

V E N D I M
Nr. 478, datë 19.7.2001

**PËR SIGURIMIN E INFORMACIONIT TË KLASIFIKUAR “SEKRET SHTETËROR” NË
RRJETET INFORMATIKE, MJETET DHE PAJISJET E TRANSMETIMIT**

Në mbështetje të nenit 100 të Kushtetutës dhe neneve 23 e 31 të ligjit nr.8457, datë 11.2.1999 “Për informacionin e klasifikuar “sekret shtetëror”, me propozimin e Kryeministrit, Këshilli i Ministrave

V E N D O S I:

I.KËRKESAT PËR RRJETET INFORMATIKE, MJETET DHE PAJISJET E TRANSMETIMIT

1. Institucionet shtetërore, të cilat për nevoja të punës duhet të prodhojnë, ruajnë, përpunojnë, shpërndajnë ose transmetojnë informacion të klasifikuar “sekret shtetëror”, nëpërmjet rrjeteve informatike, mjeteve dhe pajisjeve të transmetimit, duhet t’u përmbahen rregullave të përcaktuara në këtë vendim.

2. Rrjetet informatike, mjetet dhe pajisjet e transmetimit të informacionit të klasifikuar “sekret shtetëror”, duhet të sigurojnë:

mbrojtjen nga ndërhyrjet e paautorizuara;

mosndryshimin e paautorizuar;

mosasgjesimin apo shkatërrimin, në mënyrë të kundërligjshme.

3. Ministria apo institucioni shtetëror, para përdorimit të rrjetit informatik, mjeteve pajisjeve të transmetimit, i kërkon DSIK-së lëshimin e “Certifikatës së sigurisë së rrjetit” apo “Certifikatës së sigurisë së mjetit”.

Kërkesa shoqërore me “deklaratën e sigurisë” dhe me dokumente të tjera, që vërtetojnë dhe mbështesin sigurinë e rrjetit, të mjeteve e pajisjeve të transmetimit.

Forma dhe përmbajtja e certifikatës dhe deklaratës së sigurisë përcaktohen nga DSIK-ja.

4. “Certifikata e sigurisë së rrjetit” është dokumenti që vërteton se tërësia e mjeteve dhe pajisjeve, që përbëjnë rrjetin ku ruhet, përpunohet, administrohet, transmetohet informacioni i klasifikuar “sekret shtetëror”, plotësojnë kërkesat e sigurisë.

5. “Certifikata e sigurisë së mjetit” është dokumenti që vërteton se mjetet apo pajisjet e transmetimit plotësojnë kërkesat e sigurisë së informacionit të klasifikuar “sekret shtetëror”.

6. “Deklarata e sigurisë”, përmban përshkrimin e plotë dhe të hollësishëm të sigurisë së rrjetit informatik, mjeteve apo pajisjeve të transmetimit, gjatë instalimit dhe shfrytëzimit. Ajo i lëshohet ministrisë apo institucionit shtetëror dhe nënshkruhet nga personi fizik apo juridik, vendas apo i huaj, i cili ka prodhuar, tregtuar, dhuruar apo siguruar ato në një mënyrë tjetër.

7. DSIK-ja brenda afatit njëmuajor shqyrton kërkesën e paraqitur. Kur rrjeti informatik, mjetet apo pajisjet e transmetimit përmbushin kërkesat e sigurisë së informacionit të klasifikuar, DSIK-ja lëshon “Certifikatën e sigurisë”.

Në rast mosmiratimi të kërkesës, subjekti kërkues brenda 10 ditëve ka të drejtë të ankohet te Kryeministri, vendimi i të cilit është përfundimtar.

8. Personi apo personat që instalojnë, mirëmbajnë ose ndreqin rrjetin informatik, mjetet apo pajisjet e transmetimit, punonjës apo jo të institucionit, duhet të pajisen me “certifikatë sigurie”.

Kur nuk janë punonjës të ministrisë apo institucionit, ata janë nën mbikqyrjen e vazhdueshme të personelit të kualifikuar teknikisht dhe të certifikuar, të ministrisë apo institucionit.

9. Kur shkëmbehet informacion i klasifikuar me shtete të tjera apo organizata ndërkombëtare, në marrëveshje mund të përcaktohen edhe standarte apo kërkesa të tjera për sigurinë e rrjeteve informatike, të mjeteve e pajisjeve të transmetimit të informacionit të klasifikuar.

II. Masat e sigurimit të rrjeteve informatike, mjeteve dhe pajisjeve të transmetimit

Sigurimi fizik i rrjeteve informatike

1. Rrjetet informatike u nënshtrohen rregullave për sigurimin fizik të informacionit të klasifikuar “sekret shtetëror”, të përcaktuara me akte të tjera normative.

2. Rrjetet informatike ndërtohen në përputhje me strukturën organizative të institucionit ku

instalohen dhe me nivelin e klasifikimit të informacionit të klasifikuar “sekret shtetëror”, që përpunohet.

3. Lidhja fizike me rrjetet lokale informatike të bëhet vetëm me media të sigurtë (fibra optike) ose me pajisje të kontrolluara, duke përdorur me shumë se një tip barriere, të cilat mbështesin njëra-tjetrën.

4. Ndalohet përdorimi i modemave të ndryshme të cilat krijojnë lidhje të pakontrolluara me rrjetin informatik.

5. Sigurimi fizik i serverit të rrjetit lokal informatik të përputhet me nivelin e masave të sigurisë së informacionit të klasifikuar të nivelit më të lartë që ai ruan.

B. Aftësitë e sigurisë së personelit që punon me rrjetet informatike

1. Personeli që punon në rrjetet informatike, të jetë i certifikuar sipas akteve nënligjore në fuqi. Niveli i “certifikatës së sigurisë” të jetë në përputhje me nivelin e informacionit të klasifikuar “sekret shtetëror”, që njeh dhe administron ky personel.

2. Personeli që punon në rrjetet informatike, të jetë i trajnuar në fushën e operimit dhe shfrytëzimit të rrjetit dhe veçanërisht në veprimet që cenojnë sigurinë e rrjetit.

3. Administratorët e rrjetit janë përgjegjës për zbatimin e masave të sigurisë së tij. Ata pajisen me “certifikatë sigurie” të nivelit më të lartë të klasifikimit të informacionit që administrojnë dhe përzgjidhen ndër specialistët më të mirë të sistemeve të operimit e shfrytëzimit të rrjetit.

4. Personat, të cilët për nevoja pune hyjnë në mjediset me rrjete informatike, u nënshtrohen rregullave për ruajtjen e informacionit të klasifikuar “sekret shtetëror”, të përcaktuara nga titullari i ministrisë apo institucionit.

C. Sigurimi i informacionit të klasifikuar “sekret shtetëror”, në rrjetet informatike

1. Sigurimi i informacionit të klasifikuar “sekret shtetëror”, në rrjetet informatike, të bëhet në të gjitha fazat e ciklit të plotë të tij.

Sistemet e transmetimit të informacionit të klasifikuar “sekret shtetëror” të kenë kapacitetin dhe aftësinë që, nëpërmjet moskontakteve fizike apo elementëve speciale të software-it, të pengojnë aksesin në stacionet fundore.

2. Ndalohet ruajtja e informacionit të klasifikuar “sekret shtetëror” në kompjuter, kur ai është i lidhur në rrjet informatik. Në këtë rast ruajtja bëhet vetëm në server.

Kompjuterat me hard disk të fiksuar, kur punojnë jashtë rrjetit dhe trajtojnë informacion të klasifikuar “sekret shtetëror”, të sigurojnë nivelin maksimal të mbrojtjes, sipas klasifikimit të informacionit.

3. Masat e sigurisë dhe e drejta për t’u njohur me informacionin e klasifikuar përcaktohen sipas nivelit të klasifikimit të tij. Masat e sigurisë të parashikojnë mbrojtjen nga dëmtimet që shkaktojnë viruset e ndryshme, disiplinimin dhe kontrollin e hyrjes në rrjet dhe parandalimin e ndërhyrjeve me synime keqdashëse.

4. Përdoruesit organizohen në grupe, në përputhje me strukturën organizative dhe hierarkinë. Atyre u vihen në dispozicion llogaritë përkatëse, të cilat hapen vetëm pas përdorimit të fjalëkalimeve, të cilat ndërtohen mbi bazën e procedurave profesionale dhe ndërrohen periodikisht.

5. Përdoruesit të rrjetit informatik i ndalohet:

a) të orvatet të futet në një rrjet nën një identitet tjetër;

b) të orvatet të njohë dhe administrojë informacion të klasifikuar “sekret shtetëror” jashtë të drejtave që ai ka;

c) të importojë apo eksportojë informacion të klasifikuar “sekret shtetëror”, aplikime, lojëra me disketa etj.;

ç) të instalojë apo të ndryshojë në ndonjë mënyrë hardware-in, software-in, ose aplikime;

d. të dërgojë apo heqë informacione të klasifikuara “sekret shtetëror” ose disketa, pa autorizimin e titullarit të institucionit.

6. Rrjeti informatik i nënshtrohet kontrollit periodik, për të parë ndryshimet në rrjet, masat e sigurisë së informacionit të klasifikuar “sekret shtetëror” dhe përshtatjen e tyre me arritjet e kohës, nga personat përgjegjës, të caktuar nga titullari i ministrisë apo institucionit.

7. Veprimtaria e përdoruesve dhe administratorëve të rrjetit duhet të auditohet (monitorohet), për të zbuluar dhe parandaluar ngjarjet që mund të cenojnë sigurinë e informacionit të klasifikuar “sekret shtetëror”.

8. Për të ruajtur informacionin e klasifikuar “sekret shtetëror” dhe konfigurimin e rrjeteve që e

përpunojnë atë, bëhet rezervimi i tyre në media të ndryshme, si shirit manjetik, CD dhe server rezerve (Backup server). Për ruajtjen e këtyre pajisjeve të krijohen kushte të veçanta.

9. Prishja e autorizuar e informacionit të klasifikuar “sekret shtetëror” të magazinuar në media të ndryshme bëhet me metoda profesionale ose me shkatërrimin fizik të tyre. Prishja të bëhet vetëm kur është e domosdoshme dhe pasi informacioni i klasifikuar “sekret shtetëror” të jetë i printuar dhe regjistruar.

Printimi dhe administrimi i dokumenteve të klasifikuara të bëhet sipas rregullave përkatëse.

10. Ndalohet trajtimi i informacionit të klasifikuar “sekret shtetëror”, në kompjuterat private dhe futja e këtyre kompjuterave në mjediset ku ruhet, përpunohet dhe transmetohet informacion i klasifikuar.

D.Sigurimi i komunikimeve

1. Për transmetimin e informacionit të klasifikuar “sekret shtetëror” të përdoren mjete, pajisje e sisteme kriptografike të specializuara, fortësia e të cilave të jetë në përputhje me nivelin e klasifikimit të informacionit.

2. Drejtoria e Shifrimit dhe Transmetimit të Informacionit, e cila sot është në varësi të Shërbimit Informativ Shtetëror, është strukturë e specializuar, e cila përgjigjet për mbrojtjen e informacionit të klasifikuar “sekret shtetëror” në të gjitha strukturat shtetërore, kur ky informacion transmetohet me mjete të komunikimit, masiv e publik. Ajo përgjigjet për hartimin, prodhimin dhe përdorimin e shifrës, për të gjitha ministritë e institucionet shtetërore.

3. Përdorimi i sistemeve të shifrimit, mjeteve e pajisjeve të komunikimit të informacionit të klasifikuar “sekret shtetëror”, të bëhet pas miratimit e certifikimit nga DSIK-ja.

III.Rregulla të veçanta

1. Ministritë dhe institucionet shtetërore janë përgjegjëse për mbrojtjen dhe sigurimin e informacionit të klasifikuar “sekret shtetëror” në rrjetet informatike, mjetet dhe pajisjet e transmetimit.

2. Ngarkohen ministritë dhe institucionet e tjera shtetërore për zbatimin e këtij vendimi.

Drejtuesit e këtyre institucioneve, brenda 30 ditëve nga hyrja në fuqi e këtij vendimi, detyrohen të nxjerrin udhëzim për zbatimin e këtij vendimi.

3. Ngarkohet Drejtoria e Sigurimit të Informacionit të Klasifikuar për ndjekjen e zbatimit të këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTRI

Ilir Meta