REPUBLIKA E SHQIPËRISË
KUVENDI

LIGJ

Nr. 2/2017

PËR SIGURINË KIBERNETIKE[1]

Në mbështetje të neneve 78 dhe 83, pika 1, të Kushtetutës, me propozimin e Këshillit të Ministrave,

K U V E N D I

I REPUBLIKËS SË SHQIPËRISË

V E N D O S I:

KREU I

DISPOZITA TË PËRGJITHSHME

Neni 1

Qëllimi i ligjit

Qëllimi i këtij ligji është arritja e një niveli të lartë të sigurisë kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet, si dhe bashkëpunimin e ndërsjellë ndërmjet subjekteve që operojnë në fushën e sigurisë kibernetike.

Neni 2

Fusha e zbatimit

1. Ky ligj zbatohet për rrjetet e komunikimit dhe sistemet e informacionit, cenimi apo shkatërrimi i të cilave do të kishte impakt në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.
2. Përjashtohen nga zbatimi i këtij ligji rrjetet e komunikimeve elektronike dhe sistemet e informacionit që janë objekt i rregullimeve ligjore në fuqi për nënshkrimin elektronik,

[1] *Ky ligj është përafruar pjesërisht me Direktivën (BE) 2016/1148 të Parlamentit Europian dhe të Këshillit, datë 6 korrik 2016, "Mbi masat për një nivel të përbashkët të lartë të sigurisë së rrjeteve dhe sistemeve të informacionit në Bashkimin Europian". Numri CELEX: 32016L1148, Fletorja Zyrtare e Bashkimit Europian, Seria L, nr. 194, datë 19.7.2016, faqe 1-30.*

identifikimin elektronik dhe shërbimet e besuara, rrjetet e komunikimeve elektronike dhe sistemet e informacionit që përpunojnë, arkivojnë ose transmetojnë informacion të klasifikuar shtetëror, të cilat rregullohen me ligjin nr. 8457, datë 11.2.1999, "Për informacionin e klasifikuar "Sekret shtetëror"", si dhe rrjetet e komunikimeve elektronike e sistemet e informacionit, për aq sa parashikohet në legjislacionin mbi komunikimet elektronike në Republikën e Shqipërisë.

Neni 3

Përkufizime

Në këtë ligj termat e mëposhtëm kanë këto kuptime:

1. "Autoriteti Përgjegjës për Certifikimin Elektronik dhe për Sigurinë Kibernetike", në vijim Autoriteti, është institucioni përgjegjës, i krijuar në bazë të legjislacionit në fuqi për nënshkrimin elektronik.

2. "CSIRT" është Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kompjuterike.

3. "Hapësirë kibernetike" është mjedisi digjital i aftë të krijojë, të procesojë dhe të shkëmbejë informacionin e krijuar nga sistemet, shërbimet e shoqërisë së informacionit, si dhe rrjetet e komunikimit elektronik.

4. "Incident i sigurisë kibernetike" është një ngjarje e sigurisë kibernetike, gjatë së cilës shkaktohet cenimi i sigurisë së shërbimeve ose sistemeve të informacionit e të rrjeteve të komunikimit dhe sjell një efekt real negativ.

5. "Infrastrukturë e rëndësishme e informacionit" është tërësia e rrjeteve dhe sistemeve të informacionit të zotëruara nga një autoritet publik, i cili nuk është pjesë e infrastrukturës kritike të informacionit, por që mund të rrezikojë apo të kufizojë punën e administratës publike në rastin e cenimit të sigurisë së informacionit.

6. "Infrastrukturë kritike e informacionit" është tërësia e rrjeteve dhe sistemeve të informacionit, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë dhe/ose mirëqenien ekonomike të qytetarëve dhe/ose funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.

7. "Ministër përgjegjës" është ministri që ka në fushën e veprimtarisë së tij çështjet e teknologjisë së informacionit e të komunikimit.

8. "Operator i infrastrukturës kritike të informacionit" është një person juridik, publik ose privat, që administron infrastrukturën kritike të informacionit.

9. "Operator i infrastrukturës së rëndësishme të informacionit" është një person juridik publik, që administron infrastrukturë të rëndësishme të informacionit.

10. "Rrezik i sigurisë kibernetike" është një rrethanë ose një ngjarje, e identifikueshme në mënyrë të arsyeshme, e cila mund të shkaktojë cenimin e sigurisë së shërbimeve ose sistemeve të informacionit dhe të rrjeteve të komunikimit.

11. "Rrjet i komunikimit dhe sistem i informacionit" do të thotë:

a) një rrjet i komunikimeve elektronike, në kuptimin e pikës 36, të nenit 3, të ligjit nr. 9918, datë 19.5.2008, "Për komunikimet elektronike në Republikën e Shqipërisë", të ndryshuar";

b) çdo pajisje ose grup i lidhur ose i ndërlidhur i pajisjeve, nga të cilat, një ose më shumë se një, në bazë të një programi, kryejnë përpunimin automatik të të dhënave digjitale; ose

c) të dhënat digjitale të ruajtura, të përpunuara, të gjetura ose të transmetuara nga elementet e parashikuara në shkronjat "a" dhe "b", të kësaj pike, për qëllim të funksionimit, përdorimit, mbrojtjes dhe mirëmbajtjes së tyre.

12. "Siguria e informacionit" është sigurimi i konfidencialitetit, integritetit dhe disponueshmërisë së informacionit.

13. “Siguria kibernetike” është tërësia e mjeteve ligjore, organizative, teknike dhe edukative, me qëllim mbrojtjen e hapësirës kibernetike.

Neni 4

Përpunimi i të dhënave personale

Përpunimi i të dhënave personale, për qëllim të zbatimit të këtij ligji, duhet të kryhet në përputhje me dispozitat e ligjit nr. 9887, datë 10.3.2008, “Për mbrojtjen e të dhënave personale”, të ndryshuar.

KREU II

SUBJEKTET PËRGJEGJËSE NË FUSHËN E SIGURISË KIBERNETIKE

Neni 5

Kompetencat e autoritetit përgjegjës në fushën e sigurisë kibernetike

1. Autoriteti përgjegjës ka këto kompetenca në fushën e sigurisë kibernetike:

a) përcakton masat e sigurisë kibernetike;

b) vepron si pikë qendrore kontakti në nivel kombëtar për operatorët përgjegjës në fushën e sigurisë kibernetike dhe bashkërendon punën për zgjidhjen e incidenteve të sigurisë kibernetike;

c) administron raportet e incidenteve në fushën e sigurisë kibernetike dhe siguron ruajtjen e regjistrimin e tyre;

ç) siguron ndihmë dhe mbështetje metodike për operatorët përgjegjës në fushën e sigurisë kibernetike;

d) kryen analiza për dobësitë e konstatuara në fushën e sigurisë në internet;

dh) kryen aktivitete ndërgjegjësimi dhe edukimi në fushën e sigurisë kibernetike;

e) vepron në cilësinë e CSIRT-së kombëtare.

2. Autoriteti koordinon veprimtaritë e tij me institucionet e sigurisë dhe të mbrojtjes dhe bashkëpunon me CSIRT-të sektoriale dhe autoritetet ndërkombëtare në fushën e sigurisë kibernetike, nëpërmjet marrëveshjeve të përbashkëta, në përputhje me legjislacionin në fuqi.

Neni 6

Subjekte të tjera përgjegjëse

1. Subjekte të tjera përgjegjëse në fushën e sigurisë kibernetike janë:

a) operatorët e infrastrukturës kritike të informacionit;

b) operatorët e infrastrukturës së rëndësishme të informacionit.

2. Këshilli i Ministrave, me propozimin e ministrit përgjegjës, miraton listën e infrastrukturave kritike të informacionit dhe të infrastrukturave të rëndësishme të informacionit, e cila përditësohet të paktën një herë në dy vjet.

Neni 7

Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kompjuterike (CSIRT)

1. Ekipet e përgjigjes ndaj incidenteve të sigurisë kompjuterike (CSIRT) përbëhen nga specialistë të fushës së sigurisë kompjuterike pranë çdo operatori që administron infrastrukturën kritike të informacionit.

2. Operatorët e infrastrukturave të rëndësishme të informacionit duhet të kenë të paktën një person përgjegjës për incidentet e sigurisë kompjuterike.

3. Ministri përgjegjës nxjerr udhëzim për metodologjinë e punës, detyrat që duhet të zbatojnë ekipet ose personat përgjegjës dhe kriteret e përgjithshme që duhet të respektojnë operatorët në përzgjedhjen tyre.

KREU III

ADMINISTRIMI I SIGURISË KIBERNETIKE

Neni 8

Masat e sigurisë

1. Në masat e sigurisë përfshihet tërësia e veprimeve për rritjen e sigurisë së informacionit në sistemet e informacionit dhe disponueshmërinë e besueshmërinë e shërbimeve e të rrjeteve të komunikimit në hapësirën kibernetike.

2. Operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit janë të detyruar të zbatojnë masat e sigurisë, si dhe të dokumentojnë zbatimin e tyre.

3. Operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit janë të detyruar të zbatojnë kërkesat e masave të sigurisë gjatë ngritjes së infrastrukturës.

Neni 9

Llojet e masave të sigurisë

1. Subjektet përgjegjëse në fushën e sigurisë kibernetike, të ngarkuara me zbatimin e këtij ligji, detyrohen të zbatojnë masat e sigurisë të natyrës organizative dhe teknike.

2. Masat organizative janë ato të:

a) menaxhimit të sigurisë së informacionit;

b) menaxhimit të rrezikut;

c) politikave të sigurisë;

ç) sigurisë organizative;

d) kërkesave të sigurisë për palët e treta;

dh) menaxhimit të aseteve;

e) sigurisë së burimeve njerëzore dhe aksesit të personave;

ë) ngjarjeve të sigurisë e të menaxhimit të incidenteve të sigurisë kibernetike;

f) menaxhimit të vazhdimësisë së punës;

g) kontrollit dhe auditit.

3. Masat teknike janë ato të:

a) sigurisë fizike;

b) mbrojtjes së integritetit të rrjeteve të komunikimit;

c) verifikimit të identitetit të përdoruesve;

ç) menaxhimit për autorizimin e aksesit;

d) veprimtarisë së administratorëve e të përdoruesve;
dh) zbulimit të ngjarjeve të sigurisë kibernetike;
e) mjeteve të gjurmimit e të vlerësimit të ngjarjeve të sigurisë kibernetike;
ë) sigurisë së aplikacioneve;
f) pajisjeve kriptografike;
g) sigurisë së sistemeve industriale.

4. Autoriteti përcakton me rregullore përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë.

Neni 10

Rreziqet dhe incidentet e sigurisë kibernetike

Operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit janë të detyruar të marrin masat e duhura për të parandaluar dhe minimizuar ndikimin e rreziqeve dhe incidenteve të sigurisë kibernetike në infrastrukturat e tyre.

Neni 11

Raportimi i incidenteve të sigurisë kibernetike

1. Operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit janë të detyruar të raportojnë menjëherë pasi zbulojnë incidentet e sigurisë kibernetike pranë Autoritetit.

2. Autoriteti përcakton me rregullore llojet e kategoritë e incidentit të sigurisë kibernetike, si dhe formatin e elementet e raportit për incidentet e sigurisë kibernetike.

3. Në rastet e incidenteve dhe sulmeve ndaj sigurisë kibernetike të institucioneve kushtetuese, atyre të sigurisë dhe mbrojtjes, Autoriteti raporton menjëherë pranë drejtuesve të këtyre institucioneve mbi problematikën dhe masat që duhen ndërmarrë.

Neni 12

Ruajtja e të dhënave të incidentit

1. Autoriteti mban dhe administron regjistrin elektronik të incidenteve të sigurisë kibernetike, i cili përmban:
a) raportin e incidentit;
b) të dhëna për të identifikuar sistemin në të cilin ndodhi incidenti;
c) të dhëna për burimin e incidentit;
ç) procedurën e zgjidhjes së incidentit dhe rezultatin e saj.

2. Në menaxhimin e incidenteve, që prekin operatorët e përcaktuar në nenin 7, të këtij ligji, me qëllim përcaktimin e rëndësisë së incidentit, duhet të merren parasysh parametrat e poshtëshënuar:
a) numri i përdoruesve të prekur nga incidenti;
b) kohëzgjatja e incidentit;
c) shtrirja gjeografike e incidentit, në rast se mund të përcaktohet;
ç) dëmi financiar, në rast se mund të përcaktohet.

3. Autoriteti, me kërkesë të autoriteteve publike, jep të dhënat e administruara në lidhje me një incident kibernetik, vetëm në rast se kërkesa përputhet me qëllimet e përmbushjes së detyrave të tyre funksionale.

4. Autoriteti mund të vendosë të dhënat e administruara në lidhje me incidentet kibernetike në dispozicion të organizmave që kryejnë rolin e autoritetit në fushën e sigurisë kibernetike jashtë vendit dhe të operatorëve të tjerë që veprojnë në fushën e sigurisë kibernetike, me qëllim sigurimin e mbrojtjes së hapësirës kibernetike.

Neni 13

Konfidencialiteti i të dhënave

1. Nëpunësit e Autoritetit, që marrin pjesë në zgjidhjen e incidentit të sigurisë kibernetike, janë të detyruar të ruajnë konfidencialitetin e plotë për të gjitha të dhënat e përpunuara gjatë procedurës së zgjidhjes së incidentit. Konfidencialiteti duhet të ruhet edhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin, përveç rasteve të parashikuara në ligj.

2. Drejtori i Përgjithshëm i Autoritetit mund të heqë detyrimin për konfidencialitetin e të dhënave.

3. Ministri përgjegjës përcakton rastet dhe kriteret në të cilat hiqet detyrimi i konfidencialitetit të parashikuar në pikën 2 të këtij neni.

Neni 14

Masat në rast kërcënimi ose incidenti kibernetik

1. Me masa në rast kërcënimi ose incidenti kibernetik kuptohen veprimet e nevojshme, me qëllim mbrojtjen e sistemeve të informacionit apo rrjeteve të komunikimit elektronik ose veprimet, me qëllim zgjidhjen e një incidenti të konstatuar të sigurisë kibernetike.

2. Masat në rast kërcënimi ose incidenti kibernetik janë:

a) paralajmërimet;

b) kundërmasat;

c) masat mbrojtëse.

Neni 15

Paralajmërimet

1. Paralajmërimi është një rekomandim për përballjen me kërcënimin në fushën e sigurisë kibernetike. Në rast se Autoriteti konstaton ose merr dijeni për një kërcënim në fushën e sigurisë, jep paralajmërim.

2. Paralajmërimi u njoftohet subjekteve përgjegjëse në fushën e sigurisë kibernetike, sipas rastit. Paralajmërimi publikohet edhe në faqen e internetit të Autoritetit.

Neni 16

Kundërmasat

1. Kundërmasat janë veprime, me qëllim mbrojtjen nga rreziku kibernetik apo nga incidenti i sigurisë kibernetike ose veprime, me qëllim zgjidhjen e një incidenti të konstatuar.

2. Kundërmasat ndërmerren nga organet publike, operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit. Personi përgjegjës në cilësinë e pikës së kontaktit informon menjëherë Autoritetin për zbatimin e kundërmasave dhe rezultatin e tyre.

3. Autoriteti, në zbatim të këtij neni, përcakton kundërmasat, me qëllim zgjidhjen e incidentit kibernetik të sigurisë dhe detyrat e personave përgjegjës.

Neni 17

Masat mbrojtëse të natyrës së përgjithshme

1. Masat mbrojtëse të natyrës së përgjithshme janë masat e bazuara në një analizë të incidenteve të sigurisë kibernetike, tashmë të zgjidhura, me qëllim rritjen e mbrojtjes së sistemeve të informacionit, ose shërbimeve, ose rrjeteve të komunikimit elektronik.

2. Operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit janë të detyruar të marrin masa mbrojtëse të natyrës së përgjithshme.

3. Operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit njoftohen për nxjerrjen e masave të natyrës së përgjithshme përmes pikave të kontaktit.

4. Autoriteti nxjerr rregullore për masat mbrojtëse të natyrës së përgjithshme, të cilat publikohen në faqet e internetit të Autoritetit.

Neni 18

Pikat e kontaktit

1. Operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit caktojnë pikat e kontaktit, sipas përcaktimeve në këtë ligj. Në të dhënat për pikat e kontaktit përfshihen:

a) për personat juridikë: emri, adresa e selisë, numri i identifikimit (NIPT) të personit juridik ose numri i ngjashëm, i caktuar jashtë vendit, dhe të dhënat e personit të kontaktit që është i autorizuar të veprojë në emër të tij;

b) për personat juridikë publikë: emri, adresa e selisë, numri i regjistrimit (NIPT) dhe të dhënat e personit të kontaktit që është i autorizuar të veprojë në emër të tij.

2. Ndryshimet në të dhënat e pikave të kontaktit i komunikohen Autoritetit nga operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit brenda 7 ditëve kalendarike.

3. Autoriteti mban regjistrin elektronik të pikave të kontaktit me të dhënat e përcaktuara në pikën 1 të këtij neni.

4. Subjektet përgjegjëse, të përcaktuara në nenin 7, të këtij ligji, janë të detyruara të njoftojnë të dhënat e kontaktit brenda 3 muajve nga data e miratimit të këtij ligji.

KREU IV

GJENDJA E KRIZËS KIBERNETIKE

Neni 19

Kriza kibernetike

1. Gjendja e krizës kibernetike është situata, gjatë së cilës siguria e informacionit në sistemet e informacionit ose siguria e rrjeteve të komunikimeve elektronike është seriozisht e rrezikuar, duke vënë në rrezik interesin publik të Republikës së Shqipërisë.

2. Gjendja e krizës kibernetike shpallet me vendim të Këshillit të Ministrave, me propozimin e ministrit përgjegjës, të shoqëruar me relacionin përkatës. Urdhri për shpalljen e gjendjes së krizës kibernetike njoftohet në media.

3. Gjendja e krizës kibernetike shpallet për një periudhë kohore deri në shtatë ditë. Periudha e dhënë mund të zgjatet në mënyrë të përsëritur vetëm pas miratimit të Kryeministrit. Periudha maksimale e shpalljes së gjendjes së krizës kibernetike nuk duhet të kalojë 30 ditë.

4. Gjatë periudhës së gjendjes së krizës kibernetike, ministri përgjegjës informon Kryeministrin në lidhje me zgjidhjen e kësaj gjendjeje, si dhe për kërcënimet reale që çuan në shpalljen e kësaj gjendjeje. Gjatë gjendjes së krizës kibernetike Autoriteti ka të drejtë të nxjerrë vendim ose të marrë masa mbrojtëse të natyrës së përgjithshme dhe kundërmasa.

5. Kur është e pamundur të shmanget një kërcënim ndaj sigurisë së informacionit në sistemet e informacionit ose sigurisë së shërbimeve ose sigurisë dhe integritetit të rrjeteve të komunikimit elektronik, ministri përgjegjës i propozon menjëherë Kryeministrit vendosjen e gjendjes së krizës kibernetike. Kundërmasat e nxjerra nga Autoriteti para vendosjes së gjendjes së krizës kibernetike mbeten në fuqi për aq kohë sa këto kundërmasa nuk bien në kundërshtim me masat emergjente të deklaruara nga Këshilli i Ministrave.

6. Autoriteti koordinon veprimet e të gjitha strukturave përgjegjëse për zgjidhjen e gjendjes së krizës kibernetike.

KAPITULLI V

KUNDËRVAJTJET ADMINISTRATIVE

Neni 20

Masat korrigjuese

1. Kur Autoriteti konstaton mangësi në zbatimin e masave të sigurisë, të nxjerra në zbatim të këtij ligji, ai cakton personin përgjegjës për të korrigjuar mangësitë e konstatuara dhe, sipas rastit, cakton masat e nevojshme për t’i eliminuar këto mangësi.

2. Kostot lidhur me zbatimin e masave korrigjuese mbulohen nga operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit.

3. Autoriteti përcakton një afat të arsyeshëm, brenda të cilit operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit duhet të marrin masat korrigjuese.

4. Operatorët janë të detyruar të njoftojnë për marrjen e masave korrigjuese brenda afatit të përcaktuar dhe, nëse është e nevojshme, të paraqesin edhe provat që vërtetojnë këtë fakt.

Neni 21

Kundërvajtjet administrative

1. Në kuptim të këtij ligji, përbëjnë kundërvajtje administrative shkeljet e mëposhtme:

a) mosraportimi i incidenteve kibernetike, në zbatim të pikës 1, të nenit 11, të këtij ligji;

b) mospërmbushja e detyrimeve të caktuara nga Autoriteti, në zbatim të pikës 1, të nenit 13, të këtij ligji;

c) mosraportimi pranë Autoritetit i pikës së kontaktit apo i përditësimeve të tyre, në zbatim të pikës 4, të nenit 18, të këtij ligji;

ç) mospërmbushja e detyrimeve të përcaktuara në kuadër të masave korrigjuese, në zbatim të nenit 20 të këtij ligji.

2. Të ardhurat e siguruara nga kundërvajtjet administrative derdhen 100 për qind në Buxhetin e Shtetit.

Neni 22

Sanksionet administrative

Kur Autoriteti konstaton shkeljen e dispozitave, të cilat përbëjnë kundërvajtje administrative, sipas nenit 21, të këtij ligji, vendos dënimin me gjobë si më poshtë:

a) nga 200 000 deri në 800 000 lekë, në rast të shkeljeve administrative të përcaktuara në shkronjat “a” dhe “ç” të pikës 1;

b) nga 20 000 deri në 40 000 lekë, në rast të shkeljeve administrative të përcaktuara në shkronjën “c” të pikës 1;

c) nga 40 000 lekë deri në 200 000 lekë, në rast të shkeljeve administrative të përcaktuara në shkronjën “b” të pikës 1.

Neni 23

Procedura

Procedurat e konstatimit, shqyrtimit, ankimit dhe ekzekutimit të kundërvajtjeve administrative janë ato të parashikuara në ligjin për kundërvajtjet administrative.

Neni 24

Aktet nënligjore

1. Ngarkohet Këshilli i Ministrave të nxjerrë aktet nënligjore në zbatim të pikës 2, të nenit 6, të këtij ligji, brenda 12 muajve nga hyrja në fuqi e këtij ligji.

2. Ngarkohet Autoriteti të nxjerrë rregulloret përkatëse, në zbatim të neneve 9, pika 4; 11, pika 2; 16, pika 3; 17, pika 4, të këtij ligji, brenda 12 muajve nga hyrja në fuqi e këtij ligji.

3. Ngarkohet ministri përgjegjës të nxjerrë akte nënligjore në zbatim të pikës 3, të nenit 7, dhe të pikës 3, të nenit 13, të këtij ligji, brenda 12 muajve nga hyrja në fuqi e këtij ligji.

Neni 25

Dispozitat kalimtare

1. Për nëpunësit civilë ekzistues të Agjencisë Kombëtare për Sigurinë Kompjuterike zbatohen dispozitat e legjislacionit të nëpunësit civil në rastin e mbylljes dhe ristrukturimit të institucionit.

2. Agjencia Kombëtare për Sigurinë Kompjuterike, krijuar me vendimin nr. 766, datë 14.9.2011, të Këshillit të Ministrave, “Për krijimin e Agjencisë Kombëtare për Sigurinë

Kompjuterike”, të ndryshuar, do të vazhdojë të kryejë veprimtarinë e saj deri në momentin e fillimit të funksionimit të Autoritetit, sipas këtij ligji.

3. Mjetet, burimet e të ardhurave, arkivat, detyrimet dhe kompetencat e Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT) transferohen tek Autoriteti, sipas këtij ligji.

4. Buxhetet e miratuara për Agjencinë Kombëtare për Sigurinë Kompjuterike dhe Autoritetin Kombëtar për Certifikimin Elektronik, sipas ligjit vjetor të buxhetit, do të bashkohen, duke përbërë buxhetin e miratuar të autoritetit përgjegjës.

Neni 26

Hyrja në fuqi

Ky ligj hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare.

K R Y E T A R I

Ilir META

Miratuar në datën 26.1.2017