



MONITORUL OFICIAL

AL

ROMÂNIEI

Anul 189 (XXXIII) — Nr. 1217

PARTEA I
LEGI, DECRETE, HOTĂRĂRI ȘI ALTE ACTE

Miercuri, 22 decembrie 2021

SUMAR

Nr.	Pagina	Nr.	Pagina
DECIZII ALE CURȚII CONSTITUȚIONALE			
Decizia nr. 595 din 30 septembrie 2021 referitoare la excepția de neconstituționalitate a dispozițiilor art. 475 din Codul de procedură penală și a sintagmei „ <i>bunuri sau alte valori</i> ” cuprinse în art. 82 lit. j) din Legea nr. 254/2013 privind executarea pedepselor și a măsurilor privative de libertate dispuse de organele judiciare în cursul procesului penal	2-4		
ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE			
165. — Ordin al președintelui Autorității Naționale Sanitare Veterinare și pentru Siguranța Alimentelor privind modificarea Ordinului președintelui Autorității Naționale Sanitare Veterinare și pentru Siguranța Alimentelor nr. 64/2007 pentru aprobarea Normei sanitare veterinare privind organizarea și desfășurarea activității de control oficial sanitar-veterinar efectuat de către personalul de specialitate în unitățile care produc alimente de origine animală	5		
203. — Ordin al președintelui Comisiei Naționale pentru Controlul Activităților Nucleare pentru aprobarea Normelor privind protecția instalațiilor nucleare împotriva amenințărilor cibernetice	6-11		
1.889. — Ordin al ministrului dezvoltării, lucrărilor publice și administrației privind modificarea anexei nr. 1 la Ordinul ministrului lucrărilor publice, dezvoltării și administrației nr. 2.154/2020 pentru aprobarea		Programului național multianual privind creșterea performanței energetice a blocurilor de locuințe cu finanțare în perioada 2020—2022	12
		1.890. — Ordin al ministrului dezvoltării, lucrărilor publice și administrației privind modificarea anexei nr. 1 la Ordinul viceprim-ministrului, ministrul dezvoltării regionale și administrației publice, nr. 2.088/2019 pentru aprobarea Programului național multianual privind creșterea performanței energetice a blocurilor de locuințe cu finanțare în perioada 2019—2021	13-14
		1.894. — Ordin al ministrului dezvoltării, lucrărilor publice și administrației privind modificarea anexei nr. 1 la Ordinul ministrului dezvoltării, lucrărilor publice și administrației nr. 664/2021 pentru aprobarea Programului național multianual privind creșterea performanței energetice a blocurilor de locuințe cu finanțare în perioada 2021—2023	14-15
		2.780. — Ordin al ministrului sănătății pentru abrogarea Ordinului ministrului sănătății nr. 414/2020 privind instituirea măsurii de carantină pentru persoanele aflate în situația de urgență de sănătate publică internațională determinată de infecția cu COVID-19 și stabilirea unor măsuri în vederea prevenirii și limitării efectelor epidemiei	16

GUVERNUL ROMÂNIEI
COMISIA NAȚIONALĂ PENTRU CONTROLUL ACTIVITĂȚILOR NUCLEARE

ORDIN
pentru aprobarea Normelor privind protecția instalațiilor nucleare
împotriva amenințărilor cibernetice

În conformitate cu prevederile art. 9 alin. (7) din Hotărârea Guvernului nr. 729/2018 privind organizarea și funcționarea Comisiei Naționale pentru Controlul Activităților Nucleare, având în vedere prevederile art. 5 alin. (1) și ale art. 35 lit. a) din Legea nr. 111/1996 privind desfășurarea în siguranță, reglementarea, autorizarea și controlul activităților nucleare, republicată, cu modificările și completările ulterioare, luând în considerare Referatul nr. 15.823 din 6.12.2021,

președintele Comisiei Naționale pentru Controlul Activităților Nucleare emite următorul ordin:

Art. 1. — Se aprobă Normele privind protecția instalațiilor nucleare împotriva amenințărilor cibernetice, prevăzute în anexa care face parte integrantă din prezentul ordin.

Art. 2. — La data intrării în vigoare a prezentului ordin se abrogă Ordinul președintelui Comisiei Naționale pentru Controlul Activităților Nucleare nr. 181/2014 pentru aprobarea

Normelor privind protecția instalațiilor nucleare împotriva amenințărilor cibernetice, publicat în Monitorul Oficial al României, Partea I, nr. 803 din 4 noiembrie 2014.

Art. 3. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Președintele Comisiei Naționale pentru Controlul Activităților Nucleare,
Cantemir Ciurea-Ercău

București, 7 decembrie 2021.
Nr. 203.

ANEXĂ

NORME
privind protecția instalațiilor nucleare împotriva amenințărilor cibernetice

CAPITOLUL I
Domeniu, scop, definiții

SECȚIUNEA 1
Domeniu și scop

Art. 1. — (1) Prezentele norme sunt emise în conformitate cu prevederile Legii nr. 111/1996 privind desfășurarea în siguranță, reglementarea, autorizarea și controlul activităților nucleare, republicată, cu modificările și completările ulterioare.

(2) Prin prezentele norme se stabilesc cerințele generale privind protecția sistemelor, componentelor și echipamentelor instalațiilor nucleare, inclusiv software-ul pentru instrumentație și control și rețelele informatice, denumite în continuare *SCE*, împotriva amenințărilor cibernetice.

Art. 2. — (1) Îndeplinirea prevederilor prezentelor norme constituie o condiție necesară pentru autorizarea de către Comisia Națională pentru Controlul Activităților Nucleare, denumită în continuare *CNCAN*, a activităților de punere în funcțiune, exploatare și dezafectare a unei instalații nucleare.

(2) Prevederile prezentelor norme se aplică atât solicitanților, cât și titularilor de autorizație pentru fazele de punere în funcțiune, exploatare, respectiv dezafectare a unei instalații nucleare. În cadrul procesului de autorizare, precum și pe durata de valabilitate a unei autorizații, *CNCAN* poate impune cerințe suplimentare, după caz, pentru a ține cont de experiența de exploatare și cele mai noi standarde și bune practici recunoscute la nivel internațional.

(3) În afara cazurilor în care se precizează altfel, cerințele prezentelor norme sunt aplicabile tuturor organizațiilor responsabile pentru punerea în funcțiune, exploatarea și dezafectarea instalațiilor nucleare.

(4) Orice derogare de la aplicarea prevederilor prezentelor norme trebuie aprobată de *CNCAN*, în baza unei justificări scrise, formulate de solicitantul sau titularul de autorizație, dacă acesta demonstrează că asigură măsuri de protecție echivalente cu cele cerute prin prezentele norme.

SECȚIUNEA a 2-a
Definiții

Art. 3. — Termenii utilizați în prezentele norme sunt definiți în anexa nr. 1, cu excepția acelor ale căror definiții se regăsesc în textul prezentelor norme și în Legea nr. 111/1996, republicată, cu modificările și completările ulterioare.

CAPITOLUL II
Cerințe generale

Art. 4. — Titularul de autorizație trebuie să asigure protecția împotriva amenințărilor cibernetice pentru următoarele categorii de sisteme, componente și echipamente, inclusiv pentru programele software aferente acestora, denumite în continuare prin abrevierea *SCE*:

a) *SCE* cu funcții de securitate nucleară, inclusiv *SCE* cu funcții de securitate radiologică;

- b) SCE care fac parte din sistemul de protecție fizică;
- c) SCE care fac parte din sistemul propriu de control de garanții nucleare;
- d) SCE cu funcții în răspunsul la situații de urgență, inclusiv sistemele de comunicații utilizate în situații de urgență;
- e) SCE cu funcții în exploatarea fiabilă a instalației 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 autorizație trebuie să asigure protecția SCE care fac parte din categoriile stabilite la art. 4 împotriva amenințărilor cibernetice care ar putea avea drept consecințe:

- a) un impact advers asupra funcționării SCE;
- b) un impact advers asupra integrității sau confidențialității datelor și/sau a programelor software;
- c) indisponibilitatea și/sau limitarea accesului la sisteme, servicii și/sau date.

Art. 6. — (1) Titularul de autorizație trebuie să analizeze toate SCE care fac parte din categoriile stabilite la art. 4 și să identifice acele SCE care necesită protecție împotriva amenințărilor cibernetice, astfel încât să satisfacă cerințele din art. 5.

(2) În vederea stabilirii unei abordări gradate privind aplicarea cerințelor de securitate cibernetică, SCE identificate în conformitate cu cerințele de la alin. (1) se vor clasifica în funcție de consecințele potențiale ale materializării amenințărilor cibernetice.

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

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

Art. 7. — (1) Amenințările cibernetice care trebuie luate în considerare de titularul de autorizație se stabilesc de către CNCAN în cooperare cu autoritățile naționale responsabile pentru securitatea cibernetică și se comunică în scris solicitantului/titularului de autorizație, prin transmiterea documentului care descrie amenințările cibernetice generice care privesc instalațiile nucleare.

(2) Amenințările cibernetice trebuie tratate atât independent, cât și în combinație cu tipurile de amenințări specificate în Normele de protecție 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 instalațiilor nucleare trebuie efectuată anual, precum și ori de câte ori este necesar, la inițiativa CNCAN, a autorităților naționale responsabile pentru securitatea cibernetică sau a solicitantului/titularului de autorizație.

CAPITOLUL III

Cerințe privind planul și procedurile de securitate cibernetică

Art. 8. — (1) Titularul de autorizație trebuie să stabilească, să implementeze și să mențină un plan pentru protecția SCE identificate în conformitate cu cerințele art. 6 împotriva amenințărilor cibernetice, denumit 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 protecția SCE identificate în conformitate cu cerințele art. 6;
- b) implementarea și menținerea unei strategii de protecție în adâncime pentru detecția, răspunsul și recuperarea SCE în urma materializării amenințărilor cibernetice;
- c) limitarea consecințelor materializării amenințărilor cibernetice și menținerea funcțiilor importante pentru securitatea nucleară, protecția fizică, controlul de garanții nucleare și răspunsul la situații de urgență.

Art. 10. — (1) Planul de securitate cibernetică trebuie să țină cont de caracteristicile relevante ale amplasamentului și ale proiectului instalației sau instalațiilor nucleare aflate în responsabilitatea titularului de autorizație.

(2) Planul de securitate cibernetică trebuie să includă măsuri de răspuns la incidente și 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 autorizație va asigura următoarele:

- a) protecția SCE împotriva amenințărilor cibernetice;
- b) menținerea capacității pentru detecția rapidă și 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 autorizație trebuie să asigure, ca parte a planului de securitate cibernetică, următoarele:

- a) pregătirea personalului propriu și a contractorilor cu privire la cunoașterea, aplicarea și respectarea cerințelor de securitate cibernetică, pentru toate etapele ciclului de viață al SCE, începând cu etapa de proiectare, în funcție de sarcinile și responsabilitățile stabilite;
- b) evaluarea și gestionarea riscurilor asociate cu amenințările cibernetice;
- c) evaluarea modificărilor care afectează SCE identificate conform cerințelor art. 6, în scopul menținerii unei protecții adecvate împotriva amenințărilor cibernetice.

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

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

b) să dezvolte și să mențină 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 cibernetică 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 autorizație trebuie să aibă în permanență o echipă proprie de specialiști care să asigure detecția și răspunsul rapid la un incident de securitate cibernetică, inclusiv protecția SCE identificate în conformitate cu cerințele art. 6 și limitarea consecințelor materializării amenințărilor cibernetică.

(2) Titularul de autorizație trebuie să dezvolte și să implementeze o procedură de detecție și răspuns la incidente cibernetică, 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 unor 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 autorizație trebuie să implementeze măsuri pentru colectarea, evaluarea și utilizarea experienței de exploatare interne și externe, în vederea îmbunătățirii continue a protecției împotriva amenințărilor cibernetică, respectiv a planului de securitate cibernetică.

(2) În scopul implementării cerinței de la alin. (1) trebuie stabilite, consultate și analizate în mod continuu 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 cerințele art. 6, precum și cele mai recente incidente și atacuri cibernetică cunoscute. Titularul de autorizație trebuie să elaboreze și să implementeze o procedură specifică în acest scop.

Art. 14. — (1) Titularul de autorizație trebuie să asigure evaluarea periodică a eficacității planului de securitate cibernetică. În acest scop, trebuie constituită și 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 puțin o dată pe an;

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

(3) Evaluarea eficacității planului de securitate cibernetică trebuie să includă exerciții periodice, de testare a măsurilor de protecție împotriva amenințărilor cibernetică, ținând cont și de specificul SCE.

(4) Titularul de autorizație trebuie să confirme, prin verificare și validare, că măsurile și procedurile specifice implementate îndeplinesc cerințele de protecție împotriva amenințărilor cibernetică, ținând cont și de specificul SCE.

Art. 15. — (1) Titularul de autorizație trebuie să demonstreze că a implementat toate măsurile necesare, la nivelul celor mai noi standarde și bune practici recunoscute la nivel internațional, pentru asigurarea protecției instalațiilor nucleare împotriva amenințărilor cibernetică.

(2) Documentele de referință menționate în anexa nr. 2 reprezintă standarde și ghiduri privind bune practici recunoscute pe plan național și internațional și se recomandă ca acestea, precum și orice nouă revizie a acestora să fie luate în considerare de către titularul de autorizație, în vederea îmbunătățirii protecției instalațiilor nucleare împotriva amenințărilor cibernetică.

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

(4) Titularul de autorizație trebuie să utilizeze standardele și ghidurile tehnice menționate în anexa nr. 2, relevante pentru instalațiile nucleare pentru care este responsabil, în pregătirea și calificarea 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 protecție împotriva amenințărilor cibernetică trebuie implementate astfel încât să nu producă efecte adverse asupra funcționării SCE conform cerințelor și intenției de proiectare.

Art. 17. — (1) Titularul de autorizație trebuie să stabilească și să impună un set de cerințe și reguli de securitate cibernetică pentru furnizorii de produse și servicii pentru instalațiile nucleare, în scopul prevenirii incidentelor cibernetică. Titularul de autorizație trebuie să asigure, prin procedurile proprii, includerea cerințelor de securitate cibernetică în documentația de procurare pentru furnizorii de produse și servicii pentru instalațiile nucleare.

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

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

(4) Titularul de autorizație 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 cerințele art. 6, în vederea asigurării securității cibernetice.

Art. 18. — (1) Titularul de autorizație trebuie să asigure analiza și evaluarea modificărilor permanente și temporare din punctul 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 cerințelor 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 punctul de vedere al protecției la amenințări cibernetice, precum și din punctul 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 și raportarea

Art. 20. — (1) Titularul de autorizație trebuie să definească și să documenteze, ca proces-suport în cadrul sistemului de management, procesul pentru protecția instalațiilor 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 autorizație trebuie să păstreze toate înregistrările și documentația tehnică-suport pentru demonstrarea conformității cu cerințele prezentelor norme pentru toată durata de viață a instalației nucleare.

Art. 22. — (1) Titularul de autorizație trebuie să raporteze imediat la CNCAN orice condiție anormală cu impact real sau potențial asupra securității cibernetice a SCE identificate în conformitate cu cerințele art. 6, inclusiv incidentele cibernetice.

(2) De asemenea, titularul de autorizație trebuie să raporteze imediat la CNCAN orice incident de securitate cibernetică în care sunt accesate neautorizat sau afectate în orice alt mod bazele de date sau rețeaua de intranet în care sunt stocate informații privind SSCE ale instalației nucleare, procedurile tehnice și administrative și date privind angajații titularului de autorizație.

CAPITOLUL V

Dispoziții tranzitorii și finale

Art. 23. — (1) În termen de un an de la intrarea în vigoare a prezentelor norme, titularii de autorizație pentru instalațiile nucleare aflate în faza de exploatare trebuie să transmită la CNCAN spre evaluare un raport care să prezinte analiza conformității cu cerințele prezentelor norme și acțiunile întreprinse pentru asigurarea implementării integrale a cerințelor.

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

a) conformitatea cu cerințele prezentelor norme;

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

c) implementarea măsurilor de protecție împotriva amenințărilor cibernetice comunicate de CNCAN în cooperare cu autoritățile naționale în domeniul securității cibernetice, în conformitate cu prevederile de la art. 7.

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

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

Art. 24. — Anexele nr. 1—3 fac parte integrantă din prezentele norme.

*ANEXA Nr. 1
la norme*

DEFINIȚII

Amenințare cibernetică — circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice

Atac cibernetic — acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică

Funcție de securitate nucleară — un scop specific care trebuie îndeplinit pentru asigurarea securității nucleare; funcțiile generale de securitate nucleară sunt următoarele:

a) controlul reactivității; pentru un reactor nuclear, această funcție include atât reducerea puterii, oprirea reactorului și menținerea acestuia într-o stare de oprire sigură pentru o perioadă de timp nedeterminată, cât și prevenirea criticității în instalațiile de depozitare a combustibilului nuclear uzat;

b) răcirea combustibilului nuclear; pentru un reactor nuclear, această funcție se referă atât la răcirea combustibilului din

reactor, cât și la răcirea combustibilului uzat din instalațiile de depozitare aferente;

c) reținerea materialelor radioactive, inclusiv menținerea barierelor fizice în calea eliberării acestora în mediul înconjurător;

d) monitorizarea stării instalației nucleare și furnizarea serviciilor-suport necesare pentru menținerea funcțiilor 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 funcționare a sistemelor, structurilor, componentelor și echipamentelor cu funcții de securitate nucleară

Incident cibernetic — eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică

Infrastructuri cibernetic — infrastructuri de tehnologia informației și comunicații, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice

Securitate cibernetică — starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic. Măsurile proactive și reactive pot include politici,

concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor

SCE — sistemele, componentele și echipamentele instalației nucleare

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

SCE cu funcții în exploatarea fiabilă a instalației nucleare — acele SCE care asigură funcționarea instalației nucleare în bune condiții, la parametri nominali și a căror defectare poate cauza condiții de operare anormală, tranziții, opriri neplanificate și/sau acționarea intempestivă a sistemelor cu funcții de securitate nucleară; aceste SCE contribuie la implementarea primului nivel de protecție în adâncime pentru asigurarea securității nucleare, respectiv la prevenirea defectărilor și a condițiilor de operare anormală

*ANEXA Nr. 2
la norme*

DOCUMENTE DE REFERINȚĂ

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, SUA, 2010

14. NEI 10-04 [Revision 2] Identifying Systems and Assets Subject to the Cyber Security Rule, Nuclear Energy Institute, SUA, 2012

15. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, SUA, 2018

16. Nuclear Sector Cybersecurity Framework Implementation Guidance, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, SUA, 2020

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

CONȚINUTUL MINIM
al planului de securitate cibernetică pentru o instalație nucleară**SECȚIUNEA 1****Organizare și responsabilități**

1.1. Scheme organizatorice, inclusiv organigrama organizației titularului de autorizație și a departamentului sau departamentelor cu responsabilități pentru securitatea cibernetică a instalațiilor nucleare;

1.2. Persoanele cu responsabilități și autoritate pentru securitatea cibernetică a instalațiilor nucleare; responsabilități pentru elaborare, raportare, avizare și aprobare a procedurilor și documentelor aferente;

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

1.4. Politica de securitate cibernetică la nivelul organizației.

SECȚIUNEA a 2-a**Inventarul SCE relevante pentru securitatea cibernetică a instalațiilor nucleare**

2.1. Lista SCE identificate în conformitate cu cerințele art. 6 din norme, a căror funcționare depinde de computere și programe software;

2.2. Lista tuturor aplicațiilor și programelor software legate de SCE identificate în conformitate cu cerințele art. 6 din norme;

2.3. Diagramele rețelelor informatice asociate SCE identificate în conformitate cu cerințele art. 6 din norme, inclusiv toate conexiunile către sisteme informatice externe care nu sunt sub controlul titularului de autorizație;

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 punctul de vedere al securității cibernetică, a efectelor acestora și a măsurilor tehnice și administrative specifice de prevenire, detecție și răspuns la incidente cibernetică;

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

SECȚIUNEA a 3-a**Analiza riscurilor, vulnerabilităților și a conformității cu cerințele aplicabile**

3.1. Periodicitatea reevaluării și revizuirii planului de securitate cibernetică;

3.2. Autoevaluarea eficacității planului și măsurilor de securitate cibernetică, inclusiv testele de penetrare;

3.3. Procedurile de audit și de identificare, urmărire și corectare a neconformităților;

3.4. Conformitatea cu cerințele din legislația națională și din standardele internaționale aplicabile;

3.5. Echipa desemnată pentru evaluarea securității cibernetică.

SECȚIUNEA a 4-a**Proiectarea sistemului de securitate cibernetică și controlul configurației**

4.1. Principiile de proiectare și 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. Cerințele pentru fiecare nivel de securitate cibernetică;

4.3. Stabilirea cerințelor de securitate cibernetică pentru furnizorii de produse și servicii destinate instalațiilor nucleare;

4.4. Asigurarea securității cibernetică pentru tot ciclul de viață 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.

SECȚIUNEA a 5-a**Procedurile operaționale de securitate cibernetică**

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

5.2. Protecția datelor;

5.3. Protecția comunicațiilor;

5.4. Protecția platformelor și aplicațiilor informatice;

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

5.6. Activitățile de întreținere necesare pentru SCE a căror funcționare depinde de computere și programe software;

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

5.8. Asigurarea continuității funcțiilor de securitate și siguranță nucleară;

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

5.10. Achiziția și transferul de SCE;

5.11. Eliminarea din sistem a SCE.

SECȚIUNEA a 6-a**Managementul personalului**

6.1. Verificarea/Avizarea personalului;

6.2. Pregătirea personalului;

6.3. Calificarea personalului;

6.4. Terminarea accesului și transferul personalului.

