Norme privind protecţia instalaţiilor nucleare împotriva ameninţărilor cibernetice

CAPITOLUL I
Domeniu, scop, definiții

SECŢIUNEA 1

Domeniu şi scop

Art. 1. - (1) Prezentele norme sunt emise în conformitate cu prevederile Legii nr. 111/1996 privind desfășurarea în siguranţă, reglementarea, autorizarea şi controlul activităţilor nucleare, republicată, cu modificările şi completările ulterioare.

(2) Prin prezentele norme se stabilesc cerinţele generale privind protecţia sistemelor, componentelor şi echipamentelor instalaţiilor nucleare, inclusiv software-ul pentru instrumentație şi control şi rețelele informatice, denumite în continuare SCE, împotriva ameninţărilor cibernetice.

Art. 2. - (1) Îndeplinirea prevederilor prezentelor norme constituie o condiție necesară pentru autorizarea de către Comisia Națională pentru Controlul Activităţilor Nucleare, denumită în continuare CNCAN, a activităţilor de punere în funcțiune, exploatare şi dezafectare a unei instalaţii nucleare.

(2) Prevederile prezentelor norme se aplică atât solicitanților, cât şi titularilor de autorizaţie pentru fazele de punere în funcțiune, exploatare, respectiv dezafectare ale unei instalaţii nucleare. În cadrul procesului de autorizare, precum şi pe durata de valabilitate a unei autorizații, CNCAN poate impune cerințe suplimentare, după caz, pentru a ţine cont de experienţa de exploatare şi cele mai noi standarde şi bune practici recunoscute la nivel internaţional.

(3) În afara cazurilor în care se precizează altfel, cerinţele prezentelor norme sunt aplicabile tuturor organizaţiilor responsabile pentru punerea în funcțiune, exploatarea şi dezafectarea instalaţiilor nucleare.

(4) Orice derogare de la aplicarea prevederilor prezentelor norme trebuie aprobată de CNCAN şi de autoritatea națională responsabilă pentru securitate cibernetică, în baza unei justificări scrise, formulate de solicitantul sau titularul de autorizaţie, dacă acesta demonstrează că asigură măsuri de protecţie echivalente cu cele cerute prin prezentele norme.

SECŢIUNEA a 2-a

Definiții

Art. 3. - (1) Termenii utilizați în prezentele norme sunt definiți în anexa nr. 1, cu excepția acelora ale căror definiții se regăsesc în textul prezentelor norme, în Legea nr. 111/1996, republicată, cu modificările şi completările ulterioare şi în Hotărârea Guvernului nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel național privind implementarea Sistemului național de securitate cibernetică, publicată în Monitorul Oficial al României, Partea I nr. 296 din 23 mai 2013. .

(2) Autoritatea națională responsabilă pentru securitatea cibernetică este Centrul Național Cyberint, denumit în continuare CNC.

CAPITOLUL II
Cerințe generale

Art. 4. - Titularul de autorizaţie trebuie să asigure protecţia împotriva ameninţărilor cibernetice pentru următoarele categorii de sisteme, componente şi echipamente, inclusiv pentru programele software aferente acestora, denumite în continuare prin abrevierea SCE:

a) SCE cu funcţii de securitate nucleară, inclusiv SCE cu funcţii de protecţie radiologică a personalului expus profesional;

b) SCE care fac parte din sistemul de protecţie fizică;

c) SCE care fac parte din sistemul propriu de control de garanţii nucleare;

d) SCE cu funcţii în răspunsul la situaţii de urgenţă, inclusiv sistemele de comunicaţii utilizate în situaţii de urgenţă;

e) SCE cu funcţii în exploatarea fiabilă a instalaţiei nucleare;

f) alte sisteme suport care, dacă ar fi compromise, ar putea afecta funcționarea SCE din categoriile menționate la lit. a) - e) sau sănătatea și securitatea lucrătorilor; acestea pot include, de exemplu, sisteme de alimentare cu energie electrică, încălzire, ventilație și aer condiționat, comunicații, stingerea incendiilor etc.

Art. 5. - Titularul de autorizaţie trebuie să asigure protecţia SCE care fac parte din categoriile stabilite la art. 4 împotriva ameninţărilor cibernetice care ar putea avea drept consecinţe:

a) un impact advers asupra funcționării SCE;

b) un impact advers asupra integrității sau confidențialității datelor şi/sau a programelor software;

c) indisponibilitatea şi/sau limitarea accesului la sisteme, servicii şi/sau date.

Art. 6. - **(1)** Titularul de autorizaţie trebuie să analizeze toate SCE care fac parte din categoriile stabilite la art. 4 şi să identifice acele SCE care necesită protecţie împotriva ameninţărilor cibernetice, astfel încât să satisfacă cerinţele din art. 5.

(2) În vederea stabilirii unei abordări gradate privind aplicarea cerinţelor de securitate cibernetică, SCE identificate în conformitate cu cerinţele de la alin. (1) se vor clasifica în funcţie de consecinţele potențiale ale materializării ameninţărilor cibernetice.

(3) Lista SCE identificate în conformitate cu cerinţele de la alin. (1), inclusiv clasificarea acestora, stabilită conform prevederilor de la alin. (2), trebuie transmisă pentru evaluare și aprobare la CNCAN.

(4) Lista SCE trebuie revizuită şi actualizată, cel puțin o dată la 5 ani, precum și de ori câte ori este necesar, ținând cont de experienţa de exploatare, evaluările şi auditurile de securitate periodice. Reviziile listei SCE sunt supuse aprobării CNCAN.

(5) Ca urmare a auditurilor de securitate cibernetică efectuate de autoritatea națională responsabilă pentru securitatea cibernetică, solicitantul/titularul de autorizaţie are obligația de a include în lista SCE acele componente pentru care a fost identificată necesitatea protecţiei suplimentare.

Art. 7. - (1) Amenințările cibernetice care trebuie luate în considerare de titularul de autorizaţie se stabilesc de către CNCAN în cooperare cu autoritatea națională responsabilă pentru securitatea cibernetică şi se comunică în scris solicitantului/titularului de autorizaţie, prin transmiterea documentului care descrie amenințările cibernetice generice care privesc instalaţiile nucleare.

(2) Amenințările cibernetice trebuie tratate atât independent, cât și în combinație cu tipurile de amenințări specificate în Normele de protecţie fizică în domeniul nuclear, respectiv în documentele care stabilesc amenințările bază de proiect pentru sistemele de protecție fizică ale instalațiilor nucleare.

(3) Reevaluarea amenințărilor cibernetice pentru SCE ale instalaţiilor nucleare trebuie efectuată anual, precum și ori de câte ori este necesar, la inițiativa CNCAN, a CNC sau a solicitantului/titularului de autorizaţie.

CAPITOLUL III
Cerințe privind planul și procedurile de securitate cibernetică

Art. 8. - (1) Titularul de autorizaţie trebuie să stabilească, să implementeze şi să menţină un plan pentru protecţia SCE identificate în conformitate cu cerinţele art. 6 împotriva amenințărilor cibernetice, numit în continuare planul de securitate cibernetică.

(2) Planul de securitate cibernetică trebuie să aibă la bază o analiză de risc, ținând cont de amenințările cibernetice stabilite conform prevederilor art. 7.

Art. 9. - Prin implementarea planului de securitate cibernetică trebuie să se asigure:

a) implementarea controalelor necesare pentru protecţia SCE identificate în conformitate cu cerinţele art. 6;

b) implementarea şi menţinerea unei strategii de protecţie în adâncime pentru detecția, răspunsul şi recuperarea SCE în urma materializării amenințărilor cibernetice;

c) limitarea consecințelor materializării amenințărilor cibernetice şi menţinerea funcţiilor importante pentru securitatea nucleară, protecţia fizică, controlul de garanţii nucleare şi răspunsul la situaţii de urgenţă.

Art. 10. - (1) Planul de securitate cibernetică trebuie să țină cont de caracteristicile relevante ale amplasamentului şi ale proiectului instalaţiei sau instalaţiilor nucleare aflate în responsabilitatea titularului de autorizaţie.

(2) Planul de securitate cibernetică trebuie să includă măsuri de răspuns la incidente şi de recuperare în urma materializării amenințărilor cibernetice.

(3) Planul de securitate cibernetică trebuie să fie bazat pe conceptul protecției în adâncime, utilizând măsuri tehnice și administrative structurate pe mai multe niveluri, pentru protecția SCE împotriva amenințărilor cibernetice, pentru detecția incidentelor cibernetice și pentru răspunsul la astfel de evenimente.

(4) Planul de securitate cibernetică trebuie să descrie modul în care titularul de autorizaţie va asigura următoarele:

a) protecția SCE împotriva amenințărilor cibernetice;

b) menţinerea capacității pentru detecția rapidă şi răspunsul în timp util la incidente cibernetice;

c) limitarea consecințelor materializării amenințărilor cibernetice, astfel încât funcțiile sistemelor identificate conform cerințelor art. 6 să nu fie afectate negativ;

d) corectarea vulnerabilităților exploatate în atacurile cibernetice;

e) recuperarea / repunerea în funcțiune a SCE afectate de incidentele cibernetice.

Art. 11. - (1) Titularul de autorizaţie trebuie să asigure, ca parte a planului de securitate cibernetică, următoarele:

a) pregătirea personalului propriu şi a contractorilor cu privire la cunoaşterea, aplicarea şi respectarea cerinţelor de securitate cibernetică, pentru toate etapele ciclului de viață al SCE, începând cu etapa de proiectare, în funcţie de sarcinile şi responsabilităţile stabilite;

b) evaluarea şi gestionarea riscurilor asociate cu amenințările cibernetice;

c) evaluarea modificărilor care afectează SCE identificate conform cerinţelor art. 6, în scopul menţinerii unei protecții adecvate împotriva amenințărilor cibernetice.

(2) Pentru implementarea eficientă a planului de securitate cibernetică, titularul de autorizație trebuie să ia următoarele acțiuni:

a) să stabilească și să implementeze obiectivele și politica de securitate cibernetică la nivelul întregii organizații;

b) să dezvolte şi să menţină măsurile tehnice și administrative necesare pentru punerea în aplicare a planului de securitate cibernetică, inclusiv un set de proceduri scrise;

c) să dezvolte și să implementeze o cultură de securitate cibernetică pentru a asigura conștientizarea, la nivel de organizație a amenințărilor cibernetice și a riscurilor asociate, precum și cunoașterea și aplicarea măsurilor de prevenție, detecție și răspuns la condiții anormale și evenimente de securitate cibernetică.

Art. 12. - (1) Titularul de autorizaţie trebuie să aibă în permanență o echipă proprie de specialiști care să asigure detecția şi răspunsul rapid la un incident de securitate cibernetică, inclusiv protecţia SCE identificate în conformitate cu cerinţele art. 6 şi limitarea consecințelor materializării amenințărilor cibernetice.

(2) Titularul de autorizaţie trebuie să dezvolte și să implementeze o procedură de detecție și răspuns la incidente cibernetice, care să specifice următoarele aspecte:

a) componența echipei de investigare și răspuns; cerințele de pregătire profesională inițială și continuă și cerințele de calificare pentru personalul desemnat să facă parte din această echipă;

b) condițiile considerate incidente de securitate cibernetică;

c) analiza și urmărirea condițiilor anormale pentru a facilita detecția în timp util a potențialelor incidente de securitate cibernetică și a precursorilor pentru astfel de evenimente;

d) investigarea incidentelor de securitate cibernetică;

e) acțiunile de răspuns stabilite pentru a asigura protecția SCE;

f) notificările către autoritățile naționale și obținerea de suport tehnic extern atunci când este necesar.

Art. 13. - (1) Titularul de autorizaţie trebuie să implementeze măsuri pentru colectarea, evaluarea şi utilizarea experienţei de exploatare interne şi externe, în vederea îmbunătăţirii continue a protecţiei împotriva ameninţărilor cibernetice, respectiv a planului de securitate cibernetică.

(2) În scopul implementării cerinței de la alin. (1), trebuie stabilite, consultate și analizate periodic, cel puțin săptămânal, sursele de informații și experiență de exploatare disponibile, la nivel național și internațional, care prezintă cele mai recente vulnerabilități identificate în diferitele componente și echipamente ale sistemelor de control industrial, relevante pentru SCE din cadrul instalației nucleare, identificate în conformitate cu cerinţele art. 6, precum și cele mai recente incidente și atacuri cibernetice cunoscute. Titularul de autorizaţie trebuie să elaboreze și să implementeze o procedură specifică în acest scop.

Art. 14. - (1) Titularul de autorizaţie trebuie să asigure evaluarea periodică a eficacității planului de securitate cibernetică. În acest scop, trebuie desemnată o echipă de specialiști în securitate cibernetică, cu pregătire, experiență și calificări adecvate pentru specificul instalației nucleare și a SCE aferente acesteia.

(2) Evaluarea eficacității planului de securitate cibernetică trebuie efectuată:

a) cel puţin o dată pe an;

b) după fiecare eveniment relevant pentru securitatea cibernetică, din experienţa de exploatare internă sau externă.

(3) Evaluarea eficacității planului de securitate cibernetică trebuie să includă exerciții periodice de testare a măsurilor de protecţie împotriva ameninţărilor cibernetice.

(4) Titularul de autorizaţie trebuie să confirme, prin verificare și validare, că măsurile și procedurile specifice implementate îndeplinesc cerințele de protecție împotriva amenințărilor cibernetice.

Art. 15. - (1) Titularul de autorizaţie trebuie să demonstreze că a implementat toate măsurile necesare, la nivelul celor mai noi standarde şi bune practici recunoscute la nivel internaţional, pentru asigurarea protecţiei instalaţiilor nucleare împotriva ameninţărilor cibernetice.

(2) Documentele de referinţă menționate în anexa nr. 2 reprezintă standarde şi ghiduri privind bune practici recunoscute pe plan național şi internaţional şi se recomandă ca acestea, precum și orice nouă revizie a acestora, să fie luate în considerare de către titularul de autorizaţie, în vederea îmbunătăţirii protecţiei instalaţiilor nucleare împotriva ameninţărilor cibernetice.

(3) Titularul de autorizaţie trebuie să utilizeze standardele și ghidurile tehnice menționate în anexa nr. 2, relevante pentru instalațiile nucleare pentru care este responsabil, în procesul de auto-evaluare. Rapoartele privind auto-evaluarea față de cerințele și recomandările din aceste standarde și ghiduri trebuie transmise la CNCAN pentru informare.

(4) Titularul de autorizaţie trebuie să utilizeze standardele și ghidurile tehnice menționate în anexa nr. 2, relevante pentru instalațiile nucleare pentru care este responsabil, în pregătirea personalului de specialitate implicat în dezvoltarea, evaluarea, implementarea și îmbunătățirea

continuă a planului, procedurilor și măsurilor tehnice și administrative de securitate cibernetică.

Art. 16. - Măsurile de protecţie împotriva ameninţărilor cibernetice trebuie implementate astfel încât să nu producă efecte adverse asupra funcţionării SCE conform cerinţelor şi intenţiei de proiectare.

Art. 17. - **(1)** Titularul de autorizaţie trebuie să stabilească şi să impună un set de cerinţe şi reguli de securitate cibernetică pentru furnizorii de produse şi servicii pentru instalaţiile nucleare, în scopul prevenirii incidentelor cibernetice. Titularul de autorizaţie trebuie să asigure, prin procedurile proprii, includerea cerinţelor de securitate cibernetică în documentaţia de procurare pentru furnizorii de produse şi servicii pentru instalaţiile nucleare.

(2) Cerinţele pentru SCE noi din categoria celor identificate conform cu cerinţele art. 6, precum și pentru modernizările SCE existente, trebuie să includă remedierea vulnerabilităților pentru toată durata de viață a SCE respective.

(3) Titularul de autorizaţie trebuie să asigure procurarea de componente şi piese de schimb pentru SCE identificate conform cu cerinţele art. 6 direct de la producătorii/fabricanții originali ai acestora sau de la furnizorii agreați de aceștia, în măsura în care este practic posibil, pentru menţinerea proiectului aprobat/autorizat, în conformitate cu cerinţele privind controlul configurației de proiectare, pentru evitarea modificărilor inadvertente, precum şi pentru evitarea produselor contrafăcute, frauduloase sau suspecte, inclusiv a celor care pot induce vulnerabilităţi de securitate cibernetică.

(4) Titularul de autorizaţie trebuie să stabilească și să implementeze proceduri de acces și control pentru furnizorii de servicii cu impact asupra SCE din categoria celor identificate conform cu cerinţele art. 6, în vederea asigurării securității cibernetice.

Art. 18. - **(1)** Titularul de autorizație trebuie să asigure analiza și evaluarea modificărilor permanente și temporare din punct de vedere al impactului asupra protecției la amenințări cibernetice. Această cerință se aplică atât modificărilor de proiect care privesc SCE din categoria celor identificate conform cu cerinţele art. 6, cât și modificărilor administrative și procedurale relevante.

(2) Titularul de autorizație trebuie să stabilească, în procedurile proprii, cerințele pentru implementarea uniformă a prevederilor din art. 16 și art. 17 alin. (2), la evaluarea și implementarea modificărilor de proiect permanente și temporare.

Art. 19. - Titularul de autorizație trebuie să stabilească și să implementeze proceduri pentru identificarea și controlul, din punct de vedere al protecției la amenințări cibernetice, precum și din punct de vedere al protecției fizice, al echipamentelor portabile, inclusiv al mediilor de stocare de date, care se conectează la SCE ale instalației nucleare pentru activități de monitorizare, supraveghere, testare, diagnoză, actualizare software, inspecție etc., în care să se prevadă cerințele și măsurile preventive de securitate cibernetică, inclusiv auditurile periodice pentru verificarea conformității cu aceste cerințe și măsuri.

CAPITOLUL IV
Cerințe privind integrarea în sistemul de management, documentația, înregistrările şi raportarea

Art. 20. – (1) Titularul de autorizație trebuie să definească și să documenteze, ca proces suport în cadrul sistemului de management, procesul pentru protecţia instalaţiilor nucleare împotriva amenințărilor cibernetice, astfel încât să asigure sustenabilitatea pe termen lung a conformității cu cerințele de reglementare naționale și standardele internaționale în acest domeniu, precum și îmbunătățirea continuă a securității cibernetice.

(2) Titularul de autorizație trebuie să stabilească responsabilitățile pentru dezvoltarea, monitorizarea, implementarea, evaluarea și îmbunătățirea continuă a procesului și măsurilor de securitate cibernetică.

(3) Titularul de autorizație trebuie să asigure coordonarea diferitelor departamente responsabile pentru implementarea procesului și măsurilor de securitate cibernetică, precum și integrarea acțiunilor implementate de acestea.

(4) Titularul de autorizație trebuie să asigure resursele materiale și resursele umane, de personal tehnic pregătit și calificat în domeniul securității cibernetice pentru SCE specifice instalațiilor nucleare, inclusiv pentru sistemele de control industrial.

Art. 21. - Titularul de autorizaţie trebuie să păstreze toate înregistrările şi documentaţia tehnică suport pentru demonstrarea conformităţii cu cerinţele prezentelor norme pentru toată durata de viață a instalaţiei nucleare.

Art. 22. - **(1)** Titularul de autorizaţie trebuie să raporteze imediat la CNCAN orice condiție anormală cu impact asupra securităţii cibernetice a SCE identificate în conformitate cu cerinţele art. 6, inclusiv incidentele cibernetice.

(2) Orice incident de securitate cibernetică cu impact asupra SCE trebuie comunicat la CNC în maximum 12 ore de la constatarea acestuia.

CAPITOLUL V
Dispoziţii tranzitorii şi finale

Art. 23. - **(1)** În termen de un an de la intrarea în vigoare a prezentelor norme, titularii de autorizaţie pentru instalaţiile nucleare aflate în faza de exploatare trebuie să transmită la CNCAN spre evaluare un raport care să prezinte analiza conformităţii cu cerinţele prezentelor norme şi acţiunile întreprinse pentru asigurarea implementării integrale a cerinţelor.

(2) În termen de un an de la intrarea în vigoare a prezentelor norme, titularii de autorizaţie pentru instalaţiile nucleare aflate în faza de exploatare trebuie să transmită la CNCAN, spre evaluare şi avizare, actualizarea planului de securitate cibernetică pentru instalaţiile nucleare de care răspund, prin care să demonstreze:

a) conformitatea cu cerinţele prezentelor norme;

b) alinierea la recomandările din documentele de referinţă menționate în anexa nr. 2;

c) implementarea măsurilor de protecţie împotriva ameninţărilor cibernetice comunicate de CNCAN în cooperare cu CNC, în conformitate cu prevederile de la art. 7.

(3) Actualizarea planului de securitate cibernetică trebuie să includă măsurile de implementare şi termenele aferente.

(4) Conținutul minim recomandat al planului de securitate cibernetică este cel din anexa nr. 3.

Art. 24. - Anexele nr. 1, 2 şi 3 fac parte integrantă din prezentele norme.

ANEXA Nr. 1
la norme

Definiţii

amenințare cibernetică - circumstanță sau eveniment care constituie un pericol potențial la adresa securităţii cibernetice;

atac cibernetic - acţiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică;

funcţie de securitate nucleară - un scop specific care trebuie îndeplinit pentru asigurarea securităţii nucleare; funcţiile generale de securitate nucleară sunt următoarele:

a) controlul reactivităţii; pentru un reactor nuclear, această funcţie include atât reducerea puterii, oprirea reactorului şi menţinerea acestuia într-o stare de oprire sigură pentru o perioadă de timp nedeterminată, cât şi prevenirea criticităţii în instalaţiile de depozitare a combustibilului nuclear uzat;

b) răcirea combustibilului nuclear; pentru un reactor nuclear, această funcţie se referă atât la răcirea combustibilului din reactor, cât şi la răcirea combustibilului uzat din instalaţiile de depozitare aferente;

c) reţinerea materialelor radioactive, inclusiv menţinerea barierelor fizice în calea eliberării acestora în mediul înconjurător;

d) monitorizarea stării instalaţiei nucleare şi furnizarea serviciilor-suport necesare pentru menţinerea funcţiilor prevăzute la lit. a)-c); serviciile-suport menționate includ furnizarea de energie electrică, agent de răcire, aer instrumental, gaze și alte fluide tehnice, după cum este necesar pentru buna funcţionare a sistemelor, structurilor, componentelor și echipamentelor cu funcţii de securitate nucleară.

incident cibernetic - eveniment survenit în spațiul cibernetic ale cărui consecinţe afectează securitatea cibernetică;

infrastructuri cibernetice - infrastructuri de tehnologia informației şi comunicații, constând în sisteme informatice, aplicații aferente, rețele şi servicii de comunicații electronice;

securitate cibernetică - starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spațiul cibernetic. Măsurile proactive şi reactive pot include politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi

de instruire şi conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor;

SCE - sistemele, componentele şi echipamentele instalaţiei nucleare;

SCE cu funcţii de securitate nucleară - sunt acele SCE care contribuie, direct sau indirect, în condiţii de operare normală, în cazul evenimentelor anticipate în exploatare şi/sau în condiţii de accident, la îndeplinirea funcţiilor generale de securitate nucleară; acestea includ SCE a căror defectare poate avea un impact advers asupra îndeplinirii unei funcţii de securitate nucleară; de asemenea, sunt incluse SCE utilizate pentru răspunsul la condiții de extindere a bazelor de proiectare.

SCE cu funcţii în exploatarea fiabilă a instalaţiei nucleare - acele SCE care asigură funcționarea instalaţiei nucleare în bune condiţii, la parametrii nominali şi a căror defectare poate cauza condiţii de operare anormală, tranzienţi, opriri neplanificate şi/sau acţionarea intempestivă a sistemelor cu funcţii de securitate nucleară; aceste SCE contribuie la implementarea primului nivel de protecţie în adâncime pentru asigurarea securităţii nucleare, respectiv la prevenirea defectărilor şi a condiţiilor de operare anormală.

ANEXA Nr. 2
la norme

Documente de referinţă

1. Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T(Rev.1), International Atomic Energy Agency, Vienna, 2021

2. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Revision 5, IAEA Nuclear Security Series 13, International Atomic Energy Agency, Vienna, 2011

3. Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, International Atomic Energy Agency, Vienna, 2018

4. Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series NR-T-3.30, International Atomic Energy Agency, Vienna, 2020

5. Conducting Computer Security Assessments at Nuclear Facilities, IAEA-TDL-006, International Atomic Energy Agency, Vienna, 2016

6. Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, International Atomic Energy Agency, Vienna, 2021

7. Computer Security Incident Response Planning at Nuclear Facilities, IAEA-TDL-005, International Atomic Energy Agency, Vienna, 2016

8. IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2016, Institute of Electrical and Electronics Engineers, 2016

9. IEC 62645:2019 Nuclear power plants – Instrumentation, control and electrical power systems - Cybersecurity requirements, International Electrotechnical Commission, 2019

10. CSA N290.7-14 (R2021), Cyber Security for Nuclear Power Plants and Small Reactor Facilities, Canadian Standards Association, 2014

11. ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements, International Organization for Standardization, 2013

12. ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls, International Organization for Standardization, 2013

13. NEI 08-09 [Rev. 6] Cyber Security Plan for Nuclear Power Reactors, Nuclear Energy Institute, 2010

14. Cybersecurity Capability Maturity Model (C2M2 Version 2.0), United States Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response, SUA, 2021

ANEXA Nr. 3
la norme

Conţinutul minim al planului de securitate cibernetică pentru o instalaţie nucleară

Secţiunea 1 - Organizare şi responsabilităţi

1.1. Scheme organizatorice, inclusiv organigrama organizaţiei titularului de autorizaţie şi a departamentului sau departamentelor cu responsabilităţi pentru securitatea cibernetică a instalaţiilor nucleare;

1.2. Persoanele cu responsabilităţi şi autoritate pentru securitatea cibernetică a instalaţiilor nucleare; responsabilităţi pentru elaborare, raportare, avizare şi aprobare a procedurilor şi documentelor aferente;

1.3. Procesul de elaborare, revizie periodică şi aprobare a procedurilor şi documentelor aferente;

1.4. Politica de securitate cibernetică la nivelul organizației.

Secţiunea 2 - Inventarul SCE relevante pentru securitatea cibernetică a instalaţiilor nucleare

2.1. Lista SCE a căror funcţionare depinde de computere şi programe software;

2.2. Lista tuturor aplicaţiilor şi programelor software;

2.3. Diagramele reţelelor informatice, inclusiv toate conexiunile către sisteme informatice externe, care nu sunt sub controlul titularului de autorizaţie;

2.4. Lista echipamentelor portabile, inclusiv a mediilor de stocare de date, care se conectează la SCE importante pentru securitatea cibernetică;

2.5. Analiza, pentru fiecare SCE sau categorie de SCE importante pentru securitatea cibernetică, a mecanismelor și modurilor de defectare relevante din punct de vedere al securității cibernetice, a efectelor acestora și a măsurilor tehnice și administrative specifice de prevenire, detecție și răspuns la incidente cibernetice;

2.6. Metodologia folosită pentru identificarea și clasificarea SCE relevante pentru securitatea cibernetică a instalațiilor nucleare.

Secţiunea 3 - Analiza riscurilor, vulnerabilităţilor şi a conformităţii cu cerinţele aplicabile

3.1. Periodicitatea reevaluării şi revizuirii planului de securitate cibernetică;

3.2. Autoevaluarea eficacităţii planului şi măsurilor de securitate cibernetică, inclusiv testele de penetrare;

3.3. Procedurile de audit şi de identificare, urmărire şi corectare a neconformităţilor;

3.4. Conformitatea cu cerinţele din legislaţia naţională şi din standardele internaţionale aplicabile;

3.5. Echipa desemnată pentru evaluarea securității cibernetice.

Secţiunea 4 - Proiectarea sistemului de securitate cibernetică şi controlul configuraţiei

4.1. Principiile de proiectare şi arhitectura de bază a sistemului de securitate cibernetică; nivelurile de securitate cibernetică; descrierea modului în care s-a implementat conceptul de protecție în adâncime;

4.2. Cerinţele pentru fiecare nivel de securitate cibernetică;

4.3. Stabilirea cerinţelor de securitate cibernetică pentru furnizorii de produse şi servicii destinate instalaţiilor nucleare;

4.4. Asigurarea securităţii cibernetice pentru tot ciclul de viaţă a SCE;

4.5. Infrastructura sistemului de protecție antivirus și criteriile de acces pentru personalul responsabil;

4.6. Măsurile de verificare a integrității SCE, inclusiv a programelor software, pentru asigurarea controlului configurației.

Secţiunea 5 - Procedurile operaţionale de securitate cibernetică

5.1. Controlul accesului la SCE; controlul echipamentelor portabile și a mediilor de stocare de date;

5.2. Protecţia datelor;

5.3. Protecţia comunicaţiilor;

5.4. Protecţia platformelor şi aplicaţiilor informatice;

5.5. Supravegherea/Monitorizarea sistemelor; controlul configurației; identificarea și detecția condițiilor anormale, vulnerabilităților și incidentelor cibernetice;

5.6. Activităţile de întreţinere necesare pentru SCE a căror funcţionare depinde de computere şi programe software;

5.7. Managementul incidentelor/Răspunsul la incidente cibernetice; echipa desemnată pentru răspunsul la incidente cibernetice;

5.8. Asigurarea continuităţii funcţiilor de securitate şi siguranţă nucleară;

5.9. Măsuri pentru salvarea datelor - system backup - în caz de incident cibernetic;

5.10. Achiziţia şi transferul de SCE;

5.11. Eliminarea din sistem a SCE.

Secţiunea 6 - Managementul personalului

6.1. Verificarea/Avizarea personalului;

6.2. Pregătirea personalului;

6.3. Calificarea personalului;

6.4. Terminarea accesului şi transferul personalului.