VENDIM
Nr.922, datë 19.12.2007

PËR SIGURIMIN E INFORMACIONIT TË KLASIFIKUAR "SEKRET SHTETËROR", QË PRODHOHET, RUHET, PËRPUNOHET APO TRANSMETOHET NË SISTEMET E KOMUNIKIMIT (INFOSEC)

Në mbështetje të nenit 100 të Kushtetutës dhe të neneve 23 e 31 të ligjit nr.8457, datë 11.2.1999 "Për informacionin e klasifikuar "Sekret shtetëror"", të ndryshuar me propozimin e Zëvendëskryeministrit, Këshilli i Ministrave

VENDOSI:

I. KËRKESAT PËR SISTEMET E KOMUNIKIMIT (INFOSEC)

1. Institucionet shtetërore, që, për nevoja pune, prodhojnë, ruajnë, përpunojnë, shpërndajnë ose transmetojnë, mbrojnë informacion të klasifikuar "Sekret shtetëror", nëpërmjet sistemeve, rrjeteve informatike, mjeteve e pajisjeve të transmetimit, ndërlidhjes së sistemeve dhe mbrojtjes kriptografike, duhet të veprojnë në përputhje me kërkesat e përcaktuara në këtë vendim.

2. Sistemet, rrjetet informatike, mjetet e pajisjet e transmetimit, ndërlidhja e sistemeve dhe mbrojtja kriptografike, ku prodhohet, ruhet, përpunohet, shpërndahet ose transmetohet e mbrohet informacion i klasifikuar "Sekret shtetëror", duhet të sigurojnë konfidencialitetin, integritetin dhe disponibilitetin e informacionit të klasifikuar.

3. Pajisjet *hardware* dhe *soft-et* e ndryshme të rrjetit informatik të klasifikuar, mjetet dhe pajisjet e transmetimit, pajisjet e ndryshme të mbrojtjes kriptografike duhet të sigurohen nga shoqëri, prodhuese ose tregtare, të specializuara dhe të mirënjohura në tregun ndërkombëtar, sipas kërkesave të legjislacionit për prokurimin publik.

4. Institucioni shtetëror, para përdorimit të sistemeve të rrjetit informatik, mjeteve e pajisjeve të transmetimit, ndërlidhjes së sistemeve, mbrojtjes kriptografike i dërgon DSIK-së, si autoriteti kombëtar i akreditimit të sigurisë, një kërkesë me shkrim për lëshimin e "Certifikatës së sigurisë së sistemit".

Kjo kërkesë shoqërohet me dokumentacionin e mëposhtëm:

a) Deklaratën e sigurisë së sistemit.

b) Rregulloren e institucionit për sigurinë, ku jepen mënyra e zbatimit të deklaratës së sigurisë së sistemit e procedurat operacionale, që duhen ndjekur dhe përcaktohen përgjegjësitë e personelit.

c) Raportin e analizës së vlerësimit të riskut për sigurinë e sistemit.

ç) Dokumente të tjera, që vërtetojnë dhe mbështesin sigurinë e sistemeve, rrjetit informatik, mjeteve e pajisjeve të transmetimit, ndërlidhjes së sistemeve, mbrojtjes kriptografike.

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

5. Deklarata e sigurisë përmban përshkrimin, e plotë dhe të hollësishëm, të sigurisë së sistemit, të rrjetit informatik, mjeteve e pajisjeve të transmetimit, ndërlidhjes së sistemeve dhe të mbrojtjes kriptografike, gjatë instalimit dhe shfrytëzimit.

Deklarata e sigurisë plotësohet nga institucioni shtetëror, që paraqet në DSIK kërkesën për akreditim.

Deklaratat e sigurisë janë:

- Deklarata e sigurisë së rrjetit;
- Deklarata e sigurisë së mjeteve dhe pajisjeve të transmetimit;
- Deklarata e sigurisë së ndërlidhjes së sistemeve;
- Deklarata e sigurisë së shifrës.

Institucioni shtetëror, para se të instalojë dhe shfrytëzojë sisteme, rrjete informatike, mjete apo pajisje të transmetimit, ndërlidhje të sistemeve dhe mbrojtje kriptografike, i kërkon subjektit, shtetëror apo privat, dokumente, që vërtetojnë plotësimin e kërkesave dhe të standardeve të sigurisë, të shpallura, si certifikata, akte dhurimi, manuale etj., nënshkruar nga personi, fizik apo juridik, vendas a i huaj, i cili i ka prodhuar, tregtuar, dhuruar apo siguruar ato në një mënyrë tjetër.

6. DSIK-ja shqyrton kërkesën e përmendur në pikën 4, të këtij kreu, brenda afateve të mëposhtme:

- 3 muaj, për certifikimin e rrjeteve informatike;
- 2 muaj, për certifikimin e mjeteve dhe të pajisjeve të transmetimit;
- 3 muaj, për certifikimin e ndërlidhjes së sistemeve;
- 4 muaj, për certifikimin e shifrave kombëtare.

7. Pas shqyrtimit të të gjithë dokumentacionit të paraqitur, si dhe verifikimit të zbatimit të masave të sigurisë, siç janë deklaruar në deklaratën e sigurisë, DSIK-ja harton një akt vlerësimi për zbatimin e masave të sigurisë.

Në qoftë se sistemet, rrjetet informatike, mjetet dhe pajisjet e transmetimit, ndërlidhja e sistemeve dhe mbrojtja kriptografike përmbushin kërkesat dhe standardet e sigurisë së informacionit të klasifikuar "Sekret shtetëror", të përcaktuara në këtë vendim, DSIK-ja lëshon "Certifikatën e sigurisë" të sistemit, niveli i së cilës është në përputhje me nivelin më të lartë të informacionit të klasifikuar, që prodhohet, ruhet, përpunohet, shpërndahet, transmetohet a mbrohet në këtë sistem.

8. Certifikatat e sigurisë janë:

a) "Certifikata e sigurisë së rrjetit", dokumenti, që vërteton se tërësia e mjeteve dhe e pajisjeve, që përbëjnë rrjetin informatik, ku prodhohet, ruhet, përpunohet, shpërndahet a transmetohet dhe mbrohet informacioni i klasifikuar "Sekret shtetëror", plotësojnë standardet e sigurisë.

b) "Certifikata e sigurisë së mjetit", dokumenti, që vërteton se mjeti apo pajisja e transmetimit plotëson standardet e sigurisë së informacionit të klasifikuar "Sekret shtetëror".

c) "Certifikata e sigurisë së ndërlidhjes së sistemeve/rrjeteve", dokumenti, që vërteton se tërësia e mjeteve dhe e pajisjeve, që përbëjnë lidhjen e dy ose më shumë sistemeve/rrjeteve, ku transmetohet informacioni i klasifikuar "Sekret shtetëror", plotësojnë standardet e sigurisë.

ç) "Certifikata e sigurisë së shifrës", dokumenti, që vërteton se mbrojtja kriptografike me këtë shifër plotëson standardet e sigurisë së informacionit të klasifikuar "Sekret shtetëror".

9. Subjekti kërkues, në rast mosmiratimi të kërkesës për certifikim, brenda 10 ditëve, ka të drejtë të ankohet te Kryeministri, vendimi i të cilit është përfundimtar.

10. Pas certifikimit të sistemit, institucioni, të cilit i është lëshuar "Certifikata e sigurisë", harton dhe zbaton procedura dhe rregulla për administrimin e ndryshimeve në sistem dhe është i detyruar të raportojë, menjëherë, në DSIK për:

- çdo ndryshim, që cenon sigurinë në konfigurimin e hardit ose të softit të sistemit, shoqëruar me kërkesën për riakreditim për pjesën, që ndryshon, në kushtet e certifikimit të mëparshëm.
- çdo incident, që cenon sigurinë e sistemit.

11. Personi apo personat, punonjës të institucionit, që instalojnë, mirëmbajnë ose riparojnë rrjetin informatik, mjetet apo pajisjet e transmetimit, sistemet e ndërlidhjes duhet të jenë të pajisur më parë me "Certifikatë sigurie" të përshtatshme.

Në qoftë se nuk janë punonjës të institucionit, ata duhet të jenë nën mbikëqyrjen e vazhdueshme të personelit, të kualifikuar teknikisht dhe të certifikuar, të institucionit.

Kur punimet kryhen nga subjekte shtetërore, private, vendase apo të huaja, do të zbatohen kërkesat për sigurimin e informacionit të klasifikuar "Sekret shtetëror", në fushën industriale.

12. Në qoftë se shkëmbehet informacion i klasifikuar me shtete të tjera apo me organizata ndërkombëtare, në marrëveshje apo protokolle mund të përcaktohen edhe standarde a kërkesa të tjera, për sigurinë e rrjeteve informatike, të mjeteve e të pajisjeve të transmetimit, ndërlidhjen e sistemeve dhe mbrojtjen kriptografike të informacionit të klasifikuar.

II. MASAT E SIGURISË SË RRJETEVE INFORMATIKE, TË MJETEVE E PAJISJEVE TË TRANSMETIMIT DHE TË NDËRLIDHJES SË SISTEMEVE

A. Sigurimi fizik i rrjeteve informatike, mjeteve dhe i pajisjeve të transmetimit dhe i ndërlidhjes së sistemeve

1. Rrjetet informatike, mjetet e pajisjet e transmetimit dhe ndërlidhja e sistemeve u nënshtrohen rregullave për sigurimin fizik të informacionit të klasifikuar "Sekret shtetëror", të përcaktuara me akte normative.

2. Rrjetet informatike ndërtohen në përputhje me strukturën organizative të institucionit, ku instalohen, dhe me nivelin më të lartë të informacionit të klasifikuar "Sekret shtetëror", që përpunohet.

3. Lidhja fizike me rrjetet vendore informatike duhet të bëhet në mënyrë të sigurtë, me fibra optike, me pajisje të certifikuara, duke përdorur më shumë se një tip barriere, të cilat mbështesin njëra-tjetrën.

4. Ndalohet përdorimi i pajisjeve, si modema personale, wireless, akses point etj., të cilat krijojnë lidhje të pakontrolluara me rrjetin informatik. Lidhjet ndërmjet rrjeteve bëhen me pajisje të kriptuara, sisteme kriptografike, që plotësojnë kërkesat dhe standardet e sigurisë.

5. Sigurimi fizik i serverave të rrjetit vendor informatik përputhet me nivelin e masave të sigurisë për informacionin e klasifikuar "Sekret shtetëror", të nivelit më të lartë, që ai ruan.

6. Sistemet, rrjetet informatike, rrjetet e pajisjet e transmetimit dhe ndërlidhja e sistemeve, që përdoren për përpunimin e informacionit të klasifikuar "Sekret shtetëror" a "Konfidencial e lart" duhet të mbrohen nga emetimet elektromagnetike kompromentuese, studimi dhe kontrolli i të cilave referohet si

“TEMPEST”.

Masat e marra duhet të jenë në përputhje me përdorimin dhe ndjeshmërinë e informacionit.

B. Siguria e personelit, që punon në sisteme, rrjete informatike, mjete e pajisje të transmetimit, ndërlidhje të sistemeve dhe mbrojtje kriptografike

1. Personeli, që punon në sisteme, rrjete informatike, mjete e pajisje të transmetimit, ndërlidhje të sistemeve dhe mbrojtje kriptografike, duhet të jetë i pajisur, më parë, me “Certifikatë sigurie” të përshtatshme, niveli i së cilës është në përputhje me nivelin më të lartë të informacionit të klasifikuar “Sekret shtetëror”, që njeh e administron ky personel.

Administratorët dhe përdoruesit e rrjetit të klasifikuar nuk duhet të lejojnë akses të paautorizuar në informacionin e klasifikuar “Sekret shtetëror”.

2. Personeli, që punon në sisteme, rrjete informatike, mjete e pajisje të transmetimit, ndërlidhje të sistemeve dhe mbrojtje kriptografike, para përdorimit të tyre, duhet të jetë i trajnuar në fushën e operimit dhe të shfrytëzimit të sistemeve përkatëse, dhe, veçanërisht, të ketë njohuri për veprimet, që cenojnë sigurinë e tyre.

3. Administratorët e rrjetit, oficeri i sigurisë dhe personeli mbështetës janë përgjegjës për zbatimin e masave të sigurisë. 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 të shfrytëzimit të rrjetit dhe të sigurisë së informacionit.

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

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

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

2. Kompjuterët, që punojnë jashtë rrjetit dhe trajtojnë informacion të klasifikuar “Sekret shtetëror”, duhet të sigurojnë nivelin maksimal të mbrojtjes, fizike dhe elektronike, në përputhje me nivelin më të lartë të klasifikimit të informacionit, që trajtohet në to.

3. Masat e sigurisë përcaktohen sipas nivelit të klasifikimit të informacionit, që trajtohet, ndërsa e drejta e personelit, për t’u njohur me informacionin e klasifikuar, përcaktohet sipas parimit “nevojë për njohje”.

Në masat e sigurisë parashikohen mbrojtja nga dëmtimet, që shkaktojnë viruset e ndryshme, disiplinimi dhe kontrolli i hyrjes në rrjet, si dhe parandalimi i ndërhyrjeve me synime keqdashëse.

4. Përdoruesit e rrjetit 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. Fjalëkalimet ndërtohen në bazë të procedurave, në përputhje me politikat e sigurisë, dhe ndërrohen periodikisht.

5. Fjalëkalimet e superadministratorëve ruhen nga administratorët, në formën e një *database*, të shifruar ose në zarfe të mbyllur brenda në kasafortë. Kasaforta u nënshtrohet kushteve të sigurisë, në nivelin më të lartë.

6. Përdoruesit e rrjetit përgjigjen për fshehtësinë e fjalëkalimeve të tyre dhe raportojnë incidentet e vërejtura, që cenojnë sigurinë e rrjetit informatik.

7. Rrjeti informatik duhet të ruajë gjurmët e përdorimit dhe të ndryshimit të fjalëkalimeve, përpjekjet, e suksesshme ose të pasuksesshme, për t’u futur në rrjet, printimin e informacioneve të klasifikuara, si dhe ngjarjet jonormale, si p.sh., puna me rrjetin e klasifikuar, qëndrimi jashtë orarit zyrtar etj.

Për çdo ngjarje duhet ruajtur ora, data, tipi dhe origjina e ngjarjes.

8. Përdoruesit të rrjetit informatik i ndalohet:

a) të provojë për t’u futur në rrjet me një identitet tjetër;

b) të provojë për të njohur dhe administruar informacion të klasifikuar “Sekret shtetëror”, jashtë të drejtave që ka;

c) të importojë apo eksportojë informacion të klasifikuar “Sekret shtetëror”, aplikime, lojëra me media të lëvizshme etj.

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

d) të përdorë në rrjetin e klasifikuar media të lëvizshme, si disketa, CD, flesh drive etj., pa autorizimin, me shkrim, të titullarit të institucionit.

9. Mirëmbajtja e hardware-ve.

Mirëmbajtja e pajisjeve të ndryshme të rrjetit informatik duhet të bëhet brenda zonës së sigurisë përkatëse nga personeli përgjegjës dhe i certifikuar përshtatshmërisht.

Në qoftë se pajisjet e sistemeve të klasifikuara deklarohen të tepërta ose të papërdorshme, informacioni i klasifikuar, që mund të përmbajnë ato, kur është e mundur, transferohet e sigurohet.

Më pas, shkatërrohet media përkatëse, që përmbante informacion të klasifikuar "Konfidencial e lart", dhe bëhet deklasifikimi i pajisjeve, sipas rregullave të përcaktuara, në mbikëqyrjen e personelit të sigurisë.

Media e kompjuterit, që përmban informacion të klasifikuar "I kufizuar", mund të shfrytëzohet për qëllim tjetër, pas deklasifikimit të saj.

Në qoftë se pajisja nxirret jashtë zonës së sigurisë, informacioni i klasifikuar, që mund të përmbajë, pasi transferohet dhe sigurohet, kur është e mundur, asgjësohet nga media përkatëse.

Më pas, shkatërrohet media përkatëse me mënyra profesionale, sipas rregullave të përcaktuara, dhe bëhet deklasifikimi i pajisjes.

10. Mirëmbajtja e software-ve.

Mirëmbajtja e softeve, që kontribuojnë në sigurinë e sistemit, kryhet nga personeli i certifikuar, i cili mban përgjegjësi jo vetëm për miratimin dhe zbatimin e ndryshimeve, që mund t'u bëhen softeve, por edhe për vazhdimësinë e sigurisë së rrjetit, pas zbatimit të këtyre ndryshimeve.

Ky personel është përgjegjës për hartimin dhe zbatimin e procedurave për menaxhimin dhe kontrollin e origjinës së softeve, prokurimin, instalimin dhe mënyrën e përdorimit të tyre, duke përcaktuar:

a) përdorimin e softeve të licencuara;

b) ndalimin e përdorimit të softeve pirate dhe të softeve, me përdorim të kufizuar kohor, sepse përmbajtja e tyre mund të jetë modifikuar;

c) ndalimin e instalimit në rrjet të softeve të panevojshme;

ç) ndalimin e modifikimit të softit, të sistemit nga përdoruesit, mbrojtjen e softit të sistemit dhe monitorimin e çdo përpjekje për akses të paautorizuar.

11. Administratorët e rrjetit dhe personeli përgjegjës për sigurinë e tij, për të zvogëluar risqet, me të cilat mund të përballet rrjeti informatik, duhet të marrin masa:

a) për të parë, duke kryer kontrollin periodik të konfigurimit, fizik dhe elektronik, ndryshimet në rrjet, masat e sigurisë së informacionit të klasifikuar "Sekret shtetëror" dhe përshtatjen e tyre me arritjet e kohës;

b) për të ruajtur informacionin e klasifikuar "Sekret shtetëror" dhe konfigurimin e rrjeteve, që e përpunojnë atë, duke bërë rezervimin e tyre në media të ndryshme, si shirit manjetik, CD dhe server rezervë (Backup server). Pajisjet, ku ruhet backup-i, u nënshtrohen testimeve të vazhdueshme për rindërtimin e sistemeve. Për ruajtjen e këtyre pajisjeve krijohen kushte të veçanta, në përputhje me nivelin më të lartë të klasifikimit të informacionit, që është regjistruar në to;

c) duke monitoruar veprimtarinë e përdoruesve në rrjet, për të zbuluar dhe parandaluar ngjarjet, që mund të cenojnë sigurinë e informacionit të klasifikuar "Sekret shtetëror";

ç) duke prishur, me autorizim, informacionin e klasifikuar "Sekret shtetëror", të magazinuar në media të ndryshme, me mënyra profesionale, ose duke bërë shkatërrimin e tyre fizik. Prishja bëhet vetëm kur është e domosdoshme dhe pasi informacioni i klasifikuar "Sekret shtetëror" është printuar dhe regjistruar;

d) duke printuar dhe administruar dokumentet e klasifikuara, sipas rregullave përkatëse;

dh) duke ndaluar trajtimin e informacionit të klasifikuar "Sekret shtetëror", në pajisjet kompjuterike private dhe futjen e këtyre pajisjeve në mjediset ose rrjetet, ku ruhet, përpunohet dhe transmetohet informacion i klasifikuar.

D. Analiza e vlerësimit të riskut

1. Analiza e vlerësimit të riskut është një proces i vazhdueshëm analitik për mbledhjen e të dhënave, në shërbim të mbrojtjes së informacionit të klasifikuar.

2. Qëllimi i analizës së vlerësimit të riskut është përcaktimi i rreziqeve dhe i dëmeve, që mund të shkaktohen nga aksesi ose përpjekjet për akses të paautorizuar në rrjetet informatike, mjetet e pajisjet e transmetimit, ndërlidhjen e sistemeve dhe mbrojtjen kriptografike, e i pasojave, që mund të vijnë nga veprimtaritë terroriste apo aktet e sabotimit.

3. Analiza e vlerësimit të riskut duhet të bëhet sipas kritereve të mëposhtme:

a) nivelit të klasifikimit të informacionit;

b) vëllimit dhe tipit të informacionit të klasifikuar;

c) numrit të “Certifikatave të sigurisë”, të lëshuara sipas parimit “nevojë për njohje”, dhe nivelit të tyre të klasifikimit;

ç) mënyrës së ruajtjes së informacionit të klasifikuar.

4. Procesi i analizës së vlerësimit të riskut përmban:

a) përcaktimin e pjesëve të sistemit, të ekspozuara ndaj riskut;

b) përcaktimin e shkallës së rrezikut dhe të dobësisë së sistemit, kur aksesohet në mënyrë të paautorizuar;

c) analizën e masave ekzistuese të sigurisë;

ç) përmirësimin e masave të sigurisë së sistemit;

d) përcaktimin e riskut të mbetur dhe pranueshmërinë e tij;

dh) inspektimet periodike, rishikimet dhe rivlerësimet e riskut.

5. Procesi i analizës së vlerësimit të riskut kryhet nga personeli përgjegjës për sigurinë e sistemit.

E. Sigurimi i komunikimeve

Drejtoria e shifrës, strukturë në varësi të Shërbimit Informativ të Shtetit, është Autoriteti Kombëtar për Sigurimin e Komunikimeve dhe Autoriteti Kombëtar i Shpërndarjes.

Autoriteti Kombëtar i Sigurimit të Komunikimeve

Detyrat kryesore të këtij autoriteti janë:

1. Hartimi, prodhimi, instalimi dhe kontrolli i përdorimit të shifrës për të gjitha institucionet shtetërore.

2. Mbrojtja e informacionit të klasifikuar “Sekret shtetëror” në të gjitha strukturat shtetërore, kur ky informacion transmetohet me mjete të komunikimit, masiv e publik.

3. Përdorimi i mjeteve, pajisjeve e sistemeve kriptografike, të specializuara, fortësia e të cilave duhet të jetë në përputhje me nivelin e klasifikimit të informacionit.

4. Përdorimi i sistemeve kriptografike, i mjeteve e i pajisjeve të komunikimit të informacionit të klasifikuar “Sekret shtetëror” bëhet pas miratimit e certifikimit nga DSIK-ja.

Autoriteti Kombëtar i Shpërndarjes

Autoriteti Kombëtar i Shpërndarjes është përgjegjës për menaxhimin e materialit shifror. Detyrat e këtij autoriteti janë:

1. Shpërndarja e materialit çelës kriptografik në organet shtetërore;

2. Zbatimi i rregullave të sigurimit, fizik dhe elektronik, sipas akteve nënligjore në fuqi, për ruajtjen e materialit çelës kriptografik;

3. Sigurimi i materialit çelës kriptografik, me qëllim që të jetë në çdo kohë në kushte pune;

4. Shkatërrimi i materialit çelës kriptografik, sipas rregullores, kur është e nevojshme;

5. Hartimi i procedurave, që duhen ndjekur për raportimin e incidenteve;

6. Hartimi i procedurave, që duhen ndjekur në rastet e emergjencës;

7. Sigurimi se i gjithë personeli, që ka akses në materialin çelës kriptografik, është i autorizuar, i certifikuar, sipas akteve nënligjore në fuqi, dhe i trajnuar.

III. RREGULLA TË VEÇANTA

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

2. Ngarkohen institucionet shtetërore për zbatimin e këtij vendimi. Drejtuesit e këtyre institucioneve, brenda 30 ditëve nga hyrja në fuqi e këtij vendimi, detyrohen të nxjerrin rregullore, në zbatim të këtij vendimi.

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

4. Vendimi nr.478, datë 19.7.2001 i Këshillit të Ministrave “Për sigurimin e informacionit të klasifikuar “Sekret shtetëror” në rrjetet informatike, mjetet dhe pajisjet e transmetimit”, shfuqizohet.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTRI
Sali Berisha