Aprobată
prin ordinul Ministrului Apărării
nr.528 din 08 august 2019

POLITICA DE SECURITATE CIBERNETICĂ A MINISTERULUI APĂRĂRII

I. Generalităţi

Tendinţele realităţii actuale în care informaţia devine unul din activele primordiale ale entităţilor atât la nivel mondial, cât şi naţional, iar gestionarea acesteia se efectuează prin intermediul sistemelor informaţionale, impun atragerea unei atenţii deosebite la domeniul securităţii informaţionale şi cibernetice.

Din acest motiv, lipsa unei abordări sistemice manageriale asupra problemelor de securitate cibernetică reprezintă unul din factorii de risc sporit pentru asigurarea principiilor de bază de organizare a sistemului de management de securitate cibernetică.

În acelaşi timp, compromiterea securităţii cibernetice poate afecta funcţionalitatea Sistemului de comunicaţii şi informatică al Armatei Naţionale (SCIAN) în vederea asigurării serviciilor de comunicaţii şi informatică, fapt ce are consecinţe majore asupra îndeplinirii misiunii şi sarcinilor stabilite.

Cadrul normativ existent la momentul actual prevede următoarele definiţii:

securitatea informaţională ***(Legea Parlamentului nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova)*** - stare de protecție a resurselor informaţionale, precum și a persoanei, societăţii şi statului, în spaţiul informațional;

securitatea informaţională (*Regulamentul privind managementul securităţii informaţionale în cadrul Sistemului de comunicaţii şi informatică al Armatei Naţionale*) - ansamblul măsurilor de protecţie a informaţiilor, care sunt prelucrate, păstrate sau transmise prin intermediul sistemelor informaţionale, împotriva ameninţărilor şi a oricăror acţiuni care pot afecta confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi non-repudierea informaţiilor, precum şi afectarea funcţionării sistemelor electronice, indiferent dacă acestea apar accidental sau intenţionat;

apărare cibernetică (***Hotărîrea Guvernului nr. 811 din 29.10.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020)*** acţiuni desfăşurate în scopul protecției, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun la amenințările asupra infrastructurilor cibernetice destinate apărării naționale;

securitate cibernetică (***Hotărîrea Guvernului nr. 811 din 29.10.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020)*** - stare de normalitate rezultată în urma aplicării unui ansamblu complex de măsuri proactive şi reactive prin care în spațiul cibernetic se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi non-repudierea informaţiilor în format electronic, a sistemelor și resurselor

informaționale, a serviciilor publice și private. Măsurile proactive și reactive includ politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protecție a infrastructurilor cibernetice, managementul identității, managementul consecințelor;

spațiu cibernetic (***Hotărîrea Guvernului nr. 811 din 29.10.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2021***) **-** mediu virtual, generat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acest mediu.

II. Scop, obiective şi domeniu de activitate

Politica privind securitatea cibernetică se aplică în cadrul Ministerului Apărării, autorităţile administrative/instituţiile din subordinea Ministerului Apărării şi unităţile militare ale Armatei Naţionale faţă de:

1. Echipamentele (hardware) şi produsele de program (software) existente în dotarea Ministerului Apărării şi Armatei Naţionale;
2. Sistemele informatice şi resursele informaţionale existente, precum şi cele aflate în etapa de elaborare, testare sau implementare.

Politica Ministerului Apărării şi Armatei Naţionale privind securitatea cibernetică are ca *scop* asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei, precum şi asigurarea colectării, procesării, stocării şi accesării în condiţii de siguranţă a datelor.

Scopul enunţat al politicii presupune atingerea următoarelor obiective:

1. Respectarea şi punerea în aplicare a prevederilor cadrului normativ naţional şi internaţional, inclusiv a standardelor larg acceptate din domeniul securităţii cibernetice.
2. Implementarea procedurilor de securitate cibernetică în scopul respectării cerinţelor minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr.201 din 28.03.2017, în cadrul sistemelor informatice ale Armatei Naţionale.
3. Implementarea măsurilor organizaţionale în corespundere cu Regulamentul asigurării securităţii informaţionale şi Regulamentul managementului securităţii în cadrul Sistemului de comunicaţii şi informatică al Armatei Naţionale.
4. Prevenirea accesului nesancţionat la resursele informatice ale Armatei Naţionale.
5. Asigurarea funcţionării neîntrerupte şi în condiţii de siguranţă a sistemelor informatice.
6. Asigurarea răspunsului prompt şi eficient la incidentele de securitate cibernetică.

7. Perfecţionarea deprinderilor practice şi ale cunoştinţelor personalului tehnic specializat, precum şi ale utilizatorilor sistemelor informatice.

8. Implementarea măsurilor de evaluare şi gestionare a riscurilor de securitate cibernetică şi sporirea gradului de protecţie a sistemelor, echipamentelor (hardware) şi produselor de program (software).

Scopul securităţii cibernetice este de a proteja sistemele, echipamentele şi produsele de program din cadrul Ministerului Apărării şi Armatei Naţionale, de a asigura continuitatea activităţii şi de a minimiza daunele aduse prin prevenirea şi minimizarea impactului incidentelor de securitate, prin înlăturarea breşelor de securitate şi prin actualizarea produselor software şi echipamentelor hardware.

III. Principiile de organizare internă a managementului de securitate cibernetică

Sistemul de management al securităţii cibernetice al Ministerului Apărării şi Armatei Naţionale are la bază următoarele principii:

1. *confidenţialitatea* – asigurarea accesului la informaţie doar utilizatorilor autorizaţi. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la sistemele informaţionale;

2. *integritatea* - păstrarea acurateţei şi completitudinii informaţiei, precum şi a metodelor de procesare;

3. *disponibilitatea* - asigurarea faptului că utilizatorii autorizaţi au acces (la necesitate) la informaţie şi la resursele asociate. Diverse produse software necesită nivele diferite de disponibilitate, în funcţie de impactul daunelor produse ca urmare a nefuncţionării corespunzătoare a sistemelor informaţionale;

4. *nonrepudierea* - asigurarea faptului că, după emiterea/recepţionarea unei informaţii într-un sistem de comunicaţii securizat, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informaţiile în cauză.

Accesul la resursele din Internet, din interiorul sistemelor informatice conectate la acesta, este restricţionat prin blocarea paginilor web cu conţinut maliţios sau irelevant pentru îndeplinirea obligaţiunilor funcţionale (de exemplu: care conţin aplicaţii maliţioase sau ilegale, pornografie, pariuri, audio şi video online de divertisment etc.).

Resursele informaţionale ale Ministerului Apărării vor fi utilizate doar în interes de serviciu.

IV. Analiza ameninţărilor, vulnerabilităţilor şi riscurilor

Pentru implementarea politicii date se efectuează audite interne și externe de securitate cibernetică asupra sistemelor informatice ale Armatei Naţionale, care cuprinde următoarele aspecte:

1. Evaluarea ameninţărilor prin identificarea vulnerabilităţilor şi probabilitatea de producere a lor, precum şi estimarea impactul potenţial;

2. Identificarea riscurilor de securitate cibernetică, care trebuie eliminate sau pot fi tolerate şi stabilirea prioritizării acestora;

3. Identificarea sistemelor, echipamentelor şi produselor de program care trebuie protejate şi la ce nivel;

4. Resursele financiare, umane, tehnice etc. necesare pentru implementarea măsurilor de securitate cibernetică;

5. Procedurile şi metodele prin care urmează a fi implementată securitatea cibernetică.

V. Declaraţia conducerii Ministerului Apărării şi Armatei Naţionale de susţinere a scopului şi principiilor politicii interne privind securitatea cibernetică a instituţiei

Conducerea Ministerului Apărării şi Armatei Naţionale îşi asumă responsabilitatea pentru organizarea şi gestionarea activităţii privind menţinerea şi îmbunătăţirea sistemului de management al securităţii cibernetice.

Conducerea unităţilor şi instituţiilor militare vor asigura şi vor cere respectarea cerinţelor de securitate cibernetică de către efectivul din subordine.

VI. Responsabilităţile asigurării securităţii cibernetice

Agenţia Informaţii Militare este entitatea responsabilă de:

1. elaborarea cadrului normativ, asigurarea şi controlul implementării protecţiei informaţiilor;

2. asigurarea conformității cu politica națională, standarde, reglementări și legislație în domeniul protecţiei informaţiei;

3. analiza pericolelor globale şi posibilele căi de influenţă la protecţia informaţiei în cadrul Armatei Naţionale;

4. controlul asupra realizării şi monitorizării permanente a protecţiei informaţiei.

Serviciul securitate informaţională (din cadrul J6 Direcţiei comunicaţii şi sisteme informaţionale) este entitatea desemnată cu responsabilităţi de elaborare a cadrului normativ şi de monitorizare a implementării sistemului de management al securităţii cibernetice în cadrul Ministerului Apărării şi Armatei Naţionale şi va coordona măsurile necesare pentru protecţia sistemelor, echipamentelor şi produselor de program împotriva ameninţărilor interne sau externe, deliberate sau accidentale, pentru a asigura că:

1. serviciile şi sistemele informatice sunt protejate împotriva accesului neautorizat;

2. confidenţialitatea informaţiilor este asigurată;

3. integritatea informaţiilor, serviciilor şi a sistemelor este păstrată;

4. disponibilitatea informaţiilor, serviciilor şi sistemelor este asigurată atunci când procesele activităţii o cer;

5. cerinţele şi obiectivele organizaţionale, precum şi cerinţele cadrului normativ în domeniul securităţii cibernetice sunt îndeplinite.

Serviciul securitate informaţională are responsabilitatea de efectuare a auditului de securitate cibernetică în cadrul SCIAN, implicând la necesitate persoane competente în domeniu. Totodată, va coordona măsurile necesare pentru efectuarea controalelor tehnice privind starea securităţii cibernetice.

Centrul comunicaţii şi informatică al Marelui Stat Major, în calitate de operator tehnic principal al Sistemului de comunicaţii şi informatică al Armatei Naţionale este entitatea responsabilă de:

1. asigurarea funcţionării stabile a SCIAN;
2. implementarea soluțiilor şi măsurilor tehnice pentru asigurarea securităţii cibernetice în cadrul SCIAN;
3. efectuarea controalelor tehnice privind starea securităţii cibernetice.

VII. Respectarea şi implementarea politicii interne privind securitatea cibernetică a instituţiei

Prevederile Politicii privind securitatea cibernetică a Ministerului Apărării şi Armatei Naţionale, a Regulamentelor de securitate informaţională şi a procedurilor elaborate se respectă şi se aplică nediscriminatoriu de către utilizatorii cărora li s-a autorizat accesul la sisteme, echipamente şi produse de program, precum şi altor persoane fizice şi juridice (consultanţi, experţi, stagiari etc.).

Fiecare utilizator autorizat al sistemelor, echipamentelor şi produselor de program poartă răspundere personală pentru aplicarea întocmai în activitatea sa a regulamentelor şi procedurilor de securitate cibernetică în vigoare, elaborate şi aprobate, conform standardelor internaţionale, legislaţiei naţionale speciale şi a reglementărilor interne de funcţionare. De asemenea, orice utilizator autorizat al sistemelor, echipamentelor şi produselor de program are obligaţia raportării oricărui incident de securitate cibernetică.

Nerespectarea Politicii interne privind securitatea cibernetică a Instituţiei atrage după sine aplicarea unor măsuri de răspundere juridică, precum şi revizuirea drepturilor de acces la sistemele informatice.

Politica internă privind securitatea cibernetică a Ministerului Apărării şi Armatei Naţionale este revizuită o dată la doi ani în vederea actualizării şi adaptării la noile condiţii şi cerinţe sau imediat după modificarea semnificativă a sistemului de management al securităţii cibernetice.