë të tillë që të ndalohej aksesimi i paautorizuar në këto pajisje.

4. Pajisjet kriptografike transportohen të ndara nga çelësat kriptografikë.

5. Çelësat kriptografikë futen në përdorim vetëm pasi verifikohet paprekshmëria e tyre.

6. Në rast se dyshohet për komprometimin e çelësave, ata nuk futen në përdorim dhe për këtë njoftohet Drejtoria e Shifrës.

7. Drejtoria e Shifrës në rast defekti, merr masa për riparimin e pajisjes kriptografike.

8. Kur kryhet riparimi i pajisjes kriptografike, drejtuesi i strukturës kriptografike qendrore merr masa për mosekspozimin e përmbajtjes së informacionit të klasifikuar.

9. Instalimi apo heqja nga përdorimi i pajisjeve kriptografike kryhet në çdo rast nga persona të instruktuar dhe të autorizuar posaçërisht.

10. Drejtoria e Shifrës, sipas një plani të hartuar më parë, kryen teste periodike të sistemeve kriptografike në përdorim për funksionimin e tyre.

Neni 14

Nxjerrja nga përdorimi të pajisjes kriptografike

Pajisjet kriptografike nxirren jashtë përdorimit kur:

1. nuk janë në gjendje të sigurojnë mbrojtjen e informacionit të klasifikuar në nivelin e kërkuar ose kur konstatohet komprometimi i tyre;
2. përdorimi i tyre nuk është më i domosdoshëm.

Nxjerrja nga përdorimi i pajisjeve kriptografike shoqërohet gjithmonë me procesverbal.

Neni 15

Prodhimi, ruajtja dhe shkatërrimi i çelësve kriptografikë

1. Çelësat kriptografikë të prodhuar kanë elementet e identifikimit të tyre dhe nivelin e sigurisë së informacionit që mbrojnë.

2. Çelësat kriptografikë shpërndahen në mënyrë të sigurt. Gjatë transportit ruhet paprekshmëria e çelësve kriptografikë e konfirmuar me procesverbal nga marrësi/përdoruesi i tyre.

3. Marrësi në dorëzim i çelësve kriptografikë mban procesverbalin përkatës në rast se konstaton parregullsi.

4. Ndryshimi i çelësve kriptografikë bëhet sipas afateve të përdorimit të tyre, të përcaktuara në procedurat e operimit të sigurt.

5. Ndalohet krijimi i kopjeve të paautorizuara dhe të padokumentuara, të çelësve kriptografikë.

6. Shkatërrimi i çelësve kriptografikë kryhet në përputhje me legjislacionin në fuqi dhe udhëzimet e Drejtorisë së Shifrës.

7. Për shkatërrimin e çelësve kriptografikë mbahet një procesverbal në dy kopje, një për sektorin që kryen shkatërrimin dhe një kopje për strukturën kriptografike qendrore. Kur shkatërrimi i çelësve kriptografikë bëhet nga struktura kriptografike qendrore, ky procesverbal bëhet në një kopje.

8. Drejtoria e Shifrës inspekton jo më pak se një herë në vit strukturat kriptografike qendrore dhe sektorët kriptografikë, për përdorimin, ruajtjen dhe shkatërrimin e çelësve kriptografikë.

Neni 16

Procedurat e shpërndarjes së materialit kriptografik

1. Shpërndarja e materialit kriptografik kryhet në ministri dhe institucione shtetërore të interesuara brenda territorit të Republikës së Shqipërisë dhe në përfaqësitë diplomatike dhe konsullore jashtë vendit.

2. Përgatitja e pakove me material kriptografik

a) Materiali çelës kriptografik paketohet i ndarë nga pajisja shoqëruese kriptografike dhe transportohet si pjesë e të njëjtës ngarkesë.

b) Pajisja kriptografike të jetë në gjendjen fillestare para transportimit, përjashtuar rastet kur konfigurimi fizik i tyre e bën të pamundur fshirjen.

c) Pajisja kriptografike klasifikohet në nivelin e çelësit kriptografik dhe mbështjellja e brendshme duhet të identifikojë përmbajtjen si “kriptografike”.

d) Korrieri plotëson raportin e transportimit të materialit kriptografik për çdo ngarkesë në dy kopje. Një kopje e këtij raporti vendoset brenda kutisë së çdo ngarkese dhe një kopje mbahet nga institucioni dërgues.

e) Materiali kriptografik mbyllet me dy mbështjellëse të zeza dhe jotransparente, të vulosura. Materiali kriptografik i mbështjellë vendoset brenda një çante të posaçme ose kutie të kyçur dhe të vulosur që eliminon ekspozimin e përmbajtjes.

f) Materiali kriptografik do të ketë dy mbështjellëse me cilësitë e mëposhtme:

i) Mbështjellësja e brendshme me ngjyrë të zeze. Në të shënohet adresa e dërguesit, adresa e marrësit, niveli i klasifikimit, i shoqëruar me shenjëzimin “Kriptografik” dhe instruksionin “të hapet vetëm nga ...(emri dhe mbiemri i marrësit)”.

ii) Mbështjellësja e jashtme, me ngjyrë të zeze. Në të shënohet adresa e dërguesit, adresa e marrësit dhe numri i regjistrimit. Ndalohet vendosja e shenjëzimeve të tjera mbi këtë mbështjellëse.

g) Përpara marrjes në dorëzim të pakos verifikohet rregullsia e shenjëzimeve të përcaktuara me sipër. Kur konstatohen parregullsi rasti konsiderohet incident dhe do të trajtohet sipas nenit 20 të kësaj rregulloreje.

3. Transportimi i materialit kriptografik

a) Korrierët e Drejtorisë së Shifrës kryejnë transportimin e sigurt të materialit kriptografik në përputhje me nivelin e klasifikimit të këtij materiali.

b) Materialet kriptografike sigurohen në të gjitha fazat e transportimit të tij, përgjatë itinerarit të përcaktuar nga Drejtoria e Shifrës.

c) Dërguesi i materialit kriptografik merr nga marrësi një raport të firmosur ose mesazh elektronik për çdo ngarkesë të dërguar. Nëse nuk merret kopje e nënshkruar brenda 10 ditësh, dërguesi e ndjek çështjen e pakos së dërguar derisa të konfirmohet marrja.

4. Instruksione për korrierët

a) Autoritetet doganore dhe të sigurisë ekzaminonjë pakot me material kriptografik pa i hapur ato.

b) Për transportimin e pakove me material kriptografik që nuk mbahen me vete, korrierët marrin masa që të shohin ngarkimin dhe shkarkimin e sigurt të tyre sipas parimit “i fundit në hyrje - i pari në dalje”.

c) Korrierët duhet të sigurohen që materiali ka mbrojtjen maksimale gjatë të gjitha fazave të transportit të tij.

d) Korrierët nuk ngarkohen me detyra të tjera gjatë udhëtimit për transportimin e materialit kriptografik. Nëse i caktohen detyra të tjera, ato duhet të jenë dytësore dhe të mos cenonjë në asnjë mënyrë detyrat dhe përgjegjësitë e korrierit.

e) Korrierët duhet të jenë të instruktuar për mënyrat e mbrojtjes së vazhdueshme të materialit kriptografik që u besohet.

KREU V

AMBIENTET DHE MJEDISËT KRIPTOGRAFIKE

Neni 17

Kërkesa për sigurimin fizik të ambienteve dhe mjediseve kriptografike

1. Ambientet dhe mjediset kriptografike duhet të plotësojnë kërkesat e legjislacionit, për sigurimin fizik të informacionit të klasifikuar “sekret shtetëror”.

2. Ambientet dhe mjediset kriptografike vendosen në zona sigurie të klasit të dytë.

3. Ambientet dhe mjediset e kriptografike pajisen me kasaforta të nivelit “tepër sekret”, për ruajtjen e informacionit të klasifikuar, çelësave kriptografikë ose pajisjeve kriptografike.

4. Procesi kriptografik kryhet vetëm në sisteme të certifikuara. Ndalohet lidhja e pajisjeve kriptografike në internet, në rrjete të pacertifikuara apo rrjete me nivel certifikimi më të ulët se niveli i certifikimit të pajisjes kriptografike. Për përdorimin e tyre përgatiten

udhëzues të veçantë nga Drejtoria e Shifrës.

5. Ambientet dhe mjediset kriptografike u nënshtrohen jo më pak se një herë në vit inspektimeve dhe kontrolleve për respektimin e kërkesave të sigurisë.

Neni 18

Kërkesat për evakuim

1. Titullarët e institucioneve, që administrojnë informacion të klasifikuar, përcaktojnë dhe marrin masa për rregullat dhe procedurat e evakuimit të pajisjeve kriptografike dhe të informacionit të klasifikuar, në rastet e gjendjes së luftës, të gjendjes së jashtëzakonshme, gjendjes së fatkeqësive natyrore dhe emergjencave të tjera civile, gjatë të cilave ky informacion mund të përvetësohet, dëmtohet, shkatërrohet apo asgjësohet.

2. Përdorimi i pajisjeve kriptografike në kushte e emergjencave, bëhet me urdhër të drejtuesit të njësisë strukturore ku përdoruesi bën pjesë. Në këto raste përdoruesit i sigurohet minimumi i kushteve të sigurisë, në përputhje me nivelin e klasifikimit të pajisjes kriptografike.

KREU VI

INCIDENTET DHE MASAT PËRKATËSE

Neni 19

Incident kriptografik

Incidente kriptografike konsiderohen:

1. Humbja e materialit kriptografik;
2. Komprometimi, humbja apo kopjimi nga persona të paautorizuar i çelësve kriptografikë;
3. Përdorimi i pajisjes kriptografike pa u certifikuar me parë nga DSIK-ja;
4. Përdorimi i pajisjes kriptografike nga persona të paautorizuar;
5. Ruajtja ose përdorimi i pajisjes kriptografike jashtë kërkesave të sigurisë fizike;
6. Transmetimi i informacionit të klasifikuar me pajisje kriptografike me nivel klasifikimi më të ulët se niveli i klasifikimit të sistemit/pajisjes kriptografike;
7. Transmetimi i informacionit të klasifikuar me pajisje kriptografike të dëmtuara;
8. Administrimi në kundërshtim me rregullat e përcaktuara i materialeve kriptografike;
9. Keqfunksionimi i pajisjes kriptografike;
10. Modifikim i paautorizuar i materialit kriptografik;
11. Mospërdorimi i materialeve kriptografike.

Neni 20

Masat për incidentet kriptografike

1. Në rast incidenti kriptografik, menjëherë pas konstatimit, ndërpritet procesi i kriptim-dekriptimit me çelësat kriptografikë në përdorim dhe vihet në dijeni me shkrim struktura kriptografike qendrore.

2. Struktura kriptografike qendrore merr masa për shmangien ose kufizimin e pasojave negative dhe informon brenda 24 orëve Drejtorinë e Shifrës.

3. Për sqarimin e rrethanave të incidentit ngrihet një komision, me urdhër të përbashkët të dy institucioneve, në përbërje të të cilit bëjnë pjesë specialistë nga Drejtoria e Shifrës, nga struktura kriptografike qendrore dhe sektori kriptografik ku ka ndodhur incidenti.

4. Konkluzionet e komisionit hartohen në tri kopje, një për sektorin kriptografik ku ka ndodhur incidenti, një për strukturën kriptografike qendrore dhe një për Drejtorinë e Shifrës.

5. Për konkluzionet e nxjerra nga komisioni për incidentin e ndodhur, Drejtoria e Shifrës njofton DSIK-në.

6. Përfundimet që dalin nga analiza e incidentit trajtohen gjatë procesit të trajnimit dhe edukimit të përdoruesve.

KREU VII PËRGATITJA DHE INSPEKTIMET

Neni 21 **Përgatitja**

1. Përgatitja kriptografike kryhet sipas një plani të veçantë të hartuar nga Drejtoria e Shifrës dhe të miratuar nga titullari institucionit.

2. Përgatitja mbi përdorimin e pajisjeve kriptografike kryhet sa herë futen në përdorim pajisje të reja me qëllim përdorimin korrekt të tyre.

3. Drejtoria e Shifrës miraton programet dhe temat e trajnimit.

4. Përgatitja kryhet nga Drejtoria e Shifrës.

5. Përgatitja kriptografike shoqërohet me dhënie të dëshmisë së aftësisë, me afat vlefshmërie deri në 5 vjet.

Neni 22 **Inspektimet**

1. Inspektimet bëhen në funksion të zbatimit të legjislacionit në fuqi dhe kriterëve të përcaktuara në këtë rregullore.

2. Inspektimet për çdo institucion kryhen nga Drejtoria e Shifrës, jo më pak se një herë në vit me autorizim të titullarit të institucionit. Inspektime bën edhe drejtuesi i strukturës kriptografike qendrore, në sektorët kriptografikë vartës.

3. Pas çdo inspektimi, përpilohet raporti i inspektimit në tri kopje, një për drejtuesin e institucionit, një për strukturën kriptografike qendrore të inspektuar dhe një për Drejtorinë e Shifrës.

4. Drejtoria e Shifrës raporton periodikisht, por jo më pak se një herë në gjashtë muaj, në DSIK për inspektimet e kryera.

KREU VIII DOKUMENTACIONI

Neni 23 **Regjistrat**

1. Strukturat kriptografike pajisen me regjistra ku evidentohet procesi kriptografik që kryhet.

2. Regjistrat për evidentimin e procesit kriptografik hartohen nga Drejtoria e Shifrës dhe miratohen nga DSIK-ja.

3. Për nevoja pune strukturat kriptografike përdorin këto regjistra të klasifikuar:

a) Regjistri bazë (model 1), ku regjistrohen të gjitha regjistrat e strukturës.

b) Regjistri ku regjistrohen të gjitha pajisjet kriptografike dhe dokumentacioni përkatës (model 2).

c) Regjistri i mesazheve të hyra (model 3).

d) Regjistri i mesazheve të dala (model 4).

e) Regjistri i korrespondencës (model 5).

Neni 24

Administrimi i dokumentacionit dhe i materialit kriptografik

Dokumentacioni dhe materialet kriptografike të përdorura me qëllim zbatimin e kësaj rregulloreje, administrohen sipas legjislacionit në fuqi për informacionin e klasifikuar.

KREU IX

BUXHETI I AUTORITETIT TË MBROJTJES KRIPTOGRAFIKE

Neni 25

1. Drejtorisë së Shifrës i akordohen fonde buxhetore brenda buxhetit të miratuar për Ministrinë e Mbrojtjes.
2. Ky buxhet përdoret për:
 - a) prodhimin dhe blerjen e pajisjeve kriptografike;
 - b) instalimin e pajisjeve kriptografike;
 - c) shpërndarjen e çelësave;
 - d) trajnimin/përgatitjen e përdoruesve;
 - e) kontrollin e procesit kriptografik;
 - f) inspektimet.

KREU X

DISPOZITA TË FUNDIT

Neni 26

1. Moszbatimi i kërkesave të kësaj rregulloreje përbën shkelje të rregullave të sigurisë së informacionit të klasifikuar dhe sjell sipas rastit, përgjegjësi disiplinore, administrative ose penale.
2. Ngarkohen institucionet shtetërore që kanë të ngritura struktura kriptografike për zbatimin e kësaj rregulloreje.
3. Ngarkohet Drejtoria e Sigurimit të Informacionit të Klasifikuar (DSIK) dhe Drejtoria e Shifrës për ndjekjen e zbatimit të kësaj rregulloreje.
4. Rregullorja e miratuar me vendimin e Këshillit të Ministrave nr.14, datë 28.1.2002, për "Miratimin e rregullores për shërbimin shifrar të Republikës së Shqipërisë" shfuqizohet.