Secțiunea III – Caiet de sarcini pentru achiziție de produse
Licențe și subscripții antivirus

1. Introducere

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Caietul de sarcini conține, în mod obligatoriu, specificații tehnice. Acestea definesc, după caz și fără a se limita la cele ce urmează, caracteristici referitoare la nivelul calitativ, tehnic și de performanță, siguranța în exploatare, dimensiuni, precum și sisteme de asigurare a calității, terminologie, simboluri, teste și metode de testare, ambalare, etichetare, marcare, condițiile pentru certificarea conformității cu standarde relevante sau altele asemenea.

În cadrul acestei proceduri, U.M. 02192 Constanța - Academia Navală „Mircea cel Bătrân" îndeplinește rolul de Autoritate contractantă.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

2. Contextul realizării acestei achiziții de produse

2.1. Informații despre Autoritatea contractantă

Academia Navală „Mircea cel Bătrân" -U.M. 02192 Constanța este o instituție publică de educație și cercetare științifică, ce oferă programe acreditate de licență și masterat pentru studii universitare în domeniul maritim, fluvial și portuar. Misiunea este formarea la nivel universitar a absolvenților care să satisfacă nevoia de profesioniști a Forțelor Navale Române și mediului economic din domeniul naval și portuar maritim și fluvial.

2.2. Informații despre contextul care a determinat achiziționarea produselor

Academia Navală „Mircea cel Bătrân" desfășoară activități didactice, administrative și de cercetare care necesită o infrastructură IT sigură, disponibilă și administrată centralizat. În contextul digitalizării proceselor educaționale și operaționale, protecția endpoint-urilor, serverelor și mediilor virtualizate reprezintă o condiție esențială pentru continuitatea serviciilor informatice ale instituției.

Infrastructura IT a ANMB include în prezent o soluție enterprise Bitdefender deja achiziționată, implementată și integrată în mediul operațional al instituției. Platforma este utilizată pentru protecția echipamentelor implicate în activitățile didactice, administrative și tehnice, precum și pentru administrarea centralizată a politicilor de securitate, actualizărilor, alertelor și rapoartelor.

Menținerea aceluiași producător este justificată de necesitatea asigurării continuității operaționale și a compatibilității cu arhitectura existentă. Politicile de securitate, grupurile de administrare, excepțiile, mecanismele de actualizare și fluxurile de monitorizare sunt deja definite, validate și utilizate de personalul tehnic. Înlocuirea soluției cu un produs aparținând altui producător ar presupune dezinstalarea agenților existenți, implementarea unei noi console de administrare, reproiectarea politicilor de securitate, redistribuirea agenților pe sistemele protejate, instruirea personalului și efectuarea unei campanii de testare și validare.

Aceste operațiuni ar genera costuri suplimentare, consum semnificativ de resurse administrative, timpi ridicați de implementare și riscuri temporare de expunere a infrastructurii la amenințări informatice. Prelungirea licențelor Bitdefender și suplimentarea cu un număr necesar de licențe similare permite păstrarea configurațiilor existente, continuitatea administrării centralizate, accesul la actualizările de securitate și suportul tehnic al producătorului, reprezentând soluția cu cel mai redus risc tehnic, operațional și economic pentru protejarea infrastructurii IT a ANMB

3. Descrierea produselor solicitate

3.1. Descrierea situației actuale la nivelul Autorității contractante

Produsele solicitate reprezintă licențe și subscripții software esențiale pentru securitatea și continuitatea infrastructurii IT a Academiei Navale „Mircea cel Bătrân". Acestea sunt destinate protecției endpoint-urilor, stațiilor de lucru, serverelor și mediilor virtualizate, precum și administrării centralizate a politicilor de securitate, monitorizării, raportării și răspunsului la incidente. Licențele și subscripțiile Bitdefender trebuie să permită utilizarea completă a platformei GravityZone, inclusiv protecție antimalware, protecție comportamentală, prevenirea atacurilor de tip exploit, control aplicații, firewall, control dispozitive, administrare centralizată, managementul actualizărilor, criptarea discurilor și funcționalități de detecție și răspuns la amenințări, conform licențierii solicitate.

3.2. Obiectivul general la care contribuie furnizarea produselor

Achiziționarea produselor în termenele stabilite prin documentația de atribuire are un rol determinant pentru buna desfășurare a activităților Academiei Navale „Mircea cel Bătrân", prin menținerea unui nivel adecvat de protecție endpoint, reducerea riscurilor de securitate cibernetică și asigurarea continuității serviciilor informatice.

3.3. Serviciile solicitate și operațiunile cu titlu accesoriu necesare a fi realizate

Nr. crt	Denumire produs	Cantitate	U/M	Loc de livrare	Specificații tehnice / cerințe funcționale	Durata minimă garanție / valabilitate
1	Prelungire licențe și subscripții Bitdefender GravityZone Business Security Enterprise / Ultra, cu module Patch Management și Full Disk Encryption, suport inclus – 3 ani	545	buc	Sediul autorității contractante, str. Fulgerului nr. 1, Constanța	conform specificațiilor tehnice	minim 36 luni garanție și mentenanță
2	Licențe și subscripții Bitdefender GravityZone Business Security Enterprise / Ultra, cu module Patch Management și Full Disk Encryption, suport inclus – 3 ani	355	licență			

Specificații tehnice:

A. Specificații tehnice generale

1. Cerințe generale

1.1 Toate subscripțiile și licențele software furnizate trebuie să fie originale, legale, emise de producătorul oficial Bitdefender sau prin canal autorizat și să permită utilizarea completă a funcționalităților necesare protecției endpoint, securității cibernetice și administrării infrastructurii IT a ANMB.

1.2 Furnizorul trebuie să se asigure că producătorul nu a anunțat încetarea ciclului de viață, End of Support sau End of Engineering Support pentru licențele și subscripțiile furnizate pe perioada contractuală de 3 ani.
1.3 Produsele livrate nu trebuie să includă aplicații software suplimentare care nu sunt necesare funcționării infrastructurii IT și care ar putea afecta performanțele, securitatea sau stabilitatea sistemelor existente.
1.4 Licențele furnizate trebuie să fie compatibile cu infrastructura IT existentă a ANMB și să permită funcționarea integrată a protecției endpoint, politicilor de securitate, monitorizării, raportării și răspunsului la incidente.
1.5 Furnizorul trebuie să demonstreze experiență în furnizarea, implementarea sau administrarea soluțiilor de protecție endpoint și securitate cibernetică utilizate în mediul educațional, instituțional sau industrial.

2. Cerințe generale pentru livrare, activare și configurare

2.1 Licențele și subscripțiile vor fi livrate exclusiv în format electronic, prin certificate, coduri de activare, fișiere de licență sau acces în portalul producătorului.
2.2 După activarea licențelor, contractantul va efectua împreună cu reprezentanții beneficiarului procedurile de verificare a funcționalităților.
2.3 Verificările vor include activarea licențelor, funcționarea consolei GravityZone, instalarea sau validarea agentului de securitate, aplicarea politicilor, actualizarea semnăturilor, raportarea evenimentelor, funcționarea modulelor Patch Management și Full Disk Encryption, precum și integrarea cu infrastructura IT existentă.
2.4 La finalizarea testelor, contractantul va furniza un raport de testare în format electronic și/sau tipărit, care va include rezultatele verificărilor și confirmarea funcționării subscripțiilor conform cerințelor caietului de sarcini.
2.5 Întreaga infrastructură software trebuie să fie operațională la data recepției finale, cu toate subscripțiile active și funcționale pe perioada contractuală de 3 ani.

Cerințe tehnice minimale:

Cerințe tehnice minimale pentru licențele și subscripțiile Bitdefender

- Soluția trebuie să includă protecție avansată pentru endpoint-uri, stații de lucru, servere și medii virtualizate: antimalware, protecție comportamentală, prevenirea exploit-urilor, control aplicații, firewall, control dispozitive și protecție web.
- Soluția trebuie să permită administrarea centralizată prin Bitdefender GravityZone, inclusiv definirea și aplicarea politicilor de securitate, monitorizare, alertare, inventariere, raportare și audit.
- Soluția trebuie să permită detecția amenințărilor pe bază de semnături, comportament, tehnologii de tip machine learning și analiză cloud, cu posibilitatea de răspuns automat sau manual la incidente.
- Soluția trebuie să includă funcționalități de Endpoint Detection and Response / Extended Detection and Response, în măsura licențierii ofertate, pentru investigarea incidentelor, corelarea evenimentelor și aplicarea măsurilor de remediere.
- Soluția trebuie să includă sau să permită utilizarea modulelor Patch Management și Full Disk Encryption pentru endpoint-urile licențiate.
- Soluția trebuie să fie scalabilă și să permită extinderea ulterioară prin adăugarea de noi endpoint-uri, politici, grupuri sau module, fără modificări structurale ale arhitecturii software.
- Licențele trebuie să includă actualizări automate ale semnăturilor, actualizări ale produsului și acces la suport tehnic Bitdefender pe întreaga perioadă contractuală.

B. Specificații tehnice detaliate

3. Parametrii funcționali, tehnici și calitativi necesari

3.1 Soluția trebuie să constituie o platformă integrată de protecție endpoint, destinată protejării stațiilor de lucru, serverelor și mediilor virtualizate.

3.2 Subscripțiile trebuie să includă licențele software, modulele de securitate, serviciile de suport, actualizările și componentele necesare funcționării complete a soluției în infrastructura IT a ANMB.

3.3 Platforma trebuie să permită administrarea centralizată prin consolă web, inclusiv inventarierea endpoint-urilor, aplicarea politicilor, monitorizarea stării de securitate, generarea de rapoarte și auditarea activităților administrative.

3.4 Agentul de securitate trebuie să poată fi instalat pe stații de lucru și servere fizice sau virtuale și să permită activarea/dezactivarea modulelor în funcție de politicile stabilite de administrator.

3.5 Soluția trebuie să permită integrarea cu Active Directory sau cu mecanisme echivalente de inventariere și grupare a sistemelor administrate.

3.6 Platforma trebuie să permită extinderea ulterioară a infrastructurii protejate prin adăugarea de noi endpoint-uri, servere, politici sau module, fără modificări structurale ale arhitecturii software.

3.7 Contractantul trebuie să furnizeze documentația tehnică a licențelor/subscripțiilor, instrucțiunile de activare, utilizare și administrare, precum și suport tehnic pe perioada contractuală de 3 ani.

Licențe și subscripții securitate antivirus și suport tehnic producător Bitdefender – 3 ani

Sunt solicitate licențe și subscripții Bitdefender GravityZone Business Security Enterprise / Ultra, cu modulele Patch Management și Full Disk Encryption, suport tehnic inclus, pentru o perioadă de 3 ani. Denumirea comercială exactă a produselor ofertate poate respecta nomenclatorul curent al producătorului, cu condiția ca funcționalitățile minime solicitate prin prezentul caiet de sarcini să fie acoperite integral.

Caracteristicile generale ale produselor solicitate:

- consolă de management centralizată pentru administrare, monitorizare, raportare și audit;
- protecție antimalware pentru stații de lucru, laptopuri, servere și medii virtualizate;
- module de prevenire și detecție a amenințărilor avansate, inclusiv comportamental, exploit prevention, sandboxing și tehnologii de tip machine learning;
- funcționalități de EDR/XDR, investigare, corelare și răspuns la incidente, în măsura licențierii ofertate;
- modul Patch Management pentru identificarea și gestionarea actualizărilor de securitate;
- modul Full Disk Encryption pentru protecția datelor stocate pe endpoint-uri;
- suport tehnic și actualizări pe întreaga perioadă contractuală.

A. Consola de management

- Consola trebuie să fie accesibilă prin interfață web și să permită administrarea centralizată a endpoint-urilor, politicilor, rapoartelor și alertelor.
- Consola trebuie să permită integrarea cu Active Directory, importul inventarului, descoperirea endpoint-urilor și gruparea sistemelor în funcție de structura organizațională sau politicile de securitate.
- Trebuie să permită crearea, modificarea și aplicarea politicilor de securitate pentru stații, servere și grupuri de sisteme, inclusiv politici diferențiate în funcție de locație, rețea sau profil de utilizare.
- Trebuie să permită instalarea la distanță sau manuală a agentului de securitate și crearea de pachete de instalare pentru sistemele de operare suportate.
- Trebuie să includă panouri de monitorizare, rapoarte configurabile, export în formate uzuale și

notificări către administrator pentru evenimente relevante de securitate, licențiere sau actualizare.

- Trebuie să permită administrarea pe bază de roluri, cu drepturi diferențiate pentru administratori, operatori și utilizatori cu rol de raportare.
- Trebuie să includă auditarea acțiunilor administrative și posibilitatea de filtrare a evenimentelor după utilizator, acțiune, sistem afectat și interval de timp.

B. Protecția stațiilor și serverelor fizice/virtuale

- Agentul de securitate trebuie să permită protecție antimalware în timp real, scanare la cerere, scanare programată și configurarea listelor de excludere pentru directoare, fișiere, extensii sau procese.
- Soluția trebuie să includă protecție împotriva ransomware, atacurilor fără fișiere, exploit-urilor avansate și amenințărilor necunoscute, inclusiv prin tehnologii comportamentale și machine learning.
- Soluția trebuie să poată utiliza scanare locală, scanare hibridă sau scanare centralizată, în funcție de resursele endpoint-ului și de configurația infrastructurii.
- Trebuie să permită protecția traficului web, antiphishing, controlul aplicațiilor și controlul accesului la internet pe baza politicilor definite de administrator.
- Trebuie să includă firewall configurabil, reguli bazate pe aplicație și/sau conexiune, profiluri de rețea și mecanisme de detecție a scanărilor de porturi.
- Trebuie să includă controlul dispozitivelor, cu posibilitatea de autorizare, restricționare sau blocare a mediilor de stocare și a altor dispozitive periferice.
- Trebuie să permită gestionarea carantinei, restaurarea fișierelor, ștergerea automată a obiectelor vechi și transmiterea fișierelor suspecte către infrastructura de analiză a producătorului, dacă această funcționalitate este inclusă în licențiere.
- Trebuie să permită protecția sistemelor Windows, Linux și macOS, conform matricii oficiale de compatibilitate a producătorului valabile la data ofertării.

C. Detecție, răspuns la incidente și analiză avansată

- Soluția trebuie să permită investigarea incidentelor de securitate prin colectarea și corelarea evenimentelor relevante de pe endpoint-uri.
- Soluția trebuie să permită vizualizarea incidentelor, a lanțului de evenimente și a sistemelor afectate, precum și aplicarea unor acțiuni de remediere precum izolarea endpoint-ului, blocarea fișierelor/proceselor, carantinarea, ștergerea sau adăugarea indicatorilor în liste de blocare.
- Trebuie să permită utilizarea indicatorilor de compromitere, a scorurilor de risc sau a indicatorilor de atac pentru prioritizarea incidentelor.
- Soluția trebuie să permită corelarea evenimentelor între mai multe endpoint-uri și raportarea incidentelor extinse, în măsura licențierii ofertate.
- Trebuie să permită exportul sau raportarea informațiilor relevante pentru investigarea incidentelor și pentru documentarea măsurilor de remediere.

D. Patch Management și Full Disk Encryption

- Modulul Patch Management trebuie să permită identificarea actualizărilor lipsă pentru sistemele suportate și aplicațiile compatibile, raportarea nivelului de expunere și inițierea procesului de remediere prin politici sau taskuri administrative.
- Modulul trebuie să permită programarea instalării actualizărilor, aplicarea diferențiată pe grupuri de endpoint-uri și raportarea stării de instalare.
- Modulul Full Disk Encryption trebuie să permită administrarea centralizată a criptării discurilor pentru endpoint-urile suportate și gestionarea politicilor de criptare prin consola de administrare.
- Soluția trebuie să permită raportarea stării de criptare și sprijinirea proceselor de recuperare,

conform funcționalităților puse la dispoziție de producător.

E. Cerințe de compatibilitate și suport

- Soluția ofertată trebuie să fie compatibilă cu versiunile de sisteme de operare Windows, Windows Server, Linux și macOS suportate oficial de producător la data ofertării.
- Ofertantul trebuie să pună la dispoziție documentația oficială privind compatibilitatea produsului, cerințele de sistem, procedurile de instalare, administrare și suport.
- Suportul tehnic trebuie să fie asigurat pe întreaga perioadă contractuală și să permită accesul la actualizări de produs, semnături, patch-uri, documentație și portalul producătorului.
- Denumirile modulelor și ale produselor pot fi adaptate nomenclatorului comercial curent al Bitdefender, cu condiția demonstrării echivalenței funcționale cu cerințele minime din prezentul caiet de sarcini.

4. Disponibilitate

Livrarea licențelor/subscripțiilor se va face în maximum 15 zile de la data semnării contractului. Activarea, configurarea și punerea în funcțiune se vor realiza la sediul autorității contractante sau de la distanță, după caz, în acord cu politicile producătorului și cu cerințele de securitate ale ANMB. Termenul de activare, configurare, punere în funcțiune și instruire a personalului este de maximum 30 zile de la livrarea produselor. Licențele și subscripțiile vor fi livrate în format electronic, prin certificate, coduri de activare, fișiere de licență sau acces în portalurile producătorilor. Contractantul va activa, configura și pune în funcțiune licențele/subscripțiile software în infrastructura IT existentă a ANMB și va efectua verificările necesare împreună cu reprezentanții beneficiarului. Punerea în funcțiune se realizează prin activarea electronică a licențelor și configurarea în platforma producătorului.

5. Garanție/valabilitate

Licențele și subscripțiile securitate antivirus și suport tehnic producător Bitdefender trebuie să fie acoperite de garanție/valabilitate pentru *cel puțin 3 ani de la data recepției (acceptării)*.

Perioada de garanție/valabilitate începe de la data activării sau de la data acceptării produselor, conform documentelor emise de producător.

Orice defecțiune, neconformitate de licențiere sau funcționare necorespunzătoare va fi sesizată în scris Contractantului, în termen de 48 de ore de la constatare.

Contractantul va sprijini remedierea neconformităților în termen de maximum 5 zile de la data sesizării, fără costuri suplimentare pentru Autoritatea contractantă.

Garanția/mentenanța trebuie să acopere accesul la actualizări, suport tehnic și remedierea problemelor legate de licențiere sau funcționare pe perioada contractuală.

6. Operațiuni cu titlu accesoriu

6.1. Mentenanța preventivă în perioada de garanție

Mentenanța preventivă se realizează prin actualizări automate de securitate, patch-uri și upgrade-uri software furnizate de producător.

Contractantul va pune la dispoziția Autorității contractante - Instrucțiuni de mentenanță preventivă în perioada de garanție și valabilitate a licențelor (inclusiv ritmicitatea operațiunilor).

Operațiunile de mentenanță preventivă a licențelor cuprind o serie de activități planificate și riguroase menite să le mențină în perfectă stare de funcționare și să optimizeze eficiența acestora în conformitate cu specificațiile tehnice ale softurilor. În plus, scopul acestor operațiuni este de a extinde durata lor de viață, de a evita situațiile care pot perturba activitatea Autorității Contractante și de a minimiza posibilitatea unei defecțiuni.
Contractantul este responsabil pentru realizarea operațiunilor de mentenanță preventivă (în conformitate cu cerințele stabilite de către producătorul echipamentului, așa cum au fost agreate de părți conform contractului și caietului de sarcini).

6.2. Suport tehnic

Suportul tehnic va fi asigurat pe întreaga perioadă contractuală, conform politicilor producătorului.

6.3. Instruirea personalului pentru utilizare

Furnizorul va acorda suport pentru configurarea inițială și instruirea personalului desemnat privind utilizarea și administrarea licențelor

6.3. Mediul în care este operat produsul

Produsele software vor fi operate în cadrul Academiei Navale „Mircea cel Bătrân", în spații dotate cu infrastructură IT funcțională, conectate la rețeaua internă a instituției și la sistemele informatice existente. Produsele vor fi utilizate exclusiv în mediul IT controlat al ANMB, în conformitate cu politicile interne de securitate cibernetică, acces și administrare.

7. Documentații ce trebuie furnizate Autorității contractante în legătură cu produsele

Nr. crt.	Documentații furnizate de Contractant	Termen limită de punere la dispoziție
1	Licențe/subscripții în format electronic	cel mai târziu la data prestării serviciilor
2	Instrucțiuni de activare și administrare	
3	Acces la portalul producătorului	
4	Fișe tehnice ale serviciilor licențiate	
5	Politici de suport și mentenanță	

8. Recepție

Recepția produselor se va efectua pe bază de proces-verbal semnat de Contractant și Autoritatea contractantă. Recepția se va realiza în două etape: recepția cantitativă și recepția calitativă.

Recepția cantitativă se va realiza în maximum 1 zi de la livrare și va consta în verificarea numărului de licențe/subscripții furnizate, a codurilor de activare, certificatelor digitale și a accesului în portalul producătorului.

Recepția calitativă se va realiza în maximum 5 zile de la recepția cantitativă și va include activarea licențelor, verificarea consolei GravityZone, verificarea agentului de securitate, aplicarea politicilor, actualizarea semnăturilor, verificarea funcționării modulelor Patch Management și Full Disk Encryption, testarea raportării și confirmarea integrării în infrastructura IT a ANMB.

Criteriile referitoare la rezultatul recepției calitative, numărul și tipul defectelor identificate, precum și termenul de remediere, sunt detaliate în tabelul următor:

Rezultatul recepției	Numărul defectelor	Termen de
Acceptat	-	-
Acceptat cu observații	1-3	5 zile
Acceptat cu rezerve	4-5	7 zile
Refuzat	> 5	10 zile

9. Modalități si condiții de plata

Contractantul va emite factură fiscală pentru serviciile livrate. Fiecare factură va avea menționat numărul contractului, datele de emitere și de scadență ale facturii respective. Facturile vor fi trimise în original la sediul Autorității contractante numai după semnarea procesului verbal de recepție, prin care se confirmă livrarea, recepția și acceptarea serviciilor (instalarea update-urilor și remedierea eventualelor defecte constatate – după caz).

Procesul verbal de recepție va însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute mai jos:

- factură fiscală;
- certificat de garanție;
- documentațiile prevăzute la pct. 7 al Caietului de sarcini

Plățile în favoarea Contractantului se vor efectua în termen de 30 de zile de la data emiterii facturii fiscale în original și a tuturor documentelor justificative.

10. Obligațiile principale ale Autorității contractante

Autoritatea contractantă va pune la dispoziția Contractantului, cu promptitudine, orice informații și/sau documente pe care le deține și care pot fi relevante pentru realizarea Contractului. În măsura în care Autoritatea contractantă nu furnizează datele/informațiile/documentele solicitate de către Contractant, termenele stabilite în sarcina Contractantului se prelungesc în mod corespunzător.

Autoritatea contractantă se obligă să respecte dispozițiile din prezentul Caiet de sarcini, să desemneze persoana de contact, să recepționeze produsele furnizate și să certifice conformitatea acestora conform procedurii de recepție. Autoritatea contractantă poate notifica Contractantul cu privire la necesitatea revizuirii sau respingerii produselor, solicitarea fiind motivată prin comentarii scrise.

11. Cadrul legal care guvernează relația dintre Autoritatea contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

i. Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;
ii. Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;
iii. Convenția nr. 29 a OIM privind munca forțată;
iv. Convenția nr. 105 a OIM privind abolirea muncii forțate;
v. Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;
vi. Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);
vii. Convenția nr. 100 a OIM privind egalitatea remunerației;
viii. Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;

ix. Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;

x. Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);

xi. Convenția de la Stockholm privind poluanții organici persistenți (Convenția de la Stockholm privind POP);

Verificat,

Lt.cdor
Constantin SCHIPOR

Întocmit,

Col.
Bucur Eugen