V E N D I M

Nr. 922, Datë 19.12.2007

PËR

SIGURIMIN E INFORMACIONIT TË KLASIFIKUAR "SEKRET SHTETËROR" QË PRODHOHET, RUHET, PERPUNOHET APO TRANSMETOHET NE SISTEMET E KOMUNIKIMIT (INFOSEC)

Në mbështetje të nenit 100, të Kushtetutës dhe neneve 23 e 31, të ligjit Nr. 8457, Datë 11.02.1999 "Për informacionin e klasifikuar "Sekret Shtetëror"", i ndryshuar, me propozimin e Kryeministrit, Këshilli i Ministrave,

V E N D O S I:

I. KËRKESAT PËR SISTEMET E KOMUNIKIMIT (INFOSEC)

1. Institucionet shtetërore, që për nevoja të punës prodhojnë, ruajnë, përpunojnë, shpërndajnë ose transmetojnë, mbrojnë informacion të klasifikuar "sekret shtetëror", nëpërmjet sistemeve, rrjeteve informatike, mjeteve dhe pajisjeve të transmetimit, ndërlidhjen e sistemeve dhe mbrojtjen kriptografike**,** duhet t'u përmbahen kërkesave të përcaktuara në këtë vendim.

2. Sistemet, rrjetet informatike, mjetet dhe pajisjet e transmetimit, ndërlidhja e sistemeve dhe mbrojtja kriptografike, ku prodhohet, ruhet, përpunohet, shpërndahet ose transmetohet, 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 te rrjetit informatik te klasifikuar, mjeteve dhe pajisjeve te transmetimit, pajisjet e ndryshme te mbrojtjes kriptografike, te sigurohen nga shoqeri proshuese ose tregtare te specializuar dhe te mirenjohura ne tregun nderkombetar, sipas kerkesave te legjislacionit per prokurimin publik.

4. Institucioni shtetëror, para përdorimit të sistemeve, rrjetit informatik, mjeteve e pajisjeve të transmetimit, ndërlidhjes së sistemeve, mbrojtjes kriptografike, i kërkon DSIK-së, lëshimin e "Çertifikatës së Sigurisë së Sistemit".
DSIK-ja është Autoriteti Kombëtar i Akreditimit të Sigurisë, i cili lëshon çertifikatat e sigurisë përkatëse.

Kërkesa e institucionit shtetëror për pajisje me "çertifikatë sigurie" të përshtatëshme shoqërohet me dokumentacionin e mëposhtëm:

1- Deklaratën e sigurisë së sistemit.

2- Rregulloren e institucionit për sigurinë, e cila është një përshkrim i saktë i zbatimit të deklaratës së sigurisë së sistemit, proçedurat operacionale që duhen ndjekur dhe përgjegjësitë e personelit.

3- Raportin mbi analizën e vlerësimit të riskut për sigurinë e sistemit.

4- 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 çertifikatës së sigurisë dhe deklaratës së sigurisë përcaktohen nga DSIK-ja.
Deklaratat e sigurisë janë:

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

5. Deklarata e sigurisë, përmban përshkrimin e plotë dhe të hollësishëm të sigurisë të sistemit, rrjetit informatik, mjeteve dhe pajisjeve të transmetimit, ndërlidhjes së sistemeve, mbrojtjes kriptografike, gjatë instalimit dhe shfrytëzimit.
Deklarata e sigurisë plotësohet nga institucioni shtëtëror që paraqet në DSIK kërkesën për akreditim.

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

6. DSIK-ja, shqyrton kërkesën e paraqitur brenda afateve të mëposhtme:

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

7. Pas shqyrtimi 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.

Nëqoftëse sistemet, rrjetet informatike, mjetet dhe pajisjet e transmetimit, ndërlidhja e sistemeve dhe mbrojtja kriptografike përmbushin kërkesat dhe standartet e sigurisë të informacionit të klasifikuar “sekret shtetëror” të përcaktuara në këtë vendim, DSIK -ja lëshon “Çertifikatën 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, mbrohet në këtë sistem.

8. "Çertifikata e sigurisë e rrjetit" është dokumenti që vërteton se tërësia e mjeteve dhe pajisjeve, që përbëjnë rrjetin informatik, ku prodhohet, ruhet, përpunohet, shpërndahet ose transmetohet, dhe mbrohet informacioni i klasifikuar "sekret shtetëror", plotësojnë standartet e sigurisë.

9. "Çertifikata e sigurisë e mjetit", është dokumenti që vërteton se mjeti apo pajisja e transmetimit, plotëson standartet e sigurisë së informacionit të klasifikuar "sekret shtetëror".

10. "Çertifikata e sigurisë e ndërlidhjes së sistemeve/rrjeteve" është dokumenti që vërteton se tërësia e mjeteve dhe pajisjeve që përbëjnë lidhjen e dy ose më shumë sistemeve/rrjeteve ku transmetohet informacioni i klasifikuar "sekret shtetëror", plotësojnë standartet e sigurisë.

11. "Çertifikata e sigurisë e shifrës", është dokumenti që vërteton se mbrojtja kriptografike me këtë shifër, plotëson standartet e sigurisë së informacionit të klasifikuar "sekret shtetëror".

12. Në rast mosmiratimi të kërkesës për çertifikim, subjekti kërkues, brënda 10 ditëve, ka të drejtë të ankohet tek Kryeministri, vendimi i të cilit është përfundimtar.

13. Pas çertifikimit të sistemit, institucioni të cilit i është lëshuar "çertifikata e sigurisë", është i detyruar të raportojë menjëherë në DSIK për:

- çdo ndryshim që cënon sigurinë në konfigurimin e hardit ose softit të sistemit, shoqëruar me kërkesën për ri-akreditim për pjesën që ndryshon, në kushtet e çertifikimit të mëparshëm.
- çdo incident që cënon sigurinë e sistemit.

14. Personi apo personat, punonjës të institucionit, që instalojnë, mirëmbajnë ose riparojnë rrjetin informatik, mjetet apo pajisjet e transmetimit, sistemet e ndërlidhjes së sistemeve duhet të jenë të pajisur më parë me "Çertifikatë sigurie" të përshtatëshme. Në qoftë se nuk janë punonjës të institucionit, ata duhet të jenë nën mbikëqyrjen e vazhdueshme të personelit të kualifikuar teknikisht dhe të çertifikuar përshtatmërisht të institucionit. Në qoftë se punimet do të kryhen nga subjekte shtetërore, private, vendase apo te huaja, të zbatohen kërkesat për sigurimin e informacionit të klasifikuar "sekret shtetëror" në fushën industriale.

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

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

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

1. Rrjetet informatike, mjetet dhe pajisjet e transmetimit, ndërlidhja e sitemeve i nënshtrohen rregullave për sigurimin fizik të informacionit të klasifikuar "sekret shtetëror", të përcaktuara me akte të tjera normative. 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.

2. Lidhja fizike me rrjetet lokale informatike të bëhet në mënyrë të sigurtë, me fibra optike, me pajisje të çertifikuara, duke përdorur më shumë se një tip barriere, të cilat mbështesin njera-tjetrën.

3. Ndalohet përdorimi i pajisjeve, si modema personal, wireless, akses point, etj., të cilët krijojnë lidhje të pakontrolluara me rrjetin informatik. Lidhjet midis rrjeteve të bëhen me pajisje të kriptuara, sisteme kriptografike që plotësojnë kërkesat dhe standartet e sigurisë.

4. Sigurimi fizik i serverave të rrjetit lokal informatik të përputhet me nivelin e masave të sigurisë së informacionit të klasifikuar "sekret shtetëror" të nivelit më të lartë që ai ruan.

5. Sistemet, rrjetet informatike, mjetet dhe pajisjet e transmetimit, ndërlidhja e sitemeve, që përdoren për përpunimin e informacionit të klasifikuar "sekret shtetëror" KONFIDENCIAL e lart, të mbrohen nga emetimet elektromagnetike kompromentuese, studimi dhe kontrolli i të cilave referohet si "TEMPEST". Masat e mara të jënë në përputhje me përdorimin dhe ndjeshmërinë e informacionit.

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

1. Personeli që punon në sisteme, rrjete informatike, mjete dhe pajisje të transmetimit, ndërlidhje të sistemeve dhe mbrojtje kriptografike të jetë i pajisur me parë me çertifikatë sigurie të përshtatëshme. Niveli i "Çertifikatës së sigurisë" të jetë në përputhje me nivelin më të lartë të informacionit të klasifikuar "sekret shtetëror", që njeh dhe administron ky personel. Administratorët dhe përdoruesit e rrjetit të klasifikuar, të mos lejojnë aksesin e pa-autorizuar të informacionit të klasifikuar "sekret shtetëror".

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

3. Administratorët e rrjetit, oficeri i sigurisë dhe personeli mbështetës janë përgjegjës për zbatimin e masave të sigurisë së tij. Ata pajisen me "Çertifikatë 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 dhe sigurisë së informacionit.

4. Personat, të cilët për nevoja pune, hyjnë në ambjentet me sisteme/rrjete informatike, etj, i 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 shteteror", në rrjetet informatike, të bëhet në të gjitha fazat e ciklit të plotë të tij.

2. Kompjuterat që punojnë jashtë rrjetit dhe trajtojnë informacion të klasifikuar "sekret shtetëror", 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". Masat e sigurisë të parashikojnë mbrojtjen nga dëmtimet që shkaktojnë viruset e ndryshëm, 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. Fjalëkalimet ndërtohen mbi bazën e proçedurave bazuar në politikat e sigurisë dhe ndërrohen periodikisht.

5. Fjalëkalimet e super administratorëve ruhen nga administratorët në formën e një databaze të shifruar, ose në zarfe të mbyllur brënda në kasafortë. Kasaforta i 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 cënojnë sigurinë e rrjetit informatik.

7. Rrjeti informatik duhet të ruajë gjurmët e përdorimit dhe ndryshimit të fjalëkalimeve, përpjekjet e suksesshme ose të pa-suksesshme për tu futur në rrjet, printimin e informacioneve të klasifikuara, si dhe ngjarjet jo-normale si puna me rrjetin e klasifikuar 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 orvatet të futet në 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, lojra me media të lëvizëshme, 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 lëvizëshme 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 brënda zonës së sigurisë përkatëse nga personeli përgjegjës dhe i çertifikuar përshtatshmërisht. Në qoftëse pajisjet e sistemeve të klasifikuara deklarohen të tepërta ose të papërdorëshme, 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, nën mbikëqyrjen e personelit të sigurisë.

Media e kompjuterit që përmbante informacion të klasifikuar I KUFIZUAR, mund të përdoret për shfrytëzim 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 metoda profesionale dhe bëhet deklasifikimi i pajisjes.

10. Mirëmbajtja e software-ve.

Mirëmbajtja e softeve që kontribuojnë në sigurinë e sistemit të kryhet nga personeli i çertifikuar përshtatshmërisht, i cili mban përgjegjësi jo vetëm për miratimin dhe zbatimin e ndryshimeve që mund ti bëhen softeve, por edhe për vazhdimësinë e sigurisë së rrjetit, pas zbatimit të ndryshimeve të bëra.

Ky personel është përgjegjës për hartimin dhe zbatimin e proçedurave për menaxhimin dhe kontrollin e origjinës së softeve, prokurimin, instalimin dhe mënyrën e përdorimit të tyre, si më poshte:

a) softet të jenë të liçensuara;
b) ndalohet përdorimi i softeve pirate dhe softeve me përdorim të kufizuar kohor, sepse përmbajtja e tyre mund të jetë modifikuar;
c) ndalohet instalimi i softeve të panevojshme në rrjet;
d) ndalohet modifikimi i softit të sistemit nga përdoruesit; të mbrohet softi i sistemit dhe të monitorohet çdo tentativë për akses të pa-autorizuar të tij;

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

a) Rrjeti informatik i nënshtrohet kontrollit periodik të konfigurimit fizik dhe elektronik, për të parë 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, bëhet rezervimi i 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 të krijohen kushte të veçanta, në përputhje me nivelin më të lartë të klasifikimit të informacionit që është regjistruar në to.
c) Veprimtaria e përdoruesve dhe administratorëve të rrjetit duhet të auditohet (monitorohet), për të zbuluar dhe parandaluar ngjarjet që mund të cënojnë sigurinë e informacionit të klasifikuar "sekret shtetëror".
d) Prishja e autorizuar e informacionit te klasifikuar "sekret shtetëror" të magazinuar në media të ndryshme, bëhet me metoda profesionale ose me shkatërrimin e tyre fizik. Prishja të bëhet vetëm kur është e domosdoshme dhe pasi informacioni i klasifikuar "sekret shteteror" të jetë printuar dhe rregjistruar.
e) Printimi dhe administrimi i dokumenteve të klasifikuara të bëhet sipas rregullave përkatëse.
f) Ndalohet trajtimi i informacionit të klasifikuar "sekret shtetëror", në pajisjet kompjuterike private dhe futja e këtyre pajisjeve në ambientet ose rrjetet ku ruhet, përpunohet dhe transmetohet informacion i klasifikuar.

D. Analiza e Vlerësimit te Riskut.

1. Analiza e vlerësimit të riskut është një proçes i vazhdueshëm analitik për mbledhjen e të dhënave, analizën dhe vlerësimin nga pikëpamja e mbrojtjes së informacionit të klasifikuar.

2. Qëllimi i analizës së vlerësimit të riskut është përcaktimi i rreziqeve dhe dëmeve që mund të shkaktohen nga aksesi ose tentativat për akses të pa-autorizuar në rrjetet informatike, mjetet e pajisjet të transmetimit, ndërlidhjen e sitemeve dhe mbrojtjen kriptografike, pasojat që mund të vijnë nga aktivitetet 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) volumit dhe tipit të informacionit të klasifikuar;
   c) numrit të "Çertifikatave të sigurisë" të lëshuara sipas parimit nevojë-për-njohje dhe niveli i tyre i klasifikimit;
   d) mënyra e ruajtjes së informacionit të klasifikuar.

4. Proçesi i analizës së vlerësimit të riskut duhet të përmbajë:

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

b) përcaktimin e shkallës së rrezikut dhe dobësisë së sistemit kur ai aksesohet në mënyrë të pa-autorizuar;
c) analiza e masave ekzistuese të sigurisë;
ç) përmirësimi i masave të sigurisë së sistemit;
d) përcaktimi i riskut të mbetur dhe pranueshmëria e tij;
e) inspektime periodike, rishikime dhe rivlerësime të 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 i shifrës, 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 të jetë në përputhje me nivelin e klasifikimit të informacionit.

4. Përdorimi i sisteme kriptografike, mjeteve e pajisjeve të komunikimit të informacionit të klasifikuar "sekret shtetëror", të bëhet pas miratimit e çertifikimit nga DSIK-ja.

Autoriteti Kombëtar i Shpërndarjes.

Autoriteti Kombëtar i Shpërndarjes është përgjegjës për menaxhimin e materialit shifrar. 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 që materiali çelës kriptografik të jetë në çdo kohë në kushte pune;
4. Shkatërrimin i materialit çelës kriptografik, sipas rregullores kur është e nevojshme,;
5. Hartimi i proçedurave që duhen ndjekur për raportimin e incidenteve;
6. Hartimi i proçedurave që duhen ndjekur ne rastet e emergjencës;
7. Sigurimi që i gjithë personeli që ka akses në materialin çelës kriptografik është i autorizuar, i çertifikuar 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, brënda 30 ditëve nga hyrja në fuqi e këtij vendimi, detyrohen të nxjerrin rregullore për zbatimin e këtij vendimi.
3. Ngarkohet Drejtoria e Sigurimit të Informacionit të Klasifikuar për ndjekjen e zbatimit të këtij vendimi.

4. Vendimi Nr. 478, Datë 19.07.2001, i Këshillit të Ministrave "Për sigurimin e informacionit te klasifikuar "sekret shtetëror" në rrjetet informatike, mjetet dhe pajisjet e transmetimit" shfuqizohet.

Ky vendim hyn në fuqi pas botimit në "Fletoren Zyrtare".

K R Y E M I N I S T R I

SALI BERISHA