VENDIM
Nr. 792, datë 28.12.2023

PËR MIRATIMIN E RREGULLORES "PËR PËRCAKTIMIN E RREGULLAVE DHE TË PROCEDURAVE PËR SIGURINË E INFORMACIONIT TË KLASIFIKUAR, QË TRAJTOHET NË SISTEMET E KOMUNIKIMIT DHE INFORMACIONIT (SKI)"[1]

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 3, të nenit 49, të ligjit nr. 10/2023, "Për informacionin e klasifikuar", me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e rregullores "Për përcaktimin e rregullave dhe të procedurave për sigurinë e informacionit të klasifikuar, që trajtohet në sistemet e komunikimit dhe informacionit (SKI)", sipas tekstit që i bashkëlidhet këtij vendimi.
2. Ministritë, institucionet shtetërore dhe operatorët ekonomikë nxjerrin udhëzimet përkatëse për zbatimin e këtij vendimi brenda 90 (nëntëdhjetë) ditëve nga hyrja në fuqi e këtij vendimi.
3. Vendimi nr. 542, datë 25.7.2019, i Këshillit të Ministrave, "Për miratimin e rregullores 'Për sigurimin e informacionit të klasifikuar që trajtohet në sistemet e komunikimit dhe të informacionit (SKI)'", shfuqizohet.
4. Ngarkohen ministritë, institucionet shtetërore dhe operatorët ekonomikë për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

RREGULLORE
PËR PËRCAKTIMIN E RREGULLAVE DHE TË PROCEDURAVE PËR SIGURINË E INFORMACIONIT TË KLASIFIKUAR, QË TRAJTOHET NË SISTEMET E KOMUNIKIMIT DHE INFORMACIONIT (SKI)"

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti

Objekti i kësaj rregulloreje është:
1. përcaktimi i detyrave dhe i përgjegjësive për sigurinë e informacionit të klasifikuar, që trajtohet në sistemet e komunikimit dhe informacionit.
2. përcaktimi i kërkesave minimale, që duhet të zbatohen për sigurinë e sistemeve të komunikimit dhe informacionit.

---

[1]Ky vendim është përafruar pjesërisht me:
vendimin e Këshillit, datë 23 shtator 2013, "Mbi rregullat e sigurisë për mbrojtjen e informacionit të klasifikuar të BE-së" (2013/488/BE), nr. CELEX 32013D0488, Fletore Zyrtare e Bashkimit Evropian, seria L, nr. 274, datë 15.10.2013, faqe 1–50.

3. përcaktimi i rregullave për vlerësimin dhe akreditimin e sigurisë së sistemeve të komunikimit dhe informacionit.

Neni 2
Qëllimi

Qëllimi i kësaj rregulloreje është garantimi i sigurisë së informacionit të klasifikuar, që prodhohet, ruhet, transmetohet, trajtohet në sistemet e komunikimit dhe informacionit.

Neni 3
Fusha e veprimit

1. Kjo rregullore zbatohet për sistemet e komunikimit dhe informacionit (në vijim, SKI), që trajtojnë ose që do të trajtojnë informacion të klasifikuar "Sekret shtetëror", të NATO-s, BE-së, shteteve dhe organizatave të huaja me të cilat Republika e Shqipërisë ka marrëveshje sigurie.
2. Dispozitat e kësaj rregulloreje zbatohen nga të gjitha subjektet publike dhe private apo strukturat, të cilat kanë përgjegjësi në planifikimin, krijimin, prokurimin, zhvillimin, administrimin dhe përdorimin e SKI-ve.

Neni 4
Përkufizime

Në këtë rregullore, termat e mëposhtëm kanë këto kuptime:
1. "Akt vlerësimi", dokumenti ku përshkruhet gjendja e sigurisë së sistemit dhe pranimi ose refuzimi i riskut të mbetur.
2. "Aset", çdo gjë me vlerë, si pajisje e teknologjisë së informacionit dhe komunikimit, komponent *software* dhe informacioni.
3. "Autenticiteti", aftësia për të provuar se informacioni është i vërtetë dhe nga burime të sigurta.
4. "Autorizim kripto", dokumenti që autorizon një individ për të aksesuar ose menaxhuar materialet kriptografike.
5. "Deklarata e Kërkesave të Sigurisë së Sistemit (DKSS)", dokumenti që përshkruan masat e sigurisë së SKI-ve.
6. "Disponueshmëria", aftësia e aseteve për të qenë të arritshme dhe të përdorshme kur nevojiten.
7. "Dobësitë", mangësi në fortësinë, plotësinë ose konsistencën e kontrolleve dhe mund të jenë të natyrës teknike, procedurale ose operacionale.
8. "Emetim elektromagnetik kompromet ues", rrezatimi elektromagnetik i pakontrolluar që mundëson ekspozimin e paautorizuar të informacionit të klasifikuar.
9. "Entitet", në kuptim të kësaj rregulloreje, përfshin individë, pajisje ose shërbime.
10. "Incident sigurie", çdo ngjarje që rezulton ose mund të rezultojë në padisponueshmëri të sistemit ose të komponentëve të tij kryesorë, zbulim të informacionit të klasifikuar, humbje ose ndryshim të padëshiruar të informacionit, shkatërrim ose humbje të pajisjeve apo të aseteve.
11. "Integriteti", aftësia për të ruajtur saktësinë dhe plotësinë e aseteve.
12. "Kërcënimet", mundësi për kompromet imin e qëllimshëm ose jo të sigurisë. Në rastin e sigurisë së sistemeve, kompromet imet e tilla përfshijnë humbjen e një ose më shumë objektivave të sigurisë së SKI-ve.

13. "Dokumenti i konceptit të operimit (DKO)", dokumenti që përshkruan misionin, mjedisin operacional, mjedisin e mirëmbajtjes, funksionet dhe karakteristikat e sistemit brenda mjedisit të përgjithshëm operacional.

14. "Konfidencialiteti", aftësia për të provuar që informacioni nuk është i ekspozuar për entitete të paautorizuara.

15. "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.

16. "Metodë e kombinuar autentifikimi", mënyrë autentifikimi e përbërë nga dy ose më shumë elemente sigurie.

17. "Mjedis i sigurt global i sistemit (MSG)", rrethina e objektit ku është instaluar dhe operon sistemi.

18. "Mjedis i sigurt lokal i sistemit (MSL)", objekti ku është instaluar dhe operon sistemi.

19. "Mjedis i sigurt elektronik i sistemit (MSE)", pajisjet, shërbimet, aplikacionet që përbëjnë një SKI.

20. "Ndërlidhje e sistemeve", lidhja e drejtpërdrejtë e dy ose më shumë SKI-ve, me qëllim shkëmbimin e të dhënave ose të shërbimeve.

21. "Pamohueshmëria", aftësia për të provuar që një veprim ose ngjarje ka ndodhur, në mënyrë që ngjarja ose veprimi nuk mund të mohohen më vonë.

22. "Pajisje e lëvizshme", në kuptim të kësaj rregulloreje, përfshin telefonat *mobile*, laptop, tableta dhe pajisje të tjera të lidhura me internetin.

23. "Plani i Akreditimit të Sigurisë së Sistemit (PASS)", dokumenti që prodhohet nga AKAS-i, në bashkëpunim me autoritetet e sigurisë, në të cilin jepet informacion për sistemin që kërkohet të akreditohet, autoritetet e përfshira në procesin e akreditimit të sigurisë, aktivitetet që do të kryhen, përfshirë afatet kohore, si dhe dokumentet që do të prodhohen.

24. "Plani i menaxhimit të materialeve kriptografike", dokumenti ku përcaktohen metodat, mjetet, procedurat, si dhe rolet e përgjegjësitë për gjenerimin, vendosjen, regjistrimin, shpërndarjen, transportin, ruajtjen, arkivimin, revokimin, mbajtjen në llogari, rinovimin, rikuperimin, shkatërrimin dhe raportimin e kompromet imit të materialeve kriptografike.

25. "Plani i vlerësimit dhe testimit të sigurisë së komponentëve të sistemit (PVTSKS)" është dokumenti që përcakton komponentët e sistemit që janë subjekt i testimit dhe vlerësimit, si dhe metodat, mjetet, aktivitetet, rolet dhe përgjegjësitë për testimin dhe vlerësimin e sistemit.

26. "Plani i menaxhimit të riskut (PMR)", dokumenti ku përcaktohen risqet e sigurisë dhe procesi i menaxhimit të tyre.

27. "Plani i përgjigjes ndaj incidenteve", dokumenti ku detajohen procedurat në përgjigje të incidenteve të sigurisë kompjuterike. Ky dokument ka për qëllim ruajtjen e të dhënave që lidhen me incidentet dhe parandalimin e përshkallëzimit të tyre.

28. "Dokumenti i Procedurave të Operimit të Sigurt (DPOS)" është dokumenti ku përcaktohen procedurat për kryerjen e detyrave që lidhen me sigurinë e sistemit, si dhe rolet dhe përgjegjësitë e personelit.

29. "Dokumenti i procedurave në rastet e emergjencave" është dokumenti ku detajohen procedurat për evakuimin ose shkatërrimin e pjesëve të sistemit të ekspozuara ndaj riskut në rastet e gjendjes së luftës, gjendjes së jashtëzakonshme, krizave kibernetike, fatkeqësive natyrore dhe emergjencave të tjera civile gjatë të cilave ky informacion mund të përvetësohet, dëmtohet, kompromet ohet, shkatërrohet etj.

30. "Siguria e sistemeve të komunikimit dhe informacionit" është aplikimi i masave të sigurisë për mbrojtjen e informacionit dhe SKI-ve, sipas objektivave të sigurisë.

31. "Siguria e informacionit" përfshin përcaktimin dhe zbatimin e masave për mbrojtjen e informacionit të klasifikuar që trajtohet në SKI nga humbja aksidentale apo e qëllimshme e konfidencialitetit, integritetit dhe disponueshmërisë, dhe masat për parandalimin, humbjen e integritetit dhe disponueshmërisë së këtyre sistemeve.

32. "Sisteme të parandalimit të ndërhyrjeve *host-based*", aplikacione/platforma të instaluara me qëllim monitorimin, analizimin dhe ndalimin e aktiviteteve të dyshimta, që ndodhin në pajisjen ku ato instalohen.

33. "Skema e shtrirjes së SKI-ve në Zonat e Sigurisë", dokumenti që paraqet skicën e mjediseve të institucionit, ku pasqyrohet shtrirja e të gjithë komponentëve të lidhur në sistem dhe zonat e sigurisë përkatëse.

34. "TEMPEST", studimi dhe kontrolli i emetimeve elektromagnetike kompromet uese, fenomenit në vetvete dhe masave për mënjanimin e tyre.

35. "Raporti i testimit dhe vlerësimit", dokumenti ku paraqiten rezultatet e përftuara nga testimi dhe vlerësimi i komponentëve të sistemit.

36. "Risk", mundësia që një dobësi të shfrytëzohet me sukses nga një kërcënim, duke çuar në cenimin e objektivave të sigurisë.

37. "Risku i mbetur", risku që mbetet pas implementimit të masave të sigurisë në SKI, duke marrë parasysh që jo të gjitha kërcënimet dhe dobësitë mund të eliminohen apo të reduktohen.

38. "Vlerësimi i sistemit të komunikimit dhe informacionit", procesi i vlerësimit, testimit dhe ekzaminimit të masave/kontrolleve të sigurisë së sistemit, në bazë të standardeve specifike të sigurisë, si dhe identifikimi i dobësive të sistemit dhe përpilimi i planit të masave minimizuese të këtyre dobësive.

39. "Veprim i privilegjuar" përfshin, por pa u kufizuar në ndryshimin e konfigurimeve të sistemit, ndryshimin e parametrave të sistemit, aksesin në *log*-et e auditimit dhe sigurisë, aksesin në të dhëna, skedar dhe llogari që përdoren nga përdoruesit e tjerë, përfshirë *back-up*-et dhe mediat elektronike.

Neni 5

Objektivat e sigurisë

1. Objektivat e sigurisë janë:

a) konfidencialiteti;

b) integriteti;

c) disponueshmëria;

ç) autenticiteti;

d) pamohueshmëria.

2. Niveli i aplikimit të objektivave është specifik për SKI të ndryshme dhe përcaktohet nga misioni i sistemit, kërkesat minimale të sigurisë dhe rezultatet e procesit të menaxhimit të riskut.

Neni 6

Kriteret themelore të sigurisë

1. SKI-të ndjekin këto kritere sigurie:

a) Menaxhimi i riskut të sigurisë: aplikimi i procesit të menaxhimit të riskut për monitorimin, reduktimin, eliminimin, shmangien ose pranimin e riskut të mbetur që lidhet me sigurinë e SKI-ve;

b) Siguria gjatë të gjithë jetëgjatësisë së SKI-ve: garantimi i masave të sigurisë së SKI-ve nga vënia në funksionim dhe deri në heqjen nga shërbimi;

c) Funksionalitetet dhe privilegjet minimale: instalimi dhe përdorimi vetëm i funksioneve, protokolleve dhe shërbimeve që kërkohen për të përmbushur misionin operacional të sistemit. Entitetit që përdor SKI-në i lejohen vetëm privilegjet dhe autorizimet që nevojiten për kryerjen e detyrave;

ç) Nyja vetëmbrojtëse: secili SKI i ndërlidhur të trajtojë SKI-në tjetër si të huaj dhe të implementohen masa për kontrollin e shkëmbimit të informacionit me SKI tjetër;

d) Mbrojtja shumënivelëshe: masat e sigurisë së SKI-ve të implementohen në mënyrë të tillë që të ketë më shumë se një nivel mbrojtjeje;

dh) Përditësimi i masave të sigurisë: Rishikim i implementimit dhe efektivitetit të masave të sigurisë së SKI-ve në varësi të ndryshimeve në mjedisin e kërcënimeve dhe dobësive;

e) Akreditimi i SKI-ve: akreditimi i SKI-ve përshtatshmërish me nivelin e informacionit që trajtohet në to.

2. AKAS-i verifikon aplikimin e këtyre kritereve dhe implementimin e vazhdueshëm të standardeve të sigurisë.

PJESA I
QEVERISJA E SIGURISË SË INFORMACIONIT

KREU I
ROLET DHE PËRGJEGJËSITË PËR SIGURINË E SKI-ve

Neni 7
Rolet dhe përgjegjësitë

1. Autoriteti i Operimit të Sistemit (AOS) janë institucionet shtetërore përcaktuar si autoritet klasifikues në kuptim të ligjit për informacionin e klasifikuar, përgjegjëse për planifikimin, përcaktimin e nevojës për SKI dhe përdorimin e SKI-ve.

2. Operatorët ekonomikë, gjatë realizimit të kontratave që përmbajnë informacion të klasifikuar, kur autorizohen për përdorimin e SKI-ve të tyre nga autoriteti kontraktor kanë të njëjtat detyrime e përgjegjësi si Autoriteti i Operimit të Sistemit dhe Administratorit të SKI-ve.

3. Institucionet shtetërore dhe operatorët ekonomikë caktojnë oficerin ose strukturën e sigurisë së SKI-ve, përgjegjës për mbikëqyrjen e aspekteve të sigurisë së SKI-ve, përcaktuar në këtë rregullore.

4. Roli i administratorit të SKI-ve në institucionet apo organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, kryhet sipas ligjit nr. 43/2023, "Për qeverisjen elektronike".

5. Institucionet shtetërore që nuk përfshihen në pikën 4, të këtij neni, ndajnë rolet dhe përgjegjësitë e AOS-it dhe të Administratorit të SKI-ve bazuar në strukturën organizative të institucionit.

6. Subjektet e përcaktuara në këtë nen kryejnë detyrat e përcaktuara në këtë rregullore.

Neni 8
Detyrat e Autoritetit të Operimit të Sistemit AOS

AOS-i ka këto detyra:

a) Përcakton kërkesat funksionale të SKI-ve;

b) Përcakton mënyrën e sigurisë së operimit të sistemit;

c) Kërkon akreditimin e SKI-ve mbështetur në përcaktimet e kësaj rregulloreje;

ç) Miraton dokumentacionin e sigurisë së sistemit;

d) Miraton kërkesat operacionale dhe funksionale të ndërlidhjes së sistemeve;

dh) Pranon riskun e mbetur, që rezulton nga procesi i menaxhimit të riskut të sigurisë;

e) Cakton ose emëron Oficerin e Sigurisë së SKI-ve;

ë) Njofton AKAS-in për ndryshimet në sistem që në fazën e planifikimit të tyre;

f) Dërgon tek AKAS-i kërkesën për riakreditimin e sistemit 4 muaj para afatit të përfundimit të vlefshmërisë së akreditimit.

Neni 9

Detyrat e Oficerit të Sigurisë së SKI-ve

Oficeri i Sigurisë së SKI-ve ka këto detyra:

a) Siguron që të gjitha SKI-të në përdorim, si dhe projektet e SKI-ve që mbështesin misionin dhe detyrat e institucionit janë në përputhje me përcaktimet e kësaj rregulloreje;

b) Harton konceptin e operimit të SKI-ve, në bashkëpunim me administratorin e SKI-ve;

c) Harton procedurat e operimit të sigurt për SKI në përdorim dhe siguron njohjen e tyre nga përdoruesit e sistemit;

ç) Këshillon për sigurinë e SKI-ve dhe trajnon administratorët dhe përdoruesit e sistemit, përfshirë nivelet drejtuese, për aspektet e sigurisë së SKI-ve bazuar në programet e edukimit të personelit;

d) Harton planin e menaxhimit të riskut në bashkëpunim me Administratorin e SKI-ve;

dh) Harton planin e përgjigjes ndaj incidenteve dhe procedurat në rastet e emergjencave në bashkëpunim me Administratorin e SKI-ve;

e) Mbikëqyr ekzekutimin e vlerësimeve periodike të sigurisë së SKI-ve (p.sh.: vlerësim risku, testim dhe vlerësim i sigurisë, inspektim i sigurisë, vlerësim i dobësive, auditim);

ë) Raporton te titullari i AOS-it për mangësitë dhe dobësitë e konstatuara, që lidhen me sigurinë e SKI;

f) Në bashkëpunim me Administratorin e SKI-ve, raporton tek AKAS-i për incidentet dhe masat e marra;

g) Menaxhon materialin kriptografik që ka në përdorim, në përputhje me këtë rregullore;

gj) Mirëmban inventarin e pajisjeve, komponentëve, produkteve dhe aplikacioneve të SKI-ve;

h) Harton procedura të detajuara për pastrimin dhe shkatërrimin e komponentëve memorizues të pajisjeve TIK;

i) Harton skemën e kontrollit të aksesit, ku përcaktohen atributet e çdo entiteti që ka qasje në SKI apo në informacionin e klasifikuar që trajtohet në të, bazuar në parimin "nevojë për njohje", si dhe duke autorizuar e lejuar privilegjet që nevojiten për kryerjen e detyrave.

Neni 10

Detyrat e Administratorit të SKI-ve

Administratori i SKI-ve ka këto detyra:

a) Dërgon për miratim tek AOS projektet, ndryshimet teknike të SKI-ve, pas paraqitjes së kërkesës;

b) Implementon teknikisht skemën e shtrirjes së SKI-ve në zonat e sigurisë në bashkëpunim me Oficerin e Sigurisë së SKI-ve;

c) Përgjigjet për mbarëvajtjen e SKI-ve;

ç) Merr pjesë në procesin e menaxhimit të riskut;

d) Raporton tek Oficeri i Sigurisë së SKI-ve për mangësitë dhe dobësitë e konstatuara që lidhen me sigurinë e SKI-ve;

dh) Përgjigjet për anën teknike të Deklaratës së Kërkesave të Sigurisë së Sistemit, Procedurat e Testimit dhe Vlerësimit të Sigurisë (PVTS).

Neni 11

Autoriteti Kombëtar i Akreditimit të Sigurisë (AKAS)

Autoriteti Kombëtar i Akreditimit të Sigurisë ka këto detyra:

a) Shqyrton kërkesat për akreditimin e sistemeve;

b) Bashkëpunon dhe koordinon punën me autoritetet e sigurisë së SKI-ve për akreditimin e sigurisë së SKI;

c) Harton e miraton Planin e Akreditimit të Sigurisë së Sistemit (PASS);

ç) Verifikon zbatimin e masave të sigurisë për mbrojtjen e informacionit të klasifikuar gjatë përpunimit, ruajtjes ose transmetimit në sistemet e komunikimit dhe të informacionit nga cenimi aksidental ose i qëllimshëm i objektivave të sigurisë:

i. Verifikon zonat e sigurisë ku është instaluar dhe operon sistemi;

ii. Verifikon nëse përdoruesit e sistemit janë të pajisur me certifikata sigurie;

iii. Verifikon nëse aplikohen aspekte të sigurimit industrial;

iv. Verifikon nëse aplikohen marrëveshje sigurie me struktura të tjera brenda apo jashtë vendit;

v. Verifikon dokumentacionin e sigurisë së sistemit;

vi. Verifikon zbatimin e kërkesave të sigurisë së komunikimeve, sigurisë kriptografike dhe sigurisë së emetimeve, nëse aplikohen, në bashkëpunim me autoritetet e sigurisë;

vii. Inspekton MSG dhe MSL;

viii. Verifikon nëse masat e sigurisë së sistemit janë në përputhje me Planin e Menaxhimit të Riskut;

d) Analizon dhe vlerëson gjendjen e sigurisë së sistemit në varësi të dokumentacionit të sigurisë së sistemit, dokumenteve të lëshuara nga autoritetet e sigurisë dhe rezultateve të inspektimeve;

dh) Pranon riskun e mbetur të sistemit dhe harton aktvlerësimin për zbatimin e masave të sigurisë;

e) Lëshon deklaratën e akreditimit, që autorizon sistemin për të trajtuar informacion të klasifikuar; Kjo deklaratë lëshohet bazuar në vlerësimin pozitiv të sigurisë së SKI;

ë) Menaxhon databazën e sistemeve të klasifikuara kombëtare, të NATO-s, të shteteve dhe të organizatave të huaja të akredituara nga AKAS-i.

Neni 12

Autoriteti Kombëtar i Testimit dhe Vlerësimit të Sigurisë (AKTVS)

Autoriteti Kombëtar i Testimit dhe Vlerësimit të Sigurisë ka këto detyra:

a) Përcakton komponentët specifikë të sistemit që duhet të testohen dhe të vlerësohen, masat e sigurisë dhe pritshmëritë për secilin element;

b) Përzgjedh, përgatit dhe miraton procedurat, metodat dhe mjetet e testimit dhe vlerësimit të komponentëve specifikë të sistemit;

c) Përcakton rregullat për auditimin e implementimit të kërkesave të sigurisë në sistem dhe vlerësimin e operimit korrekt të masave të sigurisë të implementuara në sistem;

ç) Vlerëson nivelin e përputhshmërisë së dokumentacionit të sistemit dhe zbatimit në praktikë të masave të deklaruara në dokumentacion për MSE;

d) Në bashkëpunim me AOS-in, Administratorin e SKI-ve teston dhe vlerëson dobësitë e SKI-ve;

dh) Kontribuon në vlerësimin e riskut të sigurisë së sistemit;

e) Kryen dokumentimin e saktë të procedurave dhe rezultateve të testimit dhe gjeneron raportin e vlerësimit të sigurisë;

ë) Mbikëqyr AOS-in, Administratorin e SKI-ve në zbatimin e udhëzimeve për realizimin e auditimit të sigurisë;

f) Menaxhon databazën e sistemeve të testuara dhe vlerësuara nga AKAS-i.

Neni 13

Autoriteti Kombëtar i Sigurisë së Komunikimeve (AKSK)

Autoriteti Kombëtar i Sigurisë së Komunikimeve ka këto detyra:

a) Përcakton kërkesat e sigurisë specifike për sistemet, produktet dhe mekanizmat kriptografikë dhe kontrollon zbatimin e tyre nga institucionet shtetërore;

b) Përcakton procedurat për përzgjedhjen, operimin dhe mirëmbajtjen e sistemeve, produkteve dhe mekanizmave kriptografikë dhe kontrollon zbatimin e tyre nga institucionet shtetërore;

c) Administron infrastrukturën e materialit kriptografik të pajisjeve/sistemeve të përzgjedhura;

ç) Vlerëson sistemet, produktet dhe mekanizmat kriptografikë dhe harton aktvlerësimin përkatës dhe ia përcjell AKAS-it në funksion të procesit të akreditimit të sigurisë;

d) Inspekton strukturat kriptografike në institucionet shtetërore për masat për zbatimin e mbrojtjes kriptografike të informacionit të klasifikuar, instalimin, ruajtjen dhe mirëmbajtjen e pajisjeve, sistemeve dhe incidentet kriptografike;

dh) Menaxhon databazën e sistemeve, produkteve dhe mekanizmave kriptografikë të vlerësuar dhe që përdoren nga institucionet shtetërore.

Neni 14

Autoriteti Kombëtar i Shpërndarjes Kriptografike (AKSHK)

Autoriteti Kombëtar i Shpërndarjes Kriptografike ka këto detyra:

a) Administron materialet kriptografike që përdoren për mbrojtjen e informacionit të klasifikuar;

b) Mban databazën e pajisjeve dhe programeve kriptografike, materialit çelës, dokumenteve e procedurave përkatëse për menaxhimin e tyre;

c) Shpërndan materialin kriptografik në institucionet shtetërore;

ç) Administron sistemet e shkëmbimit elektronik të çelësave kriptografikë dhe të llogarisë së materialit kriptografik kombëtar, të NATO-s, BE-së, shteteve dhe organizatave të tjera ndërkombëtare;

d) Zbaton rregullat e sigurimit fizik dhe elektronik, sipas akteve nënligjore në fuqi për ruajtjen e materialit kriptografik;

dh) Siguron që materiali kriptografik të jetë në çdo kohë në kushte pune;

e) Shkatërron materialin kriptografik, sipas rregullores kur është e nevojshme;

ë) Harton procedurat që duhen ndjekur për raportimin e incidenteve;

f) Harton procedurat që duhen ndjekur në rastet e emergjencës;

g) Siguron që i gjithë personeli që ka akses në materialin kriptografik është i autorizuar, i certifikuar dhe i trajnuar, sipas akteve nënligjore në fuqi.

Neni 15

Autoriteti Kombëtar TEMPEST (AKT)

Autoriteti Kombëtar TEMPEST ka këto detyra:

a) Harton politika, standarde e procedura për mbrojtjen nga emetimet elektromagnetike komprometuese;

b) Përzgjedh, siguron dhe administron pajisjet elektronike për realizimin e matjeve TEMPEST të ambienteve dhe pajisjeve;

c) Kryen periodikisht matjet TEMPEST dhe përgatit raportin me rezultatet e matjeve për AKAS dhe institucionet përkatëse;

ç) Kontrollon dhe rekomandon masat që duhen zbatuar për të mënjanuar riskun nga emetimet elektromagnetike komprometuese;

d) Mban databazën me historikun e rezultateve të matjeve TEMPEST.

KREU II
MENAXHIMI I RISKUT TË SIGURISË SË INFORMACIONIT

Neni 16
Procesi i menaxhimit të riskut

1. Procesi i menaxhimit të riskut të sigurisë kryhet për monitorimin, reduktimin, eliminimin, shmangien ose pranimin e risqeve që lidhen me SKI.

2. Procesi i menaxhimit të riskut përfshin:

a) identifikimin dhe vlerësimin e aseteve;

b) identifikimin e agjentëve kërcënues (person, proces kompjuterik, pajisje etj.);

c) identifikimin e kërcënimeve që vijnë si pasojë e veprimit të agjentëve;

ç) identifikimin e dobësive që mund të shfrytëzohen nga agjentët kërcënues;

d) identifikimin e riskut;

dh) vlerësimin e masave ekzistuese të sigurisë;

e) vlerësimin e riskut ose përcaktimin e nivelit të riskut;

ë) identifikimin e masave përkatëse për monitorimin, reduktimin, eliminimin, shmangien ose pranimin e riskut;

f) përcaktimin e riskut të mbetur;

g) dokumentimin e riskut të sigurisë, si dhe procesin e menaxhimit të tij në planin e menaxhimit të riskut.

Neni 17
Risku i mbetur

1. Risku i sigurisë, që konsiderohet si i pranueshëm, miratohet nga AKAS gjatë procesit të akreditimit të sigurisë së SKI-ve dhe mbahet nën monitorim të vazhdueshëm nga Autoriteti i Operimit të Sistemit dhe Administratori i SKI.

2. Risku i sigurisë që konsiderohet si i papranueshëm duhet të trajtohet nëpërmjet aplikimit të masave shtesë ose masave alternative të sigurisë.

KREU III
DOKUMENTACIONI I SIGURISË SË SISTEMIT

Neni 18
Dokumentacioni i sigurisë së sistemit

1. Dokumentacioni i sigurisë së sistemit është tërësia e dokumenteve që kërkohen për akreditimin e sigurisë së SKI-ve dhe shërben si standard për vlerësimin e tij.

2. Dokumentacioni i sigurisë së sistemit:

a) Dokumentacioni i sigurisë së sistemeve hartohet në përputhje me modelet e përcaktuara nga AKAS;

b) I vihet në dispozicion personelit që ka akses në sistem, në përputhje me nevojën për njohje;

c) Përditësohet rregullisht.

3. Dokumentacioni i sigurisë së sistemit përbëhet nga:

a) koncepti i operimit (KO);

b) deklarata e kërkesave të sigurisë së sistemit (DKSS);

c) procedurat e operimit të sigurt (POS);

ç) plani i menaxhimit të riskut (PMR);

d) procedurat e testimit dhe vlerësimit të sigurisë (PVTS);

dh) plani i përgjigjes ndaj incidenteve;

e) procedurat në rastet e emergjencave;

ë) urdhri për ndarjen e zonave të sigurisë;

f) skema e shtrirjes së SKI-ve në Zonat e Sigurisë;

g) procedura për pastrimin dhe/ose shkatërrimin e pajisjeve TIK.

4. Për rastet kur sistemi është i përbërë nga një kompjuter *stand alone* dhe pajisje periferike të lidhura me të (printer, skaner), dokumentet KO, DKSS dhe PMR lejohet të përmblidhen në një dokument të vetëm.

Neni 19
Kërkesa shtesë për dokumentacionin

1. AKAS-i ka të drejtë të kërkojë dokumente shtesë, në përputhje me politikën e sigurisë së NATO-s, BE-së, shteteve dhe organizatave të huaja me të cilat Republika e Shqipërisë ka marrëveshje sigurie, në varësi të SKI-ve.

2. Për sistemet e shteteve ose organizatave ndërkombëtare dokumentet plotësohen në 2 kopje, një në gjuhën angleze dhe një në gjuhën shqipe.

KREU IV
AKREDITIMI I SIGURISË SË SKI

Neni 20
Të përgjithshme

1. Sistemet që trajtojnë informacion të klasifikuar akreditohen në përputhje me kërkesat e përcaktuara në këtë rregullore.

2. Procesi i akreditimit të sigurisë përcakton nivelin e përshtatshëm të mbrojtjes së sistemit, si dhe identifikon e pranon riskun e mbetur, që duhet të monitorohet përgjatë jetëgjatësisë së sistemit.

3. AKAS mban, administron dhe përditëson të dhënat, ku pasqyrohen kërkesat për akreditim dhe statusi i akreditimit të SKI-ve kombëtare dhe shteteve apo organizatave ndërkombëtare.

Neni 21
Mjediset e sigurisë së sistemeve

1. Ndarja e mjediseve të sigurisë së sistemeve bëhet me qëllim përcaktimin e përgjegjësive për sigurinë e SKI-ve.

2. Mjediset e sigurisë së sistemeve janë:

a) Mjedisi i Sigurisë Globale (MSG) përfaqëson zonën e sigurisë, ku ndodhet sistemi, por që është jashtë kontrollit të AOS. MGS përfshin aspektet e sigurisë së ndërtesës, vendndodhjen gjeografike, sigurinë e ndërlidhjes së sistemeve dhe mjedisin e përgjithshëm të kërcënimeve;

b) Mjedisi i Sigurisë Lokale (MSL) është zona e sigurisë nën ndikimin e AOS. MLS përfshin masat e sigurimit fizik, sigurisë së personelit, sigurisë së informacionit dhe sigurisë procedurale;

c) Mjedisi i Sigurisë Elektronike (MSE) është zona e sigurisë që përfshin mekanizmat e sigurisë elektronike të SKI-ve të implementuar brenda arkitekturës së sigurisë së SKI-ve dhe që ofrojnë funksionet e nevojshme të sigurisë. MSE përfshin:

i. ndërfaqet individ–makinë;

ii. ndërfaqet e brendshme (ndërfaqet ndërmjet pjesëve të SKI-ve që përfaqësojnë klasa të ndryshme të sigurisë p.sh. particionet e sigurisë në sistem);

iii. ndërfaqet e jashtme (*firewall*, *gateway* etj.).

Neni 22
Mënyrat e sigurisë së operimit të sistemit

1. SKI-të që trajtojnë informacion të klasifikuar në nivel "konfidencial" e lart operojnë në një nga mënyrat e mëposhtme të sigurisë:

a) Mënyrë e dedikuar në të cilën të gjithë individët me të drejtë aksesi në SKI janë të certifikuar në nivelin më të lartë të klasifikimit që trajtohet në SKI dhe me nevojë të përbashkët për njohje për të gjithë informacionin që trajtohet në SKI;

b) Mënyrë e lartë në të cilën të gjithë individët me të drejtë aksesi në SKI janë të certifikuar në nivelin më të lartë të klasifikimit që trajtohet në SKI, por jo të gjithë individët kanë të njëjtën nevojë për njohje për informacionin që ruhet, përpunohet ose transmetohet në sistem. Miratimi për akses në informacionin që trajtohet në sistem jepet në nivel individual sipas funksionit që ka individi;

c) Mënyra me shumë nivele në të cilën jo të gjithë individët me të drejtë aksesi në SKI janë të certifikuar në nivelin më të lartë të klasifikimit që trajtohet në SKI dhe jo të gjithë individët me të drejtë aksesi në SKI kanë të njëjtën nevojë për njohje me informacionin që ruhet, përpunohet ose transmetohet në sistem.

2. SKI-të që trajtojnë informacion të klasifikuar në nivel "i kufizuar" operojnë në një nga mënyrat e mëposhtme të sigurisë:

a) Mënyrë e dedikuar, në të cilën të gjithë individët me të drejtë aksesi në SKI kanë të njëjtën nevojë për njohje për informacionin që trajtohet në SKI;

b) "Mënyra e lartë" është mënyra e operimit në të cilën jo të gjithë individët kanë të njëjtën nevojë për njohje për informacionin që trajtohet në SKI. Miratimi për akses në informacionin që trajtohet në SKI jepet në nivel individual, sipas funksionit që ka individi.

Neni 23
Bazat e akreditimit të sigurisë

Bazë për akreditimin e sigurisë së SKI-ve konsiderohet, si më poshtë vijon:

1. Vlerësimi i arkitekturës së sigurisë së sistemit;
2. Vlerësimi i dokumentacionit të sigurisë së sistemit;
3. Verifikimi i implementimit dhe efektivitetit të masave të sigurisë së SKI-ve;
4. Analiza e riskut të mbetur dhe proceseve për menaxhimin e vazhdueshëm të riskut të sigurisë;
5. Monitorimi i vazhdueshëm i statusit të sigurisë së SKI-ve.

Neni 24
Procesi i akreditimit të sigurisë

1. Procesi i akreditimit të sigurisë është tërësia e hapave që ndërmerren për të përcaktuar nëse masat e sigurisë së sistemit janë implementuar sipas kërkesave të kësaj rregulloreje. Procesi i akreditimit të sigurisë është mekanizmi që garanton sigurinë e SKI.

2. Procesi i akreditimit të sigurisë ndryshon në varësi të arkitekturës së SKI, në përputhje me këtë rregullore.

3. Procesi i akreditimit kalon në fazat si më poshtë:

a) fillimi i procesit;

b) verifikimi i sistemit;

c) miratimi;

ç) aktivitetet pas akreditimit.

Neni 25
Fillimi i procesit

1. Fillimi i procesit të akreditimit ka si objektiv njohjen me misionin e sistemit, përshkrimin e aspekteve funksionale dhe arkitekturën e sigurisë së sistemit, me qëllim përcaktimin e kërkesave për akreditimin e sistemit.

2. Kjo fazë përfshin këto aktivitete:

a) Iniciimi i kërkesës:

i. Kërkesa për akreditimin e sistemit drejtuar AKAS, duhet të përfshijë përshkrimin e sistemit sipas konceptit të operimit;

ii. Pas marrjes së kërkesës, AKAS-i e konsideron procesin e akreditimit të hapur dhe kërkon shpjegime të nevojshme ose korrigjime, nëse nevojitet;

iii. Në rastet e kërkesës për riakreditim dërgohet versioni i fundit i Konceptit të Operimit;

b) Negociimi:

i. Për çdo kërkesë akreditimi AKAS-i përcakton procesin e akreditimit në PASS;

ii. AOS-i raporton tek AKAS-i çdo lloj kushti shtesë (operacional, komercial ose strategjik), nëse ka, për t'u marrë në konsideratë nga AKAS-i për t'i dhënë prioritet akreditimit të këtij sistemi në fazat pasardhëse të procesit;

c) Implementimi dhe dokumentimi i masave të sigurisë:

i. pas miratimit të konceptit të operimit merren masa për përgatitjen e dokumentacionit të sigurisë së sistemit, si dhe identifikimin e përmbushjen e aktiviteteve për akreditimin e sistemit;

ii. dokumentacioni i sigurisë së sistemit, së bashku me dokumente të tjera shtesë për aspekte të sigurisë së informacionit, personelit, fizike dhe sigurimit industrial, dërgohet tek AKAS-i për miratim.

Neni 26
Verifikimi i sistemit

1. Verifikimi ka si objektiv rishikimin e dokumentacionit të sigurisë së sistemit dhe verifikimin e masave të sigurisë së sistemit, me qëllim konfirmimin e sigurisë së sistemit dhe identifikimin e kërkesave të sigurisë që nuk janë përmbushur dhe dobësitë e sistemit.

2. Verifikimi i masave të sigurisë së sistemit kryhet me një nga këto metoda:

a) testim;

b) ekzaminim;

c) intervistim.

3. Autoritetet e sigurisë kryejnë verifikimin e masave të sigurisë në përputhje me PASS dhe dokumentojnë rezultatet dhe riskun e mbetur në raportet përkatëse.

4. Sistemi dhe dokumentacioni përditësohen me rekomandimet e rezultateve të verifikimit.

Neni 27

Auditimi i sigurisë

1. Auditimi i sigurisë është një proces sistematik i rishikimit të sigurisë të implementuar në SKI, me qëllim identifikimin e dobësive dhe mundësive që çojnë në kompromet imin e objektivave të sigurisë. Proceset e auditimit kryhen si pjesë e procesit të vazhdueshëm të menaxhimit të riskut apo si pjesë e procesit të akreditimit të sigurisë së sistemit kur përcaktohet në PASS.

2. Të gjitha SKI-të ku trajtohet informacion i klasifikuar "Sekret shtetëror" janë subjekt i auditimit të sigurisë nën drejtimin dhe miratimin e AKAS-it.

3. Qëllimi dhe procesi i auditimit të sigurisë përcaktohet qartë dhe dokumentohet.

4. Proceset e auditimit të sigurisë kryhen në përputhje me udhëzimin e miratuar nga drejtori i përgjithshëm i AKAS-it.

Neni 28

Miratimi

1. Miratimi ka si objektiv autorizimin e sistemit për të operuar brenda kushteve të sigurisë.

2. AKAS-i vendos për:

a) lëshimin e Deklaratës së Akreditimit të Sigurisë për një periudhë të caktuar kohore për mjedisin e planifikuar operacional, në të cilin përmbushen të gjitha kërkesat e sigurisë. Deklarata e Akreditimit të Sigurisë përcakton kushtet nën të cilat është i vlefshëm akreditimi i sigurisë. Periudha e vlefshmërisë së akreditimit ndryshon në varësi të nivelit të klasifikimit, si më poshtë:

i. tepër sekret ose ekuivalent – 2 vjet;

ii. sekret ose ekuivalent – 3 vjet;

iii. konfidencial ose ekuivalent – 4 vjet;

iv. i kufizuar ose ekuivalent – 5 vjet;

b) lëshimin e Deklaratës së Përkohshme të Akreditimit të Sigurisë për një periudhë të caktuar kohore për mjedisin e planifikuar operacional, në të cilin nuk janë përmbushur të gjitha kërkesat e sigurisë. Deklarata e Përkohshme e Akreditimit të Sigurisë përcakton periudhën e vlefshmërisë, si dhe kushtet dhe aktivitetet që duhen kryer për të kaluar në Deklaratë të Akreditimit të Sigurisë;

c) lëshimin e Autorizimit për Operim të Kufizuar nëse procesi i akreditimit nuk ka mbaruar. Ky lloj autorizimi lëshohet vetëm në rrethana të jashtëzakonshme deri në gjashtë muaj, pa të drejtë shtyrjeje, kur kërkesat operacionale tejkalojnë kërkesat e sigurisë. Për këtë lloj autorizimi duhet më parë të miratohet koncepti i operimit;

ç) refuzimin e akreditimit të sigurisë duke treguar mangësitë specifike dhe masat korrigjuese. AKAS-i kërkon hartimin e planit të veprimit për marrjen e masave korrigjuese;

d) shfuqizimin e akreditimit ekzistues të sigurisë, duke treguar mangësitë specifike dhe masat korrigjuese. AKAS-i kërkon hartimin e planit të veprimit për marrjen e masave korrigjuese.

3. Akreditimi i sistemeve që trajtojnë informacion të klasifikuar të NATO-s, BE-së apo shteteve e organizatave të tjera ndërkombëtare bëhet në përputhje me marrëveshjet e sigurisë për mbrojtjen e ndërsjellë të informacionit të klasifikuar, si dhe duke aplikuar këtë rregullore në të gjitha aspektet e mundshme.

Neni 29
Aktivitetet pas akreditimit

1. Aktivitetet pas akreditimit fillojnë pasi sistemi është autorizuar për operim.

2. Kjo fazë përfshin këto aktivitete:

a) Përdorimi i sistemit:

i. Sistemi operon dhe ruan kushtet e sigurisë nën të cilat u bë i mundur lëshimi i DAS.

ii. AKAS-i mbikëqyr sigurinë e SKI-ve nën përgjegjësinë e saj nëpërmjet verifikimeve periodike të sigurisë, auditimeve të sigurisë për të garantuar që sistemet e akredituara trajtojnë informacion të klasifikuar në të njëjtat kushte sigurie në të cilat u dha akreditimi;

b) Riakreditimi, i cili kryhet në këto raste:

i. Pas përfundimit të periudhës së vlefshmërisë së Deklaratës së Akreditimit të Sigurisë, sistemi nuk është i autorizuar të trajtojë informacion të klasifikuar;

ii. Nëse ndodhin ndryshime në sistem që ndikojnë në kushtet e sigurisë të tilla si:

- Ndryshimet në nivelin e informacionit të klasifikuar që trajtohet në SKI;
- Ndryshimet në kërkesat e sigurisë që vijnë si pasojë e ndryshimeve të legjislacionit për sigurinë e informacionit të klasifikuar;
- Ndryshimet në arkitekturën e sistemit;
- Ndryshimet në konfigurimet e sigurisë së SKI-ve;
- Ndryshimet në kërkesat operacionale;
- Identifikimi i kërcënimeve ose dobësive të reja në sisteme;
- Identifikimi i mosfunksionimit të masave të sigurisë;
- Përhapja e një incidenti të rëndë të sigurisë kompjuterike ose të sigurisë në përgjithësi dhe që ndikon në akreditimin e sigurisë së sistemit;
- Ndryshimet e rëndësishme në strukturën fizike të ndërtesës ose të POS;

c) Nxjerrja jashtë përdorimit e sistemit:

i. Të merren masa për arkivimin ose deklasifikimin ose shkatërrimin e SKI-ve dhe informacionit që ruhet në të, si dhe raportimin tek AKAS-i që në fazën e planifikimit të nxjerrjes jashtë përdorimit;

ii. Procedurat që do të ndiqen përcaktohen në përputhje me legjislacionin në fuqi dhe dokumentet e sigurisë së sistemit.

PJESA II
KËRKESAT E SIGURISË SË SISTEMEVE

KREU I
SIGURIA FIZIKE E SISTEMEVE

Neni 30
Mjediset dhe infrastruktura e rrjetit

1. Për mbrojtjen e sistemeve aplikohen masa të sigurisë fizike në mjediset dhe infrastrukturën e rrjetit.

2. Sistemet ku trajtohet informacion i klasifikuar "Konfidencial" e lart instalohen dhe operojnë në zona sigurie të klasit I ose II.

3. Sistemet ku trajtohet informacion i klasifikuar "I kufizuar" kur nevoja operacionale kërkon operimin e tyre jashtë zonave të sigurisë, instalohen minimalisht në zonë administrative.

4. Në rastet e shkëmbimit të informacionit të klasifikuar në formë elektronike jashtë zonave të sigurisë aplikohet mbrojtja kriptografike e informacionit.

Neni 31

Sigurimi fizik i serverëve dhe pajisjeve të komunikimit

1. Serverët dhe pajisjet e komunikimit vendosen në ambiente të veçanta të ndara nga zyrat e përdoruesve.

2. Sallat e serverëve dhe pajisjeve të komunikimit vendosen në zona sigurie të klasit I.

3. Sallat e serverëve dhe pajisjeve të komunikimit, si dhe *rack*-et sigurohen nga aksesi i paautorizuar ose dëmtimet fizike.

4. Çelësat ose mekanizmat ekuivalentë të aksesit të dhomave të serverëve dhe pajisjeve të komunikimit, si dhe *rack*-eve kontrollohen përshtatshmërish.

5. Në ambientet ku administrohen materiale ose sisteme të një rëndësie të veçantë (p.sh. materiale kriptografike) vendosen masa shtesë sigurie, si: përforcimi i integritetit të sigurisë nëpërmjet dy personave, ku të gjitha veprimet dëshmohen nga minimalisht një person tjetër i kualifikuar. Në këto zona sigurohen të gjitha pikat e hyrjeve dhe daljeve.

Neni 32

Sigurimi fizik i pajisjeve dhe mediave kompjuterike

1. Pajisjet dhe mediat elektronike që ruajnë informacion të klasifikuar regjistrohen në regjistra të veçantë me numër unik identifikimi dhe ruhen në përputhje me kërkesat e sigurisë, si gjatë orarit zyrtar të punës, ashtu edhe jashtë tij.

2. Pajisjet dhe mediat elektronike që ruajnë informacion të klasifikuar administrohen brenda zonave të sigurisë dhe pajisen me çelës për mbrojtjen ndaj ndërhyrjeve të paautorizuara.

3. Në rastet kur nuk është e mundur të aplikohen masat e përshtatshme të sigurimit fizik të pajisjeve dhe mediave kompjuterike, të bëhet fshirja e memories RAM, si dhe të përdoret një nga metodat e mëposhtme:

a) përdorimi i hard diskut të jashtëm, i cili të ruhet në kasafortë jashtë orarit zyrtar të punës;

b) konfigurimi i sistemit për të penguar ruajtjen e të dhënave lokalisht;

c) përdorimi i programeve kriptografike për kriptimin e pajisjeve dhe mediave kompjuterike.

KREU II

SIGURIA E PERSONELIT TË SISTEMEVE

Neni 33

Edukimi për sigurinë e informacionit

Me qëllim njohjen e personelit me rolet dhe përgjegjësitë, pasojat në rast moszbatimi të rregullave të sigurisë, si dhe risqet e mundshme të sigurisë e masat përkatëse, hartohen dhe aplikohen programe të edukimit të personelit për sigurinë e informacionit.

Neni 34
Autorizimi, certifikimi dhe brifimi i personelit

1. Aksesi në sistem lejohet vetëm për personat e autorizuar, të certifikuar përshtatshmërish dhe të brifuar për aksesin në sistem.

2. Në çdo rast:

a) kufizohet aksesi në sistem sipas nevojës për njohje;

b) lejohet aksesi në sistem vetëm pas autorizimit të kërkesës për akses dhe njohjen me procedurat e operimit të sigurt të sistemit;

c) u jepen përdoruesve të drejtat minimale që u nevojiten për kryerjen e detyrave të tyre;

ç) rishikohen autorizimet dhe të drejtat e aksesit të paktën një herë në vit, si dhe kur personeli ndryshon detyrën. Gjatë rishikimit të autorizimeve për akses, të konfirmohet vlefshmëria e nevojës për aksesimin e sistemit, në të kundërt të hiqet e drejta e aksesit;

d) mbahen rekorde të sakta për:

i. të gjithë personelin e autorizuar për të aksesuar sistemin;

ii. personin/personat që dhanë autorizimin për të aksesuar sistemin;

iii. datën e dhënies së autorizimit;

iv. datat e rishikimit të autorizimit;

v. datën e heqjes së autorizimit.

3. Rekordet mbahen gjatë të gjithë jetëgjatësisë së sistemit, në të cilin është lejuar aksesi.

Neni 35
Siguria industriale

Në rastet e prokurimit të mallrave, punëve dhe shërbimeve për sisteme, ku trajtohet informacion i klasifikuar "Sekret shtetëror", NATO-ja, BE-ja, operatorët ekonomikë që do të ofrojnë produkte ose shërbime të jenë të certifikuar përshtatshmërish me tipin dhe nivelin e informacionit që do të aksesojnë.

KREU III
SIGURIA E KOMUNIKIMEVE

Neni 36
Infrastruktura e komunikimeve
(menaxhimi i kabllove)

1. Kabllot grupohen në kanalina, si më poshtë vijon:

a) grupi 1 – kabllot e sistemeve të paklasifikuara;

b) grupi 2 – kabllot e sistemeve "I kufizuar", "Konfidencial" dhe "Sekret";

c) grupi 3 – kabllot e sistemeve "Tepër sekret".

2. Fibrat optike, pavarësisht grupit ku bëjnë pjesë, mund të grupohen në të njëjtën kanalinë.

3. Kabllot e informacionit të klasifikuar të përfundojnë në kabinete të veçanta.

4. Në rast të niveleve të ndryshme të klasifikimit, kabinetet të ndahen me pllaka ndarëse për secilin nivel klasifikimi.

5. Kabinetet e sistemeve të klasifikuara të jenë në largësi nga kabinetet e sistemeve të paklasifikuara minimalisht 50 cm.

6. Rrjetet e kabllimit të përfundojnë sa më afër kabineteve.

7. Kabllot etiketohen me numrin unik të identifikimit dhe të shenjëzohen në pikat e inspektimit, me shenja dalluese, sipas skemës së mëposhtme:

a) shirit portokalli – "Tepër sekret";

b) shirit i kuq – "Sekret";

c) shirit blu – "Konfidencial";

ç) shirit i bardhë – "I kufizuar".

8. Prizat e rrjetit etiketohen me nivelin e klasifikimit, numrin e kabllos dhe numrin e prizës së rrjetit.

9. Kabllot dhe prizat e rrjetit dokumentohen në regjistrin e kabllove dhe prizave të rrjetit me numrin përkatës dhe nivelin e klasifikimit. Për secilin kabull dokumentohet burimi dhe destinacioni.

10. Procedura e etiketimit dhe regjistrimit të kabllove dhe prizave të rrjetit dokumentohet në POS.

11. *Patch* panelet e sistemeve të klasifikuar ndahen fizikisht nga ato të paklasifikuara, duke i instaluar ato në kabinete të veçanta.

Neni 37

Siguria e emetimeve

Sistemet që përdoren për trajtimin e informacionit të klasifikuar "Konfidencial" e lart mbrohen nga emetimet elektromagnetike kompromet uese, studimi dhe kontrolli i të cilave referohet si "TEMPEST", sipas rregullave dhe procedurave.

Neni 38

Sistemet dhe pajisjet e komunikimit

(Pajisjet RF, *infrared* dhe *bluetooth*)

1. Në zonat e sigurisë ndalohet përdorimi i pajisjeve të tilla si:

a) access point;

b) pajisje periferike me *infrared, bluetooth* ose *wireless*;

c) pajisje RF.

2. Përjashtim bëhet vetëm në rastet kur merret autorizimi nga AKAS-i.

Neni 39

Sistemet dhe pajisjet e komunikimit

1. Për shkëmbimin e informacionit të klasifikuar përdoren pajisje faks të akredituara.

2. Mesazhet faks kriptohen në përputhje me nivelin e informacionit që transmetohet.

3. Pajisjet faks multifunksionale, të lidhura me rrjete kompjuterike të klasifikuara, ndalohet të lidhen drejtpërdrejt me rrjete të telefonisë digjitale të paakredituara përshtatshmërish.

4. Pajisjet faks multifunksionale të lidhura me rrjete kompjuterike të klasifikuara ndalohen të përdoren për skanimin ose fotokopjimin e dokumenteve në nivel më të lartë klasifikimi.

5. Sistemet dhe pajisjet e radiokomunikimit, që përdoren për komunikim të sigurt, sipas niveleve të miratuara, t'i nënshtrohen procesit të akreditimit nga Autoriteti Kombëtar i Akreditimit të Sigurisë.

Neni 40

Telefonat dhe sistemet telefonike

1. Sistemet telefonike të klasifikuara duhet të akreditohen përshtatshmërish.
2. Trafiku i të dhënave të klasifikuara të kriptohet përshtatshmërish.
3. Nuk lejohet përdorimi i telefonave (receptorëve telefonikë) pa kordë për informacionin e klasifikuar, pavarësisht nëse lidhet me pajisje të sigurta telefonike.

KREU IV
SIGURIA E TEKNOLOGJISË SË INFORMACIONIT

Neni 41
Siguria e pajisjeve TIK

1. Në SKI përdoren produkte të vlerësuara sipas një liste të njohur sipas standardeve kombëtare të NATO-s, BE-së, përveç nëse është vlerësuar, pranuar e dokumentuar risku i sigurisë që lidhet me përdorimin e tyre.
2. Kontrollohet dokumentacioni i vlerësimit të produktit, përcaktohen kërkesat specifike të produktit dhe përmbushen këto kërkesa për përdorimin e sigurt të produktit.
3. Produktet transportohen në përputhje me legjislacionin për sigurinë e informacionit.
4. Përdorimi i produkteve që ofrojnë funksione sigurie identifikohet gjatë procesit të akreditimit dhe miratohet rast pas rasti nga AKAS-i.
5. AKAS-i mban dhe përditëson listën e produkteve të miratuara.

Neni 42
Kufizime

Ndalohet përdorimi në SKI i produkteve, të cilat nuk janë prodhuar nga vendet e NATO-s, BE-së, që nuk janë pronë e institucionit, pronë e AKSHI-t ose për rastet e akreditimit të SKI-ve për operatorët ekonomikë, pronë e vetë operatorit, me përjashtim të rasteve kur ka marrëveshje sigurie me shtete dhe organizata ndërkombëtare.

Neni 43
Siguria e produkteve (instalimi dhe konfigurimi i produkteve)

1. Produktet dhe pajisjet TIK etiketohen sipas nivelit më të lartë të informacionit që trajtojnë.
2. Produktet dhe pajisjet TIK etiketohen me numrin unik të identifikimit dhe nivelin e klasifikimit përkatës e shenjëzohen me shenja dalluese sipas skemës së mëposhtme:
a) Shirit portokalli – "Tepër sekret";
b) Shirit i kuq – "Sekret";
c) Shirit blu – "Konfidencial";
ç) Shirit i bardhë – "I kufizuar".

Neni 44
Siguria e produkteve (mirëmbajtja dhe riparimi i produkteve)

1. Mirëmbajtja dhe riparimi i produkteve dhe pajisjeve të TIK-ut bëhet brenda zonave të sigurisë dhe nga personel i certifikuar përshtatshmërish.

2. Kur mirëmbajtja dhe riparimi i produkteve dhe pajisjeve të TIK-ut është e pamundur të bëhet nga personel i certifikuar ose brenda zonave të sigurisë, përmbushen këto detyrime:

a) Dokumentohet rasti dhe nevoja për një ndërhyrje të tillë;

b) Nëse është e mundur, hiqen pjesët e memories dhe deklasifikohet produkti ose pajisja e TIK-ut që do të mirëmbahet apo riparohet përpara ndërhyrjes nga persona të pacertifikuar ose jashtë zonës së sigurisë;

c) Nëse vlerësohet, pastrohet dhe deklasifikohet produkti ose pajisja e TIK-ut që do të mirëmbahet apo riparohet përpara ndërhyrjes për mirëmbajtje ose riparim jashtë zonës së sigurisë;

ç) Personeli teknik që do të kryejë mirëmbajtjen mbikëqyret gjatë të gjithë kohës nga personel i AOS i certifikuar përshtatshmërish dhe brifuar.

Neni 45

Pastrimi dhe nxjerrja jashtë përdorimit e pajisjeve TIK

1. Pastrimi i pajisjeve të TIK-ut nënkupton pastrimin e komponentëve memorizues të tyre në mënyrë të pakthyeshme.

2. Komponentët memorizues brenda pajisjeve të TIK-ut janë:

a) komponentë me memorie elektrostatike;

b) memoriet magnetike të qëndrueshme;

c) memoriet me gjysmëpërcjellës;

ç) memoriet e paqëndrueshme.

3. Pas procedurave të pastrimit, pajisjet TIK dhe komponentët e tyre memorizues trajtohen si më poshtë:

Niveli i klasifikimit para pastrimit	**Niveli i klasifikimit pas pastrimit**
Tepër sekret	Tepër sekret
Sekret	Konfidencial
Konfidencial	I paklasifikuar
I kufizuar	I paklasifikuar

4. Procedurat e pastrimit iniciohen nga pajisje të tjera TIK, të ndryshme nga pajisjet që i nënshtrohen procesit të pastrimit.

5. Rast përjashtimi nga ripërdorimi në rrjet të klasifikuar është kur në komponentët memorizues të pajisjeve TIK është ruajtur çelës kriptografik statik.

Neni 46

Shkatërrimi dhe asgjësimi i pajisjeve TIK

1. Për shkatërrimin e pajisjeve TIK përdoret një nga metodat si në tabelë:

Produkti *hardware*	**Metodat e shkatërrimit**					
	Furrë djegieje	**Mullime goditje**	**Disintegrator /shpërbërës**	**Grirës/ grimcues**	**Prerës**	***Degausser* / demagnetizues**
Pajisje me						

memorie elektrostatike	PO	PO	PO	PO	JO	JO
***Floppy disk* magnetik**	PO	PO	PO	JO	PO	PO
***Hard disk* magnetik**	PO	PO	PO	PO	JO	PO
Shirit magnetik	PO	PO	PO	JO	PO	PO
Disk optik	PO	PO	PO	PO	PO	JO
Memorie me gjysmëpërcjellës	PO	PO	PO	JO	JO	JO

2. Në rastet e përdorimit të pajisjes *degausser*/demagnetizues për shkatërrim, pajisja duhet të jetë sipas një liste të njohur, sipas standardeve kombëtare të NATO-s, BE-së.

3. Procedura për shkatërrimin e komponentëve memorizues të pajisjeve TIK, mbikëqyret nga të paktën tre punonjës të certifikuar në nivelin e klasifikimit të pajisjeve që po i nënshtrohen kësaj procedure.

Neni 47
Siguria e aplikacioneve
(të përgjithshme)

1. Në SKI përdoren aplikacione të licencuara, të miratuara nga AKAS-i.

2. Aplikacionet në përdorim regjistrohen, kontrollohen dhe ruhen për arsye *back up*.

3. Funksionet e sigurisë së aplikacioneve dokumentohen në dokumentet e sigurisë së sistemit (DSS ose POS).

Neni 48
Siguria e aplikacioneve
(kufizime)

1. Ndalohen ndryshimet në konfigurimet e aplikacioneve ose në vetë aplikacionin pa miratim paraprak. Nëse këto ndryshime ndikojnë në profilin e sigurisë së sistemit, merret paraprakisht miratimi i AKAS-it.

2. Ndalohet përdorimi i autorizuar dhe i paautorizuar i SKI-ve të aksesojë sistemin duke përdorur kredenciale dhe identitete të tjera.

3. Ndalohet përdorimi i llogarive në grup në sisteme të klasifikuara në nivel "Konfidencial" e lart, që operojnë në mënyrën e lartë të sigurisë ose në mënyrën me shumë nivele. Në SKI-të që operojnë në mënyrën e dedikuar, mund të përdoren llogaritë në grup me kusht që të miratohen nga AKAS-i rast pas rasti. Në çdo rast të merren masat përkatëse për identifikimin, autentifikimin dhe mbajtjen në llogari të individëve që aksesojnë llogaritë në grup.

Neni 49
Mjediset e operimit standard të aplikacioneve

Në mjediset e operimit standard merren masat për:

1. çaktivizimin, riemërimin ose ndryshimin e fjalëkalimeve të llogarive *default* të sistemeve operative;

2. fshirjen ose çaktivizimin e llogarive të përdoruesve, aplikacioneve, komponentëve, shërbimeve dhe funksionaliteteve të panevojshme në sistem;

3. çaktivizimin e llogarive të administratorëve lokalë dhe përdorimin e llogarive të *domain*-it me të drejta administrative lokale;

4. aktivizimin dhe konfigurimin e funksioneve të sigurisë që ofrojnë aplikacionet;

5. ndjekjen e udhëzimeve të prodhuesve, për konfigurimin e sigurt, përditësimin e produkteve të tyre;

6. përdorimin e metodave të kontrollit të aplikacioneve për kufizimin e ekzekutimit të programeve, *dll*-ve dhe skripteve sipas një liste të miratuar;

7. konfigurimin e mekanizmave të kontrollit të aplikacioneve për gjenerimin e *log*-eve gjatë ndërhyrjeve të dështuara dhe regjistrimin e informacionit në lidhje me skedarët e bllokuar, kohën dhe përdoruesin;

8. përdorimin e sistemeve të parandalimit të ndërhyrjeve *host-based* në serverë që administrojnë informacion të klasifikuar në nivel "Sekret" dhe "Tepër sekret";

9. përdorimin e aplikacioneve për kontrollin e trafikut të rrjetit;

10. përdorimin e aplikacioneve të kontrollit të pajisjeve periferike për të parandaluar përdorimin e paautorizuar të mediave kompjuterike dhe pajisjeve në kompjuterë dhe serverë;

11. moslejimin e përdoruesve të çaktivizojnë ose tejkalojnë mekanizmat e kontrollit të aplikacioneve;

12. moslejimin e përdoruesve të instalojnë, çinstalojnë ose çaktivizojnë aplikacione;

13. moslejimin e pajisjeve të lidhen njëkohësisht në dy rrjete të ndryshme.

Neni 50

Mbrojtja nga aplikacionet keqdashëse dhe viruset kompjuterike

1. Të përdoren programe kundër aplikacioneve keqdashëse dhe viruseve kompjuterike, dhe të dokumentohen detajet që lidhen me to, përfshirë kërkesat dhe procedurat për përditësim dhe skanim, si dhe personat përgjegjës për përditësimin e tyre dhe ndjekjen e procedurave të sigurisë.

2. Instruksionet për veprimet që duhen ndërmarrë dhe raportimin e incidenteve që lidhen me infektimet e aplikacioneve keqdashëse dhe viruseve kompjuterike dokumentohen në POS.

Neni 51

Përditësimi (*patching*) i *software*-eve

1. Procedurat e menaxhimit të përditësimeve të sistemeve operative, aplikacioneve, *driver*-ave dhe *firmware* të pajisjeve të përfshihen në POS.

2. Të monitorohen burimet e informacionit për dobësitë e reja dhe përditësimet përkatëse për sistemet operative, aplikacionet, *drive*-rat dhe *firmware* e pajisjeve.

3. Sistemet operative, aplikacionet dhe pajisjet *hardware* që nuk suportohen më nga prodhuesi të zëvendësohen me një version që suportohet nga prodhuesi ose me një version të suportueshëm nga një prodhues tjetër.

Neni 52

Zhvillimi i aplikacioneve

1. Gjatë zhvillimit të aplikacioneve për trajtimin e informacionit të klasifikuar, merren në konsideratë përmbushja e objektivave të sigurisë gjatë të gjithë fazave të zhvillimit të aplikacioneve (disenjimi, zhvillimi, shpërndarja dhe mirëmbajtja).

2. Aplikacionet u nënshtrohen procesit të testimit të sigurisë, menaxhimit të konfigurimeve dhe kontrollit të ndryshimeve.

3. Të mos lejohet aksesi i paautorizuar në kodin burim të aplikacioneve.

Neni 53

Implementimi i teknologjisë *web* në sistemet e klasifikuara

Gjatë implementimit të shërbimeve *intranet* në SKI:

1. hartohen dhe dokumentohen në POS procedurat për implementimin dhe përdorimin e sigurt të shërbimeve *intranet*;

2. shenjëzohen faqet *web* përshtatshmërish me nivelin më të lartë të klasifikimit të informacionit që përmbahet në atë faqe;

3. sigurohet vlefshmëria dhe pastrimi i të gjithë *input*-it në aplikacionet *web*;

4. implementohen kontrollet e sigurisë së shfletuesit për mbrojtjen e aplikacioneve *web* dhe përdoruesve të tyre.

Neni 54

Sistemet e databazave

Në databaza, ku trajtohet informacion i klasifikuar:

1. fshihen të gjithë skedarët dhe *log*-et e përkohshme të instalimit pas instalimit të sistemeve për menaxhimin e databazave;

2. konfigurohen në mënyrë të sigurt sistemet e menaxhimit të databazave në përputhje me udhëzimet e prodhuesit;

3. fshihen të gjitha databazat model që instalohen me sistemin e menaxhimit të databazave;

4. sigurohet ruajtja e fjalëkalimeve të kriptuara me algoritme të forta kriptimi në databaza;

5. aplikohen kontrolle aksesi në skedarët e databazave në përputhje me përcaktimet e AOS-it;

6. shenjëzohen përshtatshmërish me informacionin e klasifikuar që përmbajnë;

7. ndahen privilegjet e përdoruesve të databazës sipas nevojës për njohje duke u dhënë atyre privilegjet e nevojshme për akses, futje të dhënash, modifikim ose fshirje të dhënash në databazë sipas detyrave përkatëse, në përputhje me përcaktimet e AOS-it;

8. çaktivizohen, riemërohen ose ndryshohen fjalëkalimet e llogarive *default* të administratorëve;

9. fshihen llogaritë anonime të databazave;

10. ndahen funksionalisht serverët e databazave dhe serverët *web*, nëpërmjet një ndarjeje fizike ose virtuale;

11. vendosen serverët e databazave në një segment rrjeti të ndryshëm nga kompjuterët e përdoruesve;

12. filtrohen të gjithë pyetësorët (*queries*) nga aplikacionet *web* për përmbajtje të ligjshme dhe sintaksë korrekte;

13. përdoren pyetësorë me parametra të caktuar ose procedura të ruajtura në vend të pyetësorëve të gjeneruar automatikisht;

14. kontrollohet, monitorohet qasja te skedarët e databazës

15. disenjohen aplikacione *web* që të ofrojnë sa më pak informacion të sistemit të menaxhimit të databazave dhe skemave të databazave për përdoruesit gjatë gabimeve që mund të ndodhin në sistem;

16. nuk lejohen ose nuk fshihen të gjitha funksionet dhe procedurat e ruajtura të panevojshme të sistemeve për menaxhimin e databazave;

17. nuk lejohen opsionet e sistemit të menaxhimit të databazave për leximin e filave lokale nga serveri;

18. nuk kryhen aktivitetet e testimit dhe të zhvillimit të databazave në serverët e databazave që janë në përdorim;

19. nuk përdoret informacioni i klasifikuar në mjediset e testimit dhe të zhvillimit të databazave, përveç nëse janë akredituar përshtatshmërish me nivelin më të lartë të informacionit që trajtojnë.

Neni 55
Siguria e *email*-eve

Gjatë implementimit të shërbimeve të postës elektronike në sistemet e klasifikuara:

1. Sigurohet që infrastruktura e postës elektronike të jetë pjesë e sistemit të klasifikuar dhe të mos ketë lidhje me sisteme të tjera të paakredituara përshtatshmërish.

2. Dokumentohen procedura në POS për përdorimin e sigurt të postës elektronike të klasifikuar.

3. Shenjëzohen mesazhet e postës elektronike, në përputhje me nivelin e informacionit që mesazhi përmban dhe nivelin e informacionit të dokumenteve bashkëlidhur.

Neni 56
Kontrolli i aksesit

1. Për kontrollin e aksesit në SKI përcaktohet skema e kontrollit të aksesit, ku përshkruhen atributet e çdo entiteti që ka qasje në SKI apo në informacionin e klasifikuar që trajtohet në të, bazuar në parimin "nevojë për njohje", si dhe duke autorizuar dhe lejuar privilegjet që nevojiten për kryerjen e detyrave.

2. Skema e kontrollit të aksesit hartohet sipas një modeli që siguron:

a) Administrimin e entiteteve dhe atributeve, privilegjeve dhe kredencialeve të tyre gjatë të gjithë jetëgjatësisë së tyre;

b) Shërbimet e autentifikimit dhe në varësi të rezultateve të raportit të vlerësimit të riskut, implementimin e një metode të kombinuar autentifikimi;

c) Auditimin e aksesit të informacionit nga përdoruesit, shërbimet e SKI-ve;

ç) Kufizimin sipas parimit nevojë për njohje dhe monitorimin e llogarive të përdoruesve me të drejta të privilegjuara;

d) Auditimin e përdoruesve dhe aktiviteteve të SKI-ve;

dh) Parandalimin e vjedhjes së kredencialeve, si dhe ripërdorimit të tyre nga persona të paautorizuar;

e) Mbështetjen e investigimit të incidenteve dhe auditimit të sigurisë.

3. Në varësi të rezultateve të raportit të vlerësimit të riskut, implementohet një metodë e kombinuar autentifikimi për përdoruesit e privilegjuar, si:

a) administrator sistemi;

b) administrator *database*-i;

c) përdorues me të drejta jo të kufizuara;

ç) përdorues me të drejta të aksesit në largësi;

d) përdorues.

Neni 57

Auditimi dhe ruajtja e *log*-eve të sigurisë

1. Në çdo SKI ruhen dhe auditohen ngjarje që lidhen me:
a) veprimet e privilegjuara;
b) shtimin, fshirjen dhe modifikimin e të drejtave të aksesit të përdoruesve dhe grupeve;
c) përpjekjet e dështuara për akses/qasje në sisteme dhe *fil*-e kritike;
ç) paralajmërime (*alert*) dhe dështime që lidhen me sigurinë e sistemit;
d) hyrjet dhe/ose daljet në sistem;
dh) përpjekjet e dështuara për hyrje në sistem.
2. Për çdo ngjarje ruhet:
a) data dhe ora e ngjarjes;
b) përdoruesi apo procesi që lidhet me ngjarjen;
c) përshkrimi i ngjarjes;
ç) dështimi apo suksesi i ngjarjes;
d) burimi i ngjarjes (p.sh. emri i aplikacionit);
dh) vendndodhja/identifikimi i pajisjes, ku ka ndodhur.
3. Këto rekorde ruhen sipas një periudhe të rënë dakord ndërmjet AKAS-it dhe AOS-it të specifikuar në DSS-në dhe POS-në përkatëse. Për informacionin e klasifikuar në nivel "Tepër sekret" kjo periudhë të jetë minimalisht 5 vjet.
4. Informacioni i auditimit të mbrohet nga aksesi, ndryshimi ose fshirja e paautorizuar.

Neni 58

Menaxhimi i rrjetit

1. Rrjetet menaxhohen në mënyrë të përqendruar.
2. Ndryshimet në konfigurimet e rrjetit miratohen paraprakisht.
3. Konfigurimet e rrjetit kontrollohen vazhdimisht për përputhje me konfigurimet e dokumentuara.
4. Dokumentacioni i konfigurimeve të rrjetit përfshin:
a) diagramin e rrjetit, ku tregohen të gjitha lidhjet e rrjetit;
b) diagramin logjik të rrjetit, ku tregohen të gjitha pajisjet e rrjetit, shërbimet dhe serverët;
c) konfigurimet e pajisjeve të rrjetit.
5. Dokumentacioni i konfigurimeve të rrjetit përditësohet me ndryshimet e fundit dhe klasifikohet në tërësi me nivelin më të lartë të informacionit që trajtohet në rrjet.
6. Dokumentacioni i rrjetit që u vihet në dispozicion palëve të treta të përmbajë vetëm detajet e nevojshme për përmbushjen e detyrimeve, shërbimeve sipas kontratës.
7. Pajisjet e rrjetit inventarizohen rregullisht.

Neni 59

Disenjimi dhe konfigurimi i rrjetit

Në disenjimin dhe konfigurimin e rrjetit sigurohet:
1. implementimi i kontrolleve mbi aksesimin e rrjetit për të kufizuar trafikun, sipas nevojës, për njohje brenda dhe ndërmjet segmenteve të rrjetit;

2. çaktivizim i portave fizike të papërdorura në pajisjet e rrjetit;

3. çaktivizim, riemërtim ose ndryshim i fjalëkalimeve dhe llogarive *default* në pajisjet e rrjetit;

4. sinkronizim i kohës në të gjitha pajisjet e rrjetit;

5. zhvillim, implementim, mirëmbajtje e procedurave të sistemeve të detektimit dhe parandalimit të ndërhyrjeve, ku përfshihen:

a) sistemet NISP, NISD;

b) procedura dhe burime për mirëmbajtjen dhe kontrollin e nënshkrimeve elektronike;

c) procedura dhe burime për analizimin e *log*-eve dhe paralajmërimeve (*alert*) në kohë reale;

ç) procedura dhe burime për përgjigje ndaj incidenteve të detektuara (zbuluara);

d) frekuencat e rishikimit të procedurave dhe burimeve të detektimit (zbulimit) dhe parandalimit.

6. Aplikimi i sistemeve të detektimit dhe parandalimit të ndërhyrjeve në të gjitha nyjat e ndërlidhjes në rastet e ndërlidhjes së sistemeve.

7. Përdorimi i VLAN-it për ndarjen e trafikut të rrjetit vetëm ndërmjet rrjeteve në të njëjtin nivel klasifikimi.

Neni 60

Videokonferencat, rrjeti telefonik dhe telefonia IP

1. Telefonia IP të konfigurohet në mënyrë të tillë që:

a) telefonat IP të autentifikojnë vetveten te menaxhuesi i thirrjeve gjatë regjistrimit;

b) të çaktivizohet funksioni i vetëregjistrimit të pajisjeve dhe të lejohet aksesi në rrjet vetëm për një listë të mirëpërcaktuar të pajisjeve të autorizuara;

c) të bllokohen pajisjet e paautorizuara;

ç) të çaktivizohen funksionet e papërdorura dhe të ndaluara.

2. Trafiku i videokonferencave dhe telefonisë IP të ndahet fizikisht ose logjikisht nga trafiku i të dhënave të tjera të rrjetit.

KREU V

SIGURIMI KRIPTOGRAFIK

Neni 61

Të përgjithshme

1. Për kriptimin e informacionit të klasifikuar "Sekret shtetëror" të palëvizshëm ose në transit përdoren produkte, algoritme ose protokolle kriptografike të vlerësuara nga Autoriteti Kombëtar i Sigurimit të Komunikimeve dhe të miratuara nga AKAS-i.

2. AKAS-i mban listën e produkteve, algoritmeve dhe protokolleve kriptografike të miratuara për përdorim.

3. Për kriptimin e të dhënave të palëvizshme përdoret:

a) kriptimi i plotë i diskut;

b) kriptimi i pjesshëm i diskut me kusht që të lejohet shkrimi vetëm në particione të kriptuara.

4. Produktet kriptografike do të ofrojnë një mënyrë për rikuperimin e të dhënave në rast të humbjes ose të dëmtimit të çelësit kriptografik.

5. Në rastet kur informacioni i klasifikuar shkëmbehet nëpërmjet infrastrukturës së rrjeteve publike ose rrjeteve me nivel më të ulët të klasifikimit përdoret kriptimi i të dhënave në transit.

Neni 62

Menaxhimi i materialit kriptografik

1. Pajisjet dhe materialet kriptografike vendosen në zona sigurie të klasit I.

2. Për çdo pajisje dhe material kriptografik mbahet dhe përditësohet regjistri i aksesit, në të cilin ruhen:

a) detaje të personelit që ka akses në sistem në nivel administratori;

b) detaje të personelit që i është hequr aksesi në sistem në nivel administratori;

c) detaje të dokumenteve të sistemit;

ç) aktivitetet e mbajtjes në llogari të transaksioneve me pajisjet dhe materialet kriptografike;

d) aktivitetet e kontrollit të sigurisë së sistemit.

3. Përpara dhënies së aksesit personelit për sigurinë e komunikimeve sigurohet që personat:

a) kanë nevojën për akses;

b) njihen me Planin e Menaxhimit të Materialit Kriptografik për sistemin kriptografik që përdorin;

c) janë të pajisur me certifikatë të përshtatshme të sigurisë së personelit;

ç) mbrojnë dhe nuk nxjerrin informacionin e autentifikimit të sistemit kriptografik;

d) pranojnë të mbajnë përgjegjësi për të gjitha veprimet nën llogarinë e tyre;

dh) raportojnë problemet që lidhen me sigurinë në instancat e duhura.

4. Materiali kriptografik inventarizohet:

a) gjatë kalimit të përgjegjësive administrative (dorëzimit dhe/ose marrjes të detyrës) për sistemin kriptografik;

b) gjatë ndryshimit të personelit që ka akses në sistemin kriptografik;

c) të paktën 2 (dy) herë në vit për gjendjen faktike, sipas dokumenteve dhe administrimin e tyre.

5. Kontrolli i inventarit kryhet nga strukturat e autorizuara dhe të trajnuar për aspektet e sigurisë së komunikimeve.

6. Anulohen materialet çelës ose certifikatat nëse dyshohet se janë kompromentuar.

7. Raportohet te AKAS-i dhe AKSK-ja për çdo material çelës ose certifikatë që dyshohet se është kompromentuar, si dhe çdo incident kriptografik.

KREU VI
SIGURIA E NDËRLIDHJES SË SISTEMEVE TË KLASIFIKUARA

Neni 63
Të përgjithshme

1. Ndërlidhja e SKI-ve kalon në procesin e akreditimit të sigurisë.

2. Pajisjet/produktet me funksione sigurie kalojnë procesin e vlerësimit, të miratimit nga AKAS-i.

3. SKI-të mund të përdorin internetin ose rrjetet e ngjashme të *domain*-it publik vetëm si bartëse, me kusht që në to të implementohet mbrojtja e duhur kriptografike, e miratuar nga AKAS-i.

Neni 64
Rastet e ndalimit

1. Ndalohet ndërlidhja e SKI-ve që trajtojnë informacion të klasifikuar në nivel "Tepër sekret".

2. Ndalohet ndërlidhja e SKI-ve në kaskadë.

3. Ndalohet ndërlidhja e SKI-ve me rrjete të paklasifikuara, me përjashtim të rasteve:

a) ndërlidhje njëdrejtimëshe nëpërmjet përdorimit të diodës së të dhënave;

b) ndërlidhje me SKI-të në nivel "I kufizuar".

Neni 65
Pajisjet *gateway*

Gjatë ndërlidhjes:

1. Sistemet të mbrohen nga sistemet e *domain*-eve të tjera me një ose më shumë pajisje *gateway*.

2. Pajisjet *gateway* të përmbajnë mekanizma për filtrimin e rrjedhës së të dhënave në shtresën e rrjetit (nivel rrjeti).

3. Të gjitha lidhjet ndërmjet *domain*-eve të sigurisë të përmbajnë mekanizma për inspektimin dhe filtrimin e rrjedhës së të dhënave për shtresën e transportit dhe më lart sipas modelit OSI.

4. Sigurohet që pajisjet *gateway*:

a) janë të vetmet rrugë komunikimi ndërmjet rrjeteve;

b) në gjendje *default* pengojnë të gjitha lidhjet brenda dhe jashtë rrjetit;

c) lejojnë vetëm lidhjet e autorizuara në mënyrë eksplicite;

ç) janë konfiguruar me masat e përshkruara në këtë rregullore;

d) menaxhohen nëpërmjet një *path*-i të sigurt të izoluar nga rrjetet e lidhura (fizikisht me *gateway* ose në një rrjet administrues të dedikuar);

dh) ofrojnë regjistrim *log*-esh dhe kapacitete të mjaftueshme për identifikimin e incidenteve të sigurisë kompjuterike, përpjekjet për ndërhyrje dhe *pattern* të përdorimit të pazakontë;

e) ofrojnë paralajmërime (*alert*) në kohë reale.

5. Për ofrimin e shërbimeve që aksesohen nga autoritetet e tjera të ndërlidhura përdoren zonat e demilitarizuara (DMZ).

6. Kryhet vlerësimi i riskut të sigurisë në pajisjet *gateway* dhe konfigurimet përkatëse përpara implementimit të tyre.

7. Dokumentohen e vlerësohen të gjitha ndryshimet në arkitekturën e pajisjeve *gateway*.

8. Kufizohet aksesi në funksionet administrative të pajisjeve *gateway*.

9. Sigurohet që administratorët janë të trajnuar për menaxhimin e pajisjeve *gateway*.

10. Ruhen *log*-et e të gjitha veprimeve (*events*).

Neni 66
Pajisjet *firewall*

Në ndërlidhje sistemesh përdoren pajisje *firewall* si pjesë e infrastrukturës në të gjitha pikat e ndërlidhura, në mënyrë të pavarur.

Neni 67
Diodat e të dhënave

1. Në ndërlidhje sistemesh njëdrejtimësh përdoren dioda të dhënash sipas një liste të njohur sipas standardeve kombëtare, të NATO-s, BE-së dhe të certifikuar me nivelin me të lartë të informacionit, i cili trajtohet në këto SKI.

2. Gjatë përdorimit të diodës së të dhënave monitorohet volumi i të dhënave që transferohet.

Neni 68
Përmbajtjet dhe lidhjet *web*

Në rastin e implementimit të faqeve *web* në ndërlidhje sistemesh:

1. dokumentohen në POS politikat e përdorimit të sigurt të *web*-it;

2. aksesi i faqeve *web* kryhet nëpërmjet një *web proxy*. *Web proxy* autentifikon përdoruesit dhe ruan *log*-et me detajet e faqeve *web*, që aksesohen:

a) adresa URL;

b) koha/data;

c) përdoruesi;

ç) sasia e të dhënave të *upload*-uara dhe *download*-uara;

d) adresa IP.

Neni 69

Pajisjet KVM *switch*

1. Gjatë ndërlidhjes së SKI-ve, përdoren pajisje KVM *switch* sipas një liste të njohur sipas standardeve kombëtare të NATO-s, BE-së për aksesimin e sistemeve sipas rasteve:

a) sistem i klasifikuar dhe sistem i paklasifikuar;

b) sisteme me nivele të ndryshme klasifikimi;

c) sisteme në të njëjtin nivel klasifikimi por në *domain*-e të ndryshme.

2. Pajisjet KVM *switch*:

a) operohen manualisht;

b) kanë të ndarë përshtatshmërish dhe në mënyrë të dukshme kabllot nga sisteme të ndryshme;

c) përmbajnë tregues për të njoftuar përdoruesin në rastet kur kalohet në sisteme të paklasifikuara;

ç) inspektohen rregullisht lidhur me mirëfunksionimin e tyre.

3. Pajisjet KVM *switch* nuk duhet të kenë procesor ose memorie të brendshme.

4. Pajisjet KVM *switch* nuk lejohet të lidhen me sisteme të paklasifikuara, të cilat kanë konvertues analog–digjital.

Neni 70

Politika dhe procedurat e transferimit të të dhënave

Gjatë ndërlidhjes së SKI-ve sigurohet që:

1. veprimet e përdoruesve që shkëmbejnë të dhëna ndërmjet sistemeve ruhen në *log*-e;

2. përdoruesit parandalojnë incidentet kompjuterike nëpërmjet:

a) kontrollit të shenjëzimeve për të siguruar që sistemi destinacion është i përshtatshëm për administrimin e të dhënave që transferohen;

b) kryerjen e kontrollit kundër viruseve në të dhënat që transferohen;

c) ndjekjen e proceseve dhe procedurave për transferimin e të dhënave;

3. të dhënat e importuara në sistem:

a) skanohen për përmbajtje keqdashëse dhe aktive;

b) kontrollohet formati i të dhënave;

c) ruhen *log*-et për çdo ngjarje;

ç) monitorohen për identifikimin e modeleve të pazakonta të përdorimit;

4. të dhënat e eksportuara në sistem:

a) kontrollohen për shenjëzimet përkatëse;

b) ruhen *log*-et për çdo ngjarje;

c) monitorohen për identifikimin e modele të pazakonta të përdorimit;

ç) kontrollohet formati i të dhënave;

d) bëhen kontrolle të fjalëve;
dh) kontrollohet madhësia e skedarëve;
5. transferimi i të dhënave kryhet në përputhje me procedurat e përcaktuara në POS.

KREU VII
PUNA JASHTË ZONAVE TË SIGURISË

Neni 71
Pajisjet e lëvizshme

1. Dokumentohen në POS procedurat e përdorimit të sigurt të pajisjeve të lëvizshme.
2. Risku që lidhet me përdorimin e pajisjeve të lëvizshme të vlerësohet dhe dokumentohet.
3. Në rast të përdorimit të pajisjeve të lëvizshme për komunikimin e informacionit të klasifikuar për infrastrukturën e rrjeteve publike, përdorin produkte kriptografike të miratuara nga AKAS-i.
4. Në rast të lejimit të pajisjeve të lëvizshme për aksesimin e informacionit të klasifikuar, ndalohet instalimi dhe çinstalimi i aplikacioneve nga përdoruesit.
5. Në rast të lejimit të pajisjeve të lëvizshme për aksesimin e informacionit të klasifikuar, ndalohet çaktivizimi i funksioneve të sigurisë nga përdoruesit.
6. Në rast se ofrohet funksion i zerimit ose sanitizimit të pjesës memorizuese në pajisjet e lëvizshme, ky funksion të përdoret si pjesë e procedurave të asgjësimit në raste emergjence.
7. Për përpunimin ose ruajtjen e informacionit të klasifikuar në nivel "Tepër sekret", nuk lejohet përdorimi i pajisjeve të lëvizshme përveçse me miratim të AKAS-it.
8. Pajisjet e lëvizshme që nuk janë në zotërim të institucionit nuk lejohen të përdoren për aksesimin ose administrimin e informacionit të klasifikuar.
9. Pajisjet e lëvizshme që nuk janë në zotërim të institucionit nuk lejohet të futen pa autorizimin me shkrim të titullarit të AOS-it.
10. Nuk lejohen funksionet *bluetooth*, *wireless* apo *infrared* në pajisjet e lëvizshme.

Neni 72
Pajisjet e lëvizshme jashtë zonave të sigurisë

1. Pajisjet e lëvizshme transportohen në mënyrë të sigurt jashtë zonave të sigurisë pas autorizimit të AOS-it.
2. Pajisjet e lëvizshme jashtë zonave të sigurisë të mbahen nën mbikëqyrje të vazhdueshme.
3. Në pajisjet e lëvizshme kur përdoren jashtë shtetit sigurohet:
a) aplikimi i përditësimeve të aplikacioneve dhe i sistemeve operative;
b) implementimi i autentifikimit multifaktorial;
c) kryerja e *back up*-it të të dhënave;
ç) heqja e informacioneve të panevojshme nga pajisja;
d) çaktivizimi i aplikacioneve që nuk janë të rëndësishme për periudhën e udhëtimit;
dh) çaktivizimi i lidhjeve *bluetooth*, *wireless* dhe *infrared*;
e) mbajtja nën kontroll gjatë të gjithë kohës;
4. Në rast se ofrohet funksion i zerimit ose sanitizimit të pjesës memorizuese në pajisjet e lëvizshme, ky funksion të përdoret si pjesë e procedurave të asgjësimit në raste emergjence.

KREU VIII
INCIDENTET E SIGURISË KOMPJUTERIKE DHE PROCEDURAT E RAPORTIMIT

Neni 73

Përgjigjja ndaj incidenteve të sigurisë kompjuterike

1. Për trajtimin e incidenteve të sigurisë caktohet personel me kualifikimin e duhur profesional.

2. Incidentet që lidhen me sigurinë e sistemeve regjistrohen në regjistër të veçantë. Në këta regjistra regjistrohen minimalisht të dhënat e mëposhtme:

a) data e verifikimit të incidentit të sigurisë;

b) data kur ka ndodhur incidenti i sigurisë;

c) një përshkrim i incidentit të sigurisë, përfshirë personelin dhe mjediset e përfshira;

ç) veprimet e marra;

d) kujt i është raportuar incidenti;

dh) dokumenti referencë i përfshirë në incident (nëse ka të tillë).

3. Incidentet që lidhen me sigurinë e sistemeve të raportohen në strukturat e duhura, me qëllimin përgjigjen, hetimin dhe inspektimin në përputhje me legjislacionin për sigurinë e SKI-ve.

Neni 74

Njoftimi i AKAS-it për incidentet

Kushtet, në të cilat AKAS-i duhet njoftuar menjëherë pas ndodhjes së incidentit janë:

1. thyerjet e sigurisë që prekin informacionin e klasifikuar;
2. përhapje e paautorizuar e informacionit në mediat publike ose në entitete të tjera;
3. akses i paautorizuar i të dhënave;
4. dyshime për spiunazh, sabotim ose terrorizëm;
5. aktivitete të brendshme keqdashëse (p.sh. kërcënim i brendshëm);
6. incidente që përfshijnë akses të privilegjuar në SKI;
7. incidente që përfshijnë elemente kriptografike;
8. incidente që cenojnë sigurinë kombëtare.

Neni 75

Operatorët ekonomikë

1. Operatorët ekonomikë, gjatë realizimit të kontratave të klasifikuara, përdorin SKI të akredituara përshtatshmërish.

2. Periudha e vlefshmërisë së akreditimit është në përputhje me afatet e zbatimit të kontratës së klasifikuar, por jo më tepër se 3 (tre) vjet.

3. Për operatorët ekonomikë ndalohet akreditimi i SKI-ve në nivel "Tepër sekret" ose ekuivalent.

4. Ndalohet ndërlidhja e SKI-ve për operatorët ekonomikë/kontraktorët me SKI-në e institucioneve shtetërore.

Neni 76

Dispozita kalimtare dhe të fundit

1. Ministritë, institucionet shtetërore dhe operatorët ekonomikë marrin masa për zbatimin e kërkesave të kësaj rregulloreje.

2. Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar ngarkohet për kontrollin e zbatimit të kërkesave të kësaj rregulloreje.

3. Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar ngarkohet për nxjerrjen e modeleve në zbatim të shkronjës "a", të pikës 2, të nenit 18, dhe udhëzimin, në zbatim të pikës 4, të nenit 27, të kësaj rregulloreje, brenda 90 ditëve nga hyrja në fuqi e këtij vendimi.