Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE

nr. _____

din _____ 2024

Chişinău

pentru modificarea unor hotărâri ale Guvernului

(aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)

În temeiul art. 23 alin. (2) lit. c) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225),

Guvernul HOTĂRĂȘTE:

1. Regulile privind prestarea serviciilor poștale aprobate prin Hotărârea Guvernului nr. 1457/2016 (Monitorul Oficial al Republicii Moldova, 2017, nr. 24-29, art.46), cu modificările ulterioare, se modifică după cum urmează:

1) pct. 4 se completează cu subpunctul 4)[1], cu următorul cuprins:

„4)[1] securitatea rețelelor și sistemelor informatice utilizate la prestarea serviciilor poștale și, dacă sunt incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile de asigurare a securității cibernetice stabilite de legea respectivă;”.

2) după pct. 136, se completează cu un punct nou *„136[1]”* care va avea următorul cuprins:

„136[1]) Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat al respectării de către furnizorii de servicii poștale, incluși în Lista furnizorilor de servicii, a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică. Furnizorii de servicii poștale sunt obligați să ofere acces Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare realizării obiectivelor controlului.”.

2. Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr. 201/2017 (Monitorul Oficial al Republicii Moldova, 2017, nr.109-118, art. 277), se modifică după cum urmează:

1) în tot textul, cuvintele *„incidente de securitate cibernetică”* și *„incidente*

de securitate”, la orice formă gramaticală, se substituie cu cuvintele *„incidente cibernetice”* la forma gramaticală corespunzătoare.

2) în tot textul, cuvintele *„sistemul de management al securității cibernetice”* la orice formă gramaticală, se substituie cu cuvintele *„sistemul de management al securității informației”* la forma gramaticală corespunzătoare.

3) în tot textul, cuvintele *„regulament intern de securitate cibernetică”* și *„regulament intern de securitate”* la orice formă gramaticală, se substituie cu cuvintele *„reglementări interne aplicabile”* la forma gramaticală corespunzătoare.

4) la pct. 1, textul *„ :*

1) echipamentele (hardware) și produsele de program (software) existente în cadrul fiecărei instituţii;

2) sistemele informatice, resursele și sistemele informaționale existente în instituție (în continuare – sisteme), precum și cele aflate la etapa de elaborare, testare și implementare. ” se substituie cu sintagma „*rețele și sisteme informatice (în continuare – sisteme).*”

5) la pct. 5, textul „*Alţi termeni sînt utilizaţi în sensul definit de Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat, Legea nr.1069-XIV din 22 iunie 2000 cu privire la informatică şi Hotărîrea Guvernului nr. 811 din 29 octombrie 2015 „Cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020”.*”, se substituie cu textul „*Alţi termeni sînt utilizaţi în sensul definit de Legea nr. 48/2023 privind securitatea cibernetică, Legea nr. 467/2003 cu privire la informatizare şi la resursele informaţionale de stat și Legea nr.1069/2000 cu privire la informatică.*”.

6) la pct.7, textul *„Ministerului Tehnologiei Informației și Comunicațiilor”* se substituie cu textul „*Agenției pentru Securitate Cibernetică și Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică*”.

7) se completează cu punctul *„7[1]*” care va avea următorul cuprins:

„*7[1]*. În vederea asigurării unei abordări complexe și multidisciplinare a cerințelor de securitate, organizarea sistemului de management al securității informației se efectuează cu participarea tuturor subdiviziunilor instituției, definind clar rolurile acestora.”.

8) pct. 8 va avea următorul cuprins:

„*8*. Persoana (subdiviziunea) responsabilă are următoarele atribuții:

1) coordonează sistemul de management al securității informației în instituție;

2) participă, cel puțin o dată pe an, la cursuri de formare în domeniul securității cibernetice și, respectiv, organizează cursuri pentru angajații instituției;

3) coordonează elaborarea și implementarea:

a) planului de acțiuni pentru asigurarea securității cibernetice al instituției;

b) politicilor de securitate cibernetică a instituției;

c) politicilor referitoare la analizarea riscurilor și asigurarea securității rețelelor și sistemelor informatice;

d) politicilor și procedurilor privind gestionarea incidentelor cibernetice (prevenirea, detectarea și răspunsul la incidentele respective);

e) politicilor și procedurilor privind utilizarea criptografiei și a criptării, în special a criptării de la un capăt la altul;

f) politicilor și procedurilor referitoare la evaluarea eficacității măsurilor de securitate implementate;

g) măsurilor privind continuitatea activității și privind gestionarea crizelor;

h) măsurilor de securitate aplicate în achiziționarea, dezvoltarea și întreținerea rețelelor și sistemelor informatice, inclusiv în divulgarea și gestionarea vulnerabilităților;

i) măsurilor de securitate privind resursele umane, politicilor de control al accesului și de gestionare a activelor;

j) măsurilor privind asigurarea securității lanțului de aprovizionare, inclusiv aspectele, legate de securitate, referitoare la relațiile furnizorului de servicii cu prestatorii sau cu furnizorii direcți de servicii ai acestuia;

k) practicilor de bază în materie de igienă cibernetică și formarea în domeniul securității cibernetice;

l) soluțiilor de autentificare, de comunicații securizate voce, video și text;

m) sistemelor securizate de comunicații de urgență în cadrul furnizorului de servicii;

n) planului de instruire și responsabilizare în securitatea cibernetică a personalului;

o) reglementările interne pentru domeniul securității cibernetice;

4) asigură actualitatea documentației privind măsurile de securitate;

5) asigură monitorizarea situației privind securitatea rețelelor și sistemelor sale informatice, inclusiv în scopul detectării serviciilor TIC, proceselor TIC sau produselor TIC care compromit rețelele sau sistemele respective;

6) întreprinde măsuri orientate spre reducerea impactului și răspândirii incidentelor cibernetice, inclusiv, dacă este necesar, restricționează utilizarea sau accesul la rețelele și sistemele informatice;

7) verifică plenitudinea și conformitatea aplicării măsurilor de securitate, inclusiv prin efectuarea auditurilor de securitate, și documentează rezultatele verificării respective;

8) evaluează vulnerabilitățile și riscurile de securitate ale rețelelor și sistemelor informatice, determină gravitatea impactului unui eventual incident cibernetic survenit ca urmare a materializării riscurilor, descrie măsurile pentru soluționarea unui incident cibernetic și întocmește un raport de evaluare în acest sens;

9) informează continuu conducerea cu privire la situația actuală a securității cibernetice.".

9) la pct.9:

a) cuvântul *„, dacă”* se substituie cu textul „*în următoarele cazuri, fără însă a se limita la acestea*".

b) la subpunctul 2) sintagma *„la securitatea sistemului”* se substituie cu sintagma „*cibernetice la sisteme*".

c) la subpunctul 3) sintagma *„semnificativ de securitate a sistemului”* se substituie cu sintagma „*cibernetic cu impact semnificativ asupra sistemului și asupra continuității serviciului ori asupra securității rețelei și/sau sistemului informatic*".

10) la pct. 11:

a) subpunctul 1), după cuvântul „*obiectivele*" se completează cu textul „ *,corelate cu standardele în domeniul securității informației și în cel al securității cibernetice și cele mai bune practici pentru gestionarea incidentelor cibernetice și a riscurilor*;".

b) subpunctul 2), sintagma *„securitate cibernetică”* se substituie cu sintagma „*securitate a informației*".

11) la pct. 12:

a) subpunctul 2), după cuvântul *„personalului”* se completează cu textul *„ , inclusiv furnizorului extern de servicii”.*

b) subpunctul 3) se abrogă.

12) la pct. 13, textul „*Regulamentele interne de securitate cibernetică*" se substituie cu textul „*Reglementări interne aplicabile în domeniul TIC*".

13) la pct. 16, subpunctul 1), după sintagma „*grupuri de*" se completează cu sintagma „*angajați și*".

14) la pct. 17, subpunctul 4), lit. c), textul „*private de rețelele adiacente*" se substituie cu textul „*instituției, precum și segmentarea acesteia în rețele în scopul protejării sistemelor, serviciilor și grupurilor de angajați*".

15) la pct. 21:

a) subpunctul 3), cuvântul „*autoritățile*" se substituie cu cuvântul „*instituțiile*".

b) subpunctul 7) va avea următorul cuprins:

„*7)* analiza riscurilor se efectuează periodic, dar nu mai rar de o dată pe an, și servește pentru ajustarea politicii de securitate cibernetică și a reglementărilor

interne aplicabile”.

c) subpuntul 9), cuvântul „*entității*” se substituie cu cuvântul „*instituției*”.

d) subpunctul 10) va avea următorul cuprins:

„*10)* efectuarea periodică a testului de penetrare în conformitate cu politica de securitate cibernetică a instituției. Rezultatele testului se prezintă Agenției pentru Securitate Cibernetică, în termen de o lună, împreună cu planul de remediere a deficiențelor depistate.”.

16) capitolul VI va avea următorul cuprins:

„VI. CERINȚE DE SECURITATE ÎN RELAȚIILE CU PRESTATORII DE SERVICII

23. În cazul în care instituția încheie un contract cu furnizorul extern de servicii, contractul trebuie să includă și cerințe relevante de securitate, convenite cu fiecare furnizor pe baza tipului de relație cu acesta. Contractul trebuie să stabilească cel puțin:

1) reglementările interne de securitate cibernetică ale instituției pe care trebuie să le respecte prestatorul de servicii în realizarea prevederilor contractuale;

2) cerințele precise pentru volumul și calitatea serviciilor prestate, după caz documentate ca nivel agreat de servicii;

3) drepturile și obligațiile instituției și prestatorului de servicii:

a) dreptul instituției de a monitoriza continuu calitatea serviciilor furnizate;

b) dreptul instituției de a înainta prestatorului de servicii o prescripție cu privire la nerespectarea aspectelor legate de prestarea serviciilor de înaltă calitate, executarea la timp și corectă a actelor normative și reglementărilor interne ale instituției în domeniul securității cibernetice;

c) dreptul instituției de a înainta prestatorului extern de servicii o cerere scrisă motivată pentru încetarea imediată a contractului de prestări servicii, în cazul în care instituția a constatat că prestatorul de servicii nu respectă cerințele contractului privind valoarea sau calitatea serviciului;

d) obligația prestatorului de servicii de a furniza instituției informația privind monitorizarea continuă a calității serviciilor prestate;

e) de a pune la dispoziţia entității orice informaţie, ori de câte ori este necesar, privind serviciile externalizate;

f) obligația prestatorului de servicii de a asigura că persoanele implicate în executarea contractului sunt instruite în mod corespunzător cu privire la rolurile și responsabilitățile lor înainte de a li se permite accesul la orice informație vizată în realizarea contractului respectiv;

g) obligația prestatorului de servicii de a respecta reglementările interne ale instituției;

e) dreptul de audit al prestatorului de serviciu, dacă au fost notificate nonconformități critice.

23[1]. Instituția este responsabilă de măsurile de securitate în ce privește activitatea personalului prestatorilor de servicii, inclusiv coordonarea responsabilităților, acorduri de nedivulgare a informațiilor, autorizarea accesului și monitorizarea și planul de contingență (intervenție) în caz de întrerupere/încetare a prestării serviciilor.”.

17) la pct. 24:

a) subpunctul 1), sintagma „*răspuns de incidente cibernetice*” se substituie cu textul „*răspuns la incidente cibernetice, respectând măsurile privind continuitatea activității și privind gestionarea crizelor*”;

b) subpunctul 2), după cuvântul *„stabilite”* se completează cu textul *„, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică”*

3. Punctul 8 din **Statutul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică” aprobat prin Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat** (Monitorul Oficial al Republicii Moldova, 2018, nr. 157-166, art.474), cu modificările ulterioare, se modifică după cum urmează :

1) se completează cu subpunctul *„20[1]”* cu următorul cuprins:

„*20[1])* asigură securitatea rețelelor și sistemelor informatice proprietate a statului;”.

2) se completează cu subpunctul *„31[1]”* cu următorul cuprins:

„*31[1])* informează Agenția pentru Securitate Cibernetică cu privire la incidentele cibernetice notificate de autoritățile și instituțiile publice, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică;”.

3) La subpunctul 34) cuvintele *„Centrul guvernamental de reacție la incidente de securitate cibernetică”* se substituie cu cuvintele *„Centrul guvernamental de răspuns la incidentele cibernetice”.*

4) se completează cu subpunctul *„34[1]*” cu următorul cuprins:

„*34[1])* facilitează interacțiunea dintre autoritățile și instituțiile publice cu Agenția pentru Securitate Cibernetică și echipa de răspuns la incidentele cibernetice la nivel național, inclusiv îndeplinirea de către acestea a obligațiilor privind securitatea cibernetică stabilite de Legea nr. 48/2023 privind securitatea cibernetică;”.

4. Regulamentul cu privire la tipurile şi modul de stabilire a sporurilor cu caracter specific, aprobat prin Hotărârea Guvernului nr. 1231/2018 pentru punerea în aplicare a prevederilor Legii nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar (Monitorul Oficial al Republicii

Moldova, 2018, nr. 480-485, art. 1310), cu modificările ulterioare, se completează cu punctul „*5[1]*” cu următorul cuprins:

”*5[1]*. Pentru personalul Agenției pentru Securitate Cibernetică sporul cu caracter specific se acordă pentru exercitarea funcțiilor de:

1) răspuns la incidente și crize cibernetice la nivel național;

2) identificarea și evidența furnizorilor de servicii;

3) supravegherea și controlul de stat al respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice;

4) asigurarea cooperării la nivel național și internațional și schimb de informații în materie de securitate cibernetică, inclusiv rolul de punct național unic de contact;

5) orientare metodologică, reglementare, cercetare și dezvoltare în domeniul securității cibernetice, precum și pentru caracterul specific al suportului în realizarea funcțiilor Agenției pentru Securitate Cibernetică.”.

5. Regulamentul privind modul de utilizare a platformei de interoperabilitate (MConnect) aprobat prin Hotărârea Guvernului nr. 211/2019 (Monitorul Oficial al Republicii Moldova, 2019, nr. 132-138, art.254), cu modificările ulterioare, se modifică după cum urmează:

1) la pct. 6:

a) subpunctul 14), textul *„ , inclusiv”,* se substituie cu cuvântul *„și”.*

b) subpunctul 15), după sintagma *„precum și pentru”* se completează cu sintagma *„prevenirea și”.*

2) la pct. 8, subpunctul 19), după sintagma *„și pentru”* se completează cu sintagma *„prevenirea și”.*

6. Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat (Monitorul Oficial al Republicii Moldova, 2020, nr. 180-187, art.614), se modifică după cum urmează:

1) în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și *„incidente de securitate”,* la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare.

2) în tot textul hotărârii și anexei, cuvintele *„Centrul guvernamental de reacție la incidente de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„Centrul guvernamental de răspuns la incidentele cibernetice”* la forma gramaticală corespunzătoare.

3) la anexă:

a) în tot textul, cuvintele *„incidente de securitate informațională”,* la orice formă gramaticală, se substituie cu cuvintele *„incidente cibernetice”* la forma gramaticală corespunzătoare.

b) la pct.3, textul „*incident de securitate cibernetică – eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică*” se substituie cu textul „*incident cibernetic – astfel cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică*”.

c) la pct. 5:

- subpunctul 12), sintagma „*securitatea sistemelor informaționale și a rețelelor*” se substituie cu sintagma „*securitatea rețelelor și sistemelor informatice*”;

- subpunctul 14) va avea următorul cuprins:

„*14)* furnizează entităților publice care au notificat un incident cibernetic imediat, însă nu mai târziu de 24 ore de la recepționarea notificării, un răspuns cu privire la incidentul cibernetic care să cuprindă recomandări și instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv;”.

- subpunctul 16), după sintagma „*cooperează cu*”, se completează cu textul „*echipa de răspuns la incidentele cibernetice la nivel național,* ”.

- după subpunctul 16), se completează cu subpunctele *„16[1]-16[3]*” care vor avea următorul cuprins:

„*16[1])* asigură securitatea rețelelor și sistemelor informatice proprietate a statului;

16[2]) notifică echipa de răspuns la incidente cibernetice la nivel național, informează cu privire la incidentele cibernetice notificate de autoritățile și instituțiile publice, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică;

16[3]) facilitează interacțiunea dintre autoritățile și instituțiile publice cu Agenția pentru Securitate Cibernetică și echipa de răspuns la incidentele cibernetice la nivel național, inclusiv îndeplinirea de către acestea a obligațiilor privind securitatea cibernetică stabilite de Legea nr. 48/2023 privind securitatea cibernetică;”.

- subpunctul 18), sintagma „*Serviciul de Informații și Securitate al Republicii Moldova*”, se substituie cu sintagma „*Agenția pentru Securitate Cibernetică*”.

d) după punctul „6”, se completează cu un punct nou „6[1]”, care va avea următorul cuprins:

„6[1]. Notificarea incidentelor cibernetice cu impact semnificativ de către CERT Gov către echipa de răspuns la incidente cibernetice la nivel național *(în*

continuare - CSIRT național) cu privire la incidentele cibernetice, nu exclude dreptul entităților publice să notifice și CSIRT-ul național cu privire la incidentele cibernetice.”.

e) la pct. 7, subpunctul 1), textul „*necesare pentru asigurarea securității cibernetice*” se substituie cu textul „*tehnice și organizatorice pentru a gestiona riscurile de securitate a rețelelor și a sistemelor informatice pe care le utilizează*”.

f) la pct. 8, sintagma „*CERT Gov*” se substituie cu sintagma „*Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică*”.

g) la pct. 11, subpunctul 3), după litera a) se completează cu o literă nouă „*a[1]*” care va avea următorul cuprins:

”*a[1])* notifică CSIRT-ul național, în condițiile stabilite de Legea nr. 48/2023 privind securitatea cibernetică, cu privire la:

- incidentele cibernetice cu impact semnificativ asupra securității rețelelor sau sistemelor informatice ale statului ori asupra continuității serviciilor;
- incidentele cibernetice ale căror impact semnificativ asupra securității rețelelor sau sistemelor informatice ale statului ori asupra continuității serviciilor nu este evident, dar poate fi presupus în mod rezonabil, și
- impactul semnificativ al unui incident cibernetic, care a afectat un terț, asupra continuității serviciului prestat de persoanele juridice de drept public, în cazul în care serviciului respectiv depinde de serviciile terțului afectat”.

h) pct. 12., la sfârșit se completează cu textul „ *și cu Agenția pentru Securitate Cibernetică*”.

7. Programul național de securitate în domeniul aviației civile aprobat prin Hotărârea Guvernului nr. 124/2021 (Monitorul Oficial al Republicii Moldova, 2021, nr.212-218, art. 365), cu modificările ulterioare, se modifică după cum urmează :

1) în tot textul, cuvântul *„STISC”,* la orice formă gramaticală, se substituie cu sintagma *„Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”* la forma gramaticală corespunzătoare.

2) punctul „*557[1]*” va avea următorul cuprins:

„*557[1]*. Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” este responsabilă de asigurarea securității rețelelor și sistemelor informatice proprietate a statului, de facilitarea îndeplinirii de către furnizorii de servicii persoane juridice de drept public a obligațiilor privind asigurarea securității cibernetice prevăzute de prezentul Program, inclusiv a celor privind notificarea, și de facilitarea interacțiunii acestora cu autoritatea competentă și echipa de răspuns la incidentele cibernetice la nivel național.”

3) după punctul „*560*”, se completează cu punctele „*560[1] și 560[2]*”, care vor

avea următorul cuprins:

„*560[1]*. Operatorii aeroportuari, transportatorii aerieni, FSNA și alte entități definite în prezentul Program trebuie să asigure securitatea rețelelor și sistemelor informatice utilizate la prestarea serviciilor și, dacă sunt incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile de asigurare a securității cibernetice stabilite de legea respectivă.

560[2]. Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat al respectării de către operatorii aeroportuari, transportatorii aerieni, FSNA și alte entități definite în prezentul Program, incluși în Lista furnizorilor de servicii, a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică. Aceștia sunt obligați să ofere acces Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare realizării obiectivelor controlului.”.

8. Hotărârea Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” (Monitorul Oficial al Republicii Moldova, 2020, nr. 201-207, art.516), se modifică după cum urmează:

1) în hotărâre:

a) în titlu și în textul hotărârii de Guvern cuvintele *„incidentelor de securitate cibernetică”* se substituie cu cuvintele *„incidentelor cibernetice”.*

b) în clauza de adoptare, după cuvântul „*temeiul*”, se completează cu textul „ *art. 10 alin (1) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225),*”.

4) în anexă:

a) la introducere, cuvintele „*Centrul guvernamental de reacție la incidente de securitate cibernetică*” se substituie cu cuvintele „*Centrul guvernamental de răspuns la incidentele cibernetice*”.

b) în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare.

c) în tot textul, cuvintele *„SI RSISC”* se substituie cu cuvintele *„SI RSIC”*.

9. Regulamentul sanitar privind supravegherea și monitorizarea calității apei potabile aprobat prin Hotărârea Guvernului nr. 651/2023 (Monitorul Oficial al Republicii Moldova, 2023, nr.387-390, art. 928), se completează cu punctele *„72[1] și 72[2]”* cu următorul cuprins:

„72[1]. Furnizorii de apă potabilă, trebuie să asigure securitatea rețelelor și sistemelor informatice utilizate la prestarea serviciilor și, dacă sunt incluși în Lista

furnizorilor de servicii în sectoarele și subsectoarele critice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile de asigurare a securității cibernetice stabilite de legea respectivă.

72^2. Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat al respectării de către furnizorii de apă potabilă, incluși în Lista furnizorilor de servicii, a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică. Furnizorii de apă potabilă sunt obligați să ofere acces Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare realizării obiectivelor controlului.”.

10. Prezenta hotărâre intră în vigoare la data de 1 ianuarie 2025, cu excepția prevederilor punctului 4 care intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova .

PRIM-MINISTRU **Dorin RECEAN**

Contrasemnează:

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării **Dumitru ALAIBA**

NOTA DE FUNDAMENTARE
la proiectul de hotărâre de Guvern pentru modificarea unor hotărâri ale Guvernului (aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
Proiectul a fost elaborat de Ministerul Dezvoltării Economice și Digitalizării, cu suportul proiectului „Asistență rapidă Republicii Moldova în domeniul securității cibernetice”, finanțat de Comisia Europeană și implementat de Academia de Guvernare Electronică din Estonia.
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ
Articolul 23 al.(1) lit.c) din Legea nr. 48/2023 privind securitatea cibernetică stabilește obligația Guvernului de a aduce actele sale normative în concordanță cu legea în cauză.
2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative
La 16 martie 2023, Parlamentul a adoptat Legea nr. 48/2023 privind securitatea cibernetică, ce urmează să intre în vigoare la 1 ianuarie 2025. Scopul principal al acestei legi este de a asigura legalitatea în spațiul cibernetic prin reglementarea principalelor elemente indispensabile implementării unui model de guvernanță eficient la nivel național în vederea protecției și asigurării securității rețelelor și sistemelor informatice, utilizate de către persoanele juridice, publice sau private, în procesul de prestare a serviciilor considerate a fi esențiale pentru susținerea unor activități societale și economice critice. Un element juridic fundamental în procesul de reglementare a acestui domeniu a fost legislația Uniunii Europene, mai ales având în vedere statutul de țară candidat la aderarea la Uniunea Europeană al Republicii Moldova. Prin această lege s-a urmărit, deși doar parțial, armonizarea cadrului normativ național cu prevederile Directivei NIS2 (Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148) și implicit, cu elementele esențiale ale Directivei NIS1 (Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune). Astfel, Legea privind securitatea cibernetică cuprinde un set de reglementări care au ca scop în principal: • stabilirea cadrului general privind cooperarea și coordonarea strategică la nivel național și internațional, prin reglementarea expresă a constituirii unui consiliul coordonator cu rol consultativ al Guvernului, dedicat exclusiv domeniului securității cibernetice și stabilirea obligativității adoptării unei strategii naționale în acest domeniu; • desemnarea/instituirea de către Guvern a unei autorități competente în domeniul securității cibernetice la nivel național, care să includă în competența sa, de rând cu funcțiile de coordonare, cooperare internă, supraveghere și control de stat, și pe cele de echipă națională de răspuns la incidentele cibernetice și de punct unic de contact la nivel național; • reglementarea legală primară a procesului de coordonare și gestionare a crizelor în domeniul securității cibernetice și atribuirea competenței legale în această materie viitoarei autorități responsabile; • stabilirea cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice nu doar de către persoanele juridice de drept public, ci și de către cele de drept privat, în mod special în ce privește obligațiile de implementare a măsurilor de securitate și în ce privește obligațiile de notificare a incidentelor cibernetice semnificative, și

împuternicirea autorității competente la nivel național în acest domeniu cu exercitarea funcțiilor de supraveghere și control de stat al modului în care persoanele vizate îndeplinesc aceste obligații;

- determinarea cadrului normativ primar pentru identificarea persoanelor juridice ca fiind furnizori de servicii esențiale, împuternicire atribuită de asemenea autorității respective, ca parte componentă a funcției de supraveghere etc. Potrivit prevederilor Legii privind securitatea cibernetică, Guvernul este învestit cu competență de intervenție, de diferită natură (normativă, organizatorică și tehnică), pe un șir de chestiuni în vederea punerii în aplicare a prevederilor acesteia, dintre care în mod special ținem să le evidențiem pe cele care sunt pertinente obiectului de reglementare a proiectului propus spre avizare și anume:
- aprobarea listei sectoarelor, subsectoarelor și, respectiv, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și/sau subsectoare și care vor cădea sub incidența prevederilor legii și a cadrului metodologic de identificare a acestora (art. 4 alin. (2));
- desemnarea/constituirea, reglementarea modului de organizare și funcționare, a structurii și efectivului-limită a entității care va exercita funcțiile autorității competente (art. 7 alin. (1));
- modul de aplicare a măsurilor de supraveghere de către autoritatea competentă (art. 18 alin. (5));
- modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii privind securitatea cibernetică (art. 19 alin. (5)). Suplimentar, la 21 martie 2024, a fost aprobat în a doua lectură4 proiectul de lege pentru modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică). Legea nr. 58/2024 pentru modificarea unor acte normative are ca obiectiv general să aducă în concordanță cu Legea privind securitatea cibernetică prevederile legale existente. Intervențiile propuse prin respectiva inițiativă legislativă constau în principal în următoarele:
- asigurarea interconexiunii dintre normele Legii privind securitatea cibernetică și cele cuprinse în legile sectoriale care reglementează activitatea viitorilor furnizori de servicii și eliminarea/revizuirea unor prevederi care ar putea suscita interpretări echivoce sau contradictorii în procesul aplicării legii
- finalizarea instituirii cadrului normativ primar necesar stabilirii modelului de guvernanță în domeniul securității cibernetice la nivel național.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul de hotărâre de Guvern are ca obiectiv general aducerea în concordanță a hotărârilor de Guvern cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe. În acest context, finalitățile urmărite prin adoptarea actului normativ sunt determinate de diferitele categorii de intervenții normative propuse în proiect și constau, în principal, în următoarele:

- Alinierea cadrului normativ secundar care stabilește rigori în domeniul securității cibernetice la măsurile de securitate stabilite de Legea nr. 48/2023 privind securitatea cibernetică;
- Revizuirea unor prevederi din hotărârile de guvern sectoriale care ar putea suscita interpretări echivoce sau contradictorii în aplicarea Legii privind securitatea cibernetică și legislației sectoriale care reglementează activitatea viitorilor furnizori de servicii.

În proiectul de hotărâre de Guvern sunt propuse modificări la 11 hotărâri de Guvern, care pot fi divizate, în funcție de factorii ce le determină, finalitățile pe care le urmăresc și efectele pe care le vor produce, în următoarele categorii:

1. Prima categorie de modificări propuse în proiect (pct. 2 și 6) constau în necesitatea alinierii cadrului normativ secundar care stabilește rigori în domeniul securității

cibernetice la măsurile de securitate stabilite de Legea nr. 48/2023 privind securitatea cibernetică.

Modificările propuse în pct. 2 din proiectul de hotărâre de Guvern vizează Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr. 201/2017 și au ca obiectiv corelarea modului de organizare a sistemului intern de securitate cibernetică în cadrul autorităților și instituțiilor publice cu noile măsuri de securitate stabilite de Legea privind securitatea cibernetică pentru a asigura un nivel înalt de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii. Aceste modificări vizează, de asemenea, uniformizarea terminologiei folosite în legislație, înlocuind sintagmele „incidente de securitate cibernetică" și „incidente de securitate" cu sintagma „incidente cibernetice", sintagma „sistemul de management al securității cibernetice" cu sintagma „sistemul de management al securității informației", asigurând corelarea cu noțiunile și terminologia din Legea nr. 48/2023 privind securitatea cibernetică. De asemenea, în vederea evitării unei interpretări rigide a termenului de „regulament intern de securitate cibernetică" ca un act propriu-zis și reieșind din abordarea practică a prezentului termen când acesta este un set de politici și instrucțiuni, se propune a fi substituit acesta cu „reglementări interne aplicabile", ceea ce oferă mai multă flexibilitatea în realizarea obiectivelor instituționale la asigurarea unui nivel corespunzător de securitate cibernetică în cadrul instituției. În ceea ce privește autorizarea terților să administreze rețelele și/sau sistemele informatice sau să găzduiască sisteme informatice, se propune completarea Cerințelor minime cu prevederi specifice, care să reglementeze responsabilitatea instituției și stipuleze că această rămâne responsabilă pentru aplicarea măsurilor de securitate chiar și atunci când apelează la serviciile unui terț, evitându-se exonerarea sa de responsabilitate. Adițional, se propune actualizarea prevederilor normative pentru a include competențele Agenției pentru Securitate Cibernetică și ale Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică", conform Legii nr. 48/2023 și altor acte normative, excluzând Ministerul Tehnologiei Informației și Comunicațiilor, care a fost absorbit în urma reorganizării administrației publice centrale.

Modificările propuse în pct. 6 din proiect vizează Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat și au ca obiectiv corelarea prevederilor acesteia cu prevederile Legii privind securitatea cibernetică în partea ce vizează obligațiile de notificare a Agenției pentru Securitate Cibernetică. Adițional, reieșind din faptul că desemnarea unei autorități competente la nivel național în domeniul securității cibernetice este o entitate nouă cu domenii noi de competențe, se propune completarea normelor care stabilesc obligativitatea cooperării CERT Gov inclusiv cu Agenția pentru Securitate Cibernetică și nemijlocit echipa de răspuns la incidentele cibernetice la nivel național, precum și remiterea raportului privind riscurile și incidentele de securitate cibernetică identificate, măsurile întreprinse și planificate pentru remedierea acestora în adresa Agenției pentru Securitate Cibernetică. Recepționarea și analiza raportului respectiv va permite Agenției să-și realizeze atât funcția de cercetare și dezvoltare a acesteia, cât și celelalte funcții care sunt stabilite în competența acesteia prin Regulamentul de organizare și funcționare a Agenției pentru Securitate Cibernetică, aprobat prin Hotărârea Guvernului nr. 1028/2023.

Totodată, sunt corelate funcțiile CERT Gov din Hotărârea de Guvern cu cele stabilite în Legea nr. 48/2023. În același timp, pentru asigurarea unei predictibilități pentru entitățile publice care notifică incidente cibernetice în adresa CERT Gov, este stabilită obligația pentru cei din urmă de a oferi un răspuns în termen de 24 ore, inclusiv se prevede posibilitatea pentru entitățile publice de a notifica și echipa de răspuns la incidente cibernetice la nivel național.

Suplimentar, similar ca și în cazul punctului 2 menționat supra, se propune ajustarea terminologiei și noțiunile la cele stabilite de Legea privind securitatea cibernetică, nemijlocit „incidente cibernetice" și „Centrul guvernamental de răspuns la incidentele cibernetice".

2. A doua categorie de modificări se referă nemijlocit la terminologie, vizând pct. 3 și 8. Aceste hotărâri de Guvern operează cu o terminologie diferită decât cea care se utilizează în Legea nr. 48/2023 privind securitatea cibernetică. În acest sens, se propun substituirea sintagmelor „incidente de securitate cibernetică” și „incidente de securitate” cu termenul „incidente cibernetice”, SI „RSISC” cu SI „RSIC”, „Centrul guvernamental de reacție la incidente de securitate cibernetică” cu „Centrul guvernamental de răspuns la incidentele cibernetice”. Suplimentar, se propune indicarea în clauza de adoptare la Hotărârea Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” a temeiului stabilit de art. 10 alin. (1) din Legea nr.48/2023 privind securitatea cibernetică.

3. A treia categorie vizează hotărârile de Guvern de la punctele 1, 3, 5, 7 și 9 și rezidă în alinierea și completarea hotărârilor de Guvern sectoriale cu Legea nr. 48/2023 privind securitatea cibernetică și legile care au ca obiect de reglementare a activități din domenii și subdomenii, corespondente sectoarelor sau subsectoarelor enumerate în anexele I și II ale Directivei NIS2 și pentru care sunt propuse modificări prin Legea nr. 58/2024 pentru modificarea unor acte normative, care a fost aprobată în lectura a doua de către Parlament la data de 21 martie 2024. Aceste modificări vin cu completări la prevederile generale privind limitele competenței de supraveghere și control, ce urmează a fi exercitată de Agenția pentru Securitate Cibernetică și obligațiile exprese de asigurare a securității cibernetice de către diferitele categorii de furnizori de servicii.

4. Ultima intervenție se referă la modificarea Regulamentului cu privire la tipurile şi modul de stabilire a sporurilor cu caracter specific aprobat prin Hotărârea Guvernului nr. 1231/2018 pentru punerea în aplicare a prevederilor Legii nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar. Această modificare urmărește corelarea și reflectarea la nivel de normă secundară a modificărilor propuse la art. 17 alin. (2) lit. b2) din Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar prin care se stabilește pentru Agenția pentru Securitate Cibernetică un spor cu caracter specific. În același timp, sunt indicate funcțiile și rolurile pentru care urmează a fi achitat sporul specific.

Totodată, proiectul prevede intrarea în vigoare a hotărârii de Guvern la data de 1 ianuarie 2025, cu excepția prevederilor punctului 4 care intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

Intrarea în vigoare este determinată de necesitatea urgentării asigurării condițiilor necesare pentru operaționalizarea Agenției pentru Securitate Cibernetică, proces care depinde direct de recrutarea angajaților cu calificarea suficientă și necesară realizării obiectivelor acestei autorități.

Astfel, recrutarea angajaților calificați va permite atingerea finalităților urmărite prin crearea Agenției pentru Securitate Cibernetică, și anume:

- consolidarea securității cibernetice la nivel general, asigurându-se protecția datelor și informațiilor, precum și reacția imediată la incidentele cibernetice;
- protecția infrastructurii informaționale critice și creșterea rezilienței în domeniul securității cibernetice în sectoarele esențiale: energetic, bancar, de transport etc.
- consolidarea capacităților autorităților și instituțiilor publice în materie de securitate cibernetică;
- implementarea unui mecanism obligatoriu de raportare a incidentelor cibernetice;
- reducerea riscului de întreruperi majore în funcționarea serviciilor importante prin asigurarea stabilității și continuității acestora.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Opțiunile alternative nu au fost analizate, deoarece proiectul urmărește alinierea cadrului normativ secundar la prevederile privind măsurile de securitate cibernetică stabilite de Legea nr. 48/2023 privind securitatea cibernetică.

4. Analiza impactului de reglementare
4.1. Impactul asupra sectorului public
Proiectul nu presupune careva reforme structurale sau instituționale, dar va avea impact asupra competențelor subdiviziunilor interne ale autorităților și instituțiilor publice. În acest sens, menționăm că în vederea asigurării unei abordări complexe și multidisciplinare a cerințelor de securitate, organizarea sistemului de management al securității informației se efectuează cu participarea tuturor subdiviziunilor instituției, definind clar rolurile acestora.
4.2. Impactul financiar și argumentarea costurilor estimative
Implementarea prevederilor proiectului nu necesită alocarea resurselor financiare suplimentare de la bugetul de stat pentru anul 2024, la subprogramul 1504 ,,Tehnologii informaționale" fiind prevăzută suma de 15 000,0 mii lei, dintre care cheltuieli de personal 12 449,2 mii lei.
4.3. Impactul asupra sectorului privat
Proiectul vine să completeze inițiativa de legiferare realizată prin Legea nr. 48/2023 privind securitatea cibernetică și legile conexe, având ca obiectiv primordial alinierea cadrului normativ secundar la legislația primară, respectiv, proiectul nu impune careva obligații suplimentare pentru sectorul privat decît cele stabilite prin Legea nr. 48/2023 privind securitatea cibernetică.
4.4. Impactul social 4.4.1. Impactul asupra datelor cu caracter personal 4.4.2. Impactul asupra echității și egalității de gen
Nu este aplicabil
4.5. Impactul asupra mediului
Nu este aplicabil
4.6. Alte impacturi și informații relevante
Nu este aplicabil
5. Compatibilitatea proiectului actului normativ cu legislația UE
5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională
Nu este aplicabil
5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE
Proiectul de hotărâre de Guvern are ca obiectiv aducerea în concordanță a hotărârilor de Guvern cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe. Legea nr. 48/2023 privind securitatea cibernetică a transpus parțial prevederile Directivei NIS2 (Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148).
6. Avizarea și consultarea publică a proiectului actului normativ
În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md, la data de 2 mai 2024 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de hotărâre de Guven (link de acces - https://particip.gov.md/ro/document/stages/anunt-de-initiere-a-procesului-de-elaborare-a-proiectului-hotararii-guvernului-pentru-modificarea-unor-hotarari-ale-guvernului-aducerea-actelor-normative-subsidiare-in-concordanta-cu-legea-nr-482023-privind-securitatea-cibernetica-si-legile-conexe/12512).

Totodată, proiectul a fost supus consultării prealabile procesului de avizare cu Ministerul Finanțelor, Instituția Publică „Agenția de Guverna Electronică” și Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”.

7. Concluziile expertizelor

Proiectul urmează a fi remis conform procedurii legale Centrului Național Anticorupție pentru efectuarea expertizei anticorupție a acestuia.

Proiectul nu are ca scop transpunerea directă a unor prevederi din Directiva (UE) 2022/2555, precum și nu instituie careva prevederi noi care contravin actului UE, inserând obligații generale aferente securității cibernetice pentru furnizorii de servicii în actele normative secundare.

Informația referitoare la concluziile expertizei privind compatibilitatea proiectului de hotărâre cu alte acte normative în vigoare, precum și respectarea normelor de tehnică legislativă va fi inclusă după recepționarea expertizei juridice.

Proiectul nu cade sub incidența altor expertize necesare de a fi efectuate în condițiile Legii nr.100/2017 cu privire la actele normative, dat fiind faptul că nu reglementează activitatea de întreprinzător, nu conține reglementări cu impact asupra bugetului public național sau a unor componente din cadrul acestuia și nu prevede reorganizări și reforme structurale sau instituționale ale autorităților ori ale instituțiilor publice. Prin urmare, proiectul nu cade sub incidența Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr.23/2019.

8. Modul de încorporare a actului în cadrul normativ existent

Proiectul elaborat se încadrează în prevederile cadrului normativ în vigoare, respectiv aprobarea acestuia nu implică necesitatea modificării altor acte normative. Totodată, având în vedere amploarea efectelor pe care le va avea proiectul de hotărâre de Guvern și modificările propuse prin Legea nr. 58/2024 pentru modificarea unor acte normative, este important ca autoritățile administrației publice centrale de specialitate, responsabile de realizarea politicii statului în domeniile reglementate de actele normative propuse spre adoptare, să efectueze o evaluare a actelor normative ale acestora în vederea identificării necesității de revizuire a acestora.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Măsurile de bază necesare pentru implementarea prevederilor proiectului constau în următoarele aspecte:

În partea ce ține implementarea modificărilor la Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr. 201/2017, urmează a fi create capacitățile necesare în cadrul autorităților și instituțiilor publice privind:

- recrutarea și instruirea persoanelor responsabile de punerea în aplicare a sistemului de management al securității cibernetice în instituție;
- analiza riscurilor periodic, dar nu mai rar de o dată pe an;
- efectuarea periodică a testului de penetrare în conformitate cu politica de securitate cibernetică a instituției și prezentarea rezultatelor testului Agenției pentru Securitate Cibernetică, în termen de o lună, împreună cu planul de remediere a deficiențelor depistate.”;

În partea ce ține de implementarea modificărilor punctului 8 din Statutul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică” aprobat prin Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, urmează a fi create capacitățile necesare în cadrul STISC în scopul asigurării securității rețelelor și sistemelor informatice proprietate a statului, și informării Agenției pentru Securitate Cibernetică cu privire la incidentele cibernetice notificate de autoritățile și instituțiile publice, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică;”;

În partea ce ține implementarea modificărilor la Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, urmează a fi create capacitățile necesare în cadrul CERT Gov privind:

- furnizarea entităților publice care au notificat un incident cibernetic imediat, însă nu mai târziu de 24 ore de la recepționarea notificării, unui răspuns cu privire la incidentul cibernetic care să cuprindă recomandări și instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv;";

- notificarea CSIRT-ul național, în condițiile stabilite de Legea nr. 48/2023 privind securitatea cibernetică, cu privire la incidentele cibernetice cu impact semnificativ asupra securității rețelelor sau sistemelor informatice ale statului ori asupra continuității serviciilor.

Secretar de stat **Cătălina PLINSCHI**

Tabel comparativ al proiectului de hotărâre de Guvern pentru modificarea unor hotărâri ale Guvernului

(aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)

	Prevederea actuală	**Modificarea propusă**	**Prevederea după modificare**
Regulile privind prestarea serviciilor poștale, adoptat prin Hotărârea Guvernului nr. 1457/2016			
1.	-	pct. 4 se completează cu subpunctul $4)^1$, cu următorul cuprins: „$4)^1$ securitatea rețelelor și sistemelor informatice utilizate la prestarea serviciilor poștale și, dacă sunt incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile de asigurare a securității cibernetice stabilite de legea respectivă.”.	Subpunct nou
2.	-	după pct. 136, se completează cu un punct nou *„136^1”* care va avea următorul cuprins: „*$136^1)$* Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat al	Punct nou

		respectării de către furnizorii de servicii poștale, incluși în Lista furnizorilor de servicii, a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică. Furnizorii de servicii poștale sunt obligați să ofere acces Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare realizării obiectivelor controlului.”.	
Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr. 201/2017			
3.	1. Cerinţele minime obligatorii de securitate cibernetică (în continuare – Cerinţe minime) se aplică în cadrul Cancelariei de Stat, ministerelor, altor autorităţi administrative centrale subordonate Guvernului, inclusiv al structurilor organizaţionale din sfera lor de competenţă (autorităţile administrative din subordine, serviciile publice desconcentrate şi cele aflate în subordine, instituţiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), al autorităților administrative	la pct. 1, textul *„:* *1) echipamentele (hardware) și produsele de program (software) existente în cadrul fiecărei instituţii;* *2) sistemele informatice, resursele și sistemele informaționale existente în instituție (în continuare – sisteme), precum și cele aflate la etapa de elaborare, testare și implementare.*” se substituie cu sintagma „*rețele și sisteme informatice (în continuare – sisteme).*”	1. Cerinţele minime obligatorii de securitate cibernetică (în continuare – Cerinţe minime) se aplică în cadrul Cancelariei de Stat, ministerelor, altor autorităţi administrative centrale subordonate Guvernului, inclusiv al structurilor organizaţionale din sfera lor de competenţă (autorităţile administrative din subordine, serviciile publice desconcentrate şi cele aflate în subordine, instituţiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), al autorităților administrative autonome și unităţilor cu autonomie financiară (în continuare – instituții) față de rețele și sisteme informatice (în continuare – sisteme).

	autonome și unităţilor cu autonomie financiară (în continuare – instituții) faţă de: 1) echipamentele (hardware) și produsele de program (software) existente în cadrul fiecărei instituţii; 2) sistemele informatice, resursele și sistemele informaționale existente în instituție (în continuare – sisteme), precum și cele aflate la etapa de elaborare, testare și implementare.		
4.	5. În sensul prezentelor Cerințe, următoarele noţiuni principale semnifică: … *cerințe minime obligatorii de securitate cibernetică* – sistemul de management al securității cibernetice – toate politicile, procedurile, planurile, procesele, practicile, rolurile, responsabilitățile, resursele și structurile care sînt folosite pentru a proteja și păstra intactă informaţia; ... Alţi termeni sînt utilizaţi în sensul definit de Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat, Legea nr.1069-XIV din 22 iunie 2000 cu privire la informatică şi Hotărîrea Guvernului nr. 811 din 29 octombrie 2015 „Cu privire la Programul	la pct. 5, textul „*Alţi termeni sînt utilizaţi în sensul definit de Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat, Legea nr.1069-XIV din 22 iunie 2000 cu privire la informatică şi Hotărîrea Guvernului nr. 811 din 29 octombrie 2015 „Cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020”.*”, se substituie cu textul „*Alţi termeni sînt utilizaţi în sensul definit de Legea nr. 48/2023 privind securitatea cibernetică, Legea nr. 467/2003 cu privire la informatizare şi la resursele informaţionale de stat şi Legea nr.1069/2000 cu privire la informatică.*”.	1. În sensul prezentelor Cerințe, următoarele noţiuni principale semnifică: … *cerințe minime obligatorii de securitate cibernetică* – <u>sistemul de management al securității informației</u> – toate politicile, procedurile, planurile, procesele, practicile, rolurile, responsabilitățile, resursele și structurile care sînt folosite pentru a proteja și păstra intactă informaţia; ... <u>Alţi termeni sînt utilizaţi în sensul definit de Legea nr. 48/2023 privind securitatea cibernetică, Legea nr. 467/2003 cu privire la informatizare şi la resursele informaţionale de stat şi Legea nr.1069/2000 cu privire la informatică.</u>”

	național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020”.	în tot textul, cuvintele *„sistemul de management al securității cibernetice”* la orice formă gramaticală, se substituie cu cuvintele *„sistemul de management al securității informației”* la forma gramaticală corespunzătoare.	
2.	7. Conducătorul autorității desemnează, prin act administrativ, persoana (subdiviziunea) responsabilă de punerea în aplicare a sistemului de management al securității cibernetice în instituție și prezintă Ministerului Tehnologiei Informației și Comunicațiilor informația respectivă în termen de cinci zile lucrătoare de la desemnarea acesteia.	la pct.7, textul *„Ministerului Tehnologiei Informației și Comunicațiilor”* se substituie cu textul „*Agenției pentru Securitate Cibernetică și Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică*”. în tot textul, cuvintele *„sistemul de management al securității cibernetice”* la orice formă gramaticală, se substituie cu cuvintele *„sistemul de management al securității informației”* la forma gramaticală corespunzătoare.	7. Conducătorul autorității desemnează, prin act administrativ, persoana (subdiviziunea) responsabilă de punerea în aplicare a sistemului de management al securității informației în instituție și prezintă Agenției pentru Securitate Cibernetică și Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică informația respectivă în termen de cinci zile lucrătoare de la desemnarea acesteia.
3.	-	se completează cu punctul *„7[1]*” care va avea următorul cuprins: „*7[1]*. În vederea asigurării unei abordări complexe și multidisciplinare a cerințelor de securitate, organizarea sistemului de management al securității informației se efectuează cu	*7[1]*. În vederea asigurării unei abordări complexe și multidisciplinare a cerințelor de securitate, organizarea sistemului de management al securității informației se efectuează cu participarea tuturor subdiviziunilor instituției, definind clar rolurile acestora.

		participarea tuturor subdiviziunilor instituției, definind clar rolurile acestora.”.	
4.	8. Persoana responsabilă are următoarele atribuții: 1) organizează sistemul de management al securității cibernetice în instituție conform sistemului de management al securității cibernetice; 2) participă, cel puțin o dată pe an, la cursurile de formare organizate de Ministerul Tehnologiei Informației și Comunicațiilor privind securitatea cibernetică și, respectiv, organizează cursuri pentru angajații instituției; 3) asigură elaborarea, implementarea și respectarea prevederilor următoarelor documente: planul de acțiuni pentru asigurarea securității cibernetice al instituției, politica de securitate cibernetică a instituției, planul de instruire și responsabilizare în securitatea cibernetică a personalului, regulamentele interne de securitate cibernetică, procedurile de recuperare.	pct. 8 va avea următorul cuprins: „*8*. Persoana (subdiviziunea) responsabilă are următoarele atribuții: 10) coordonează sistemul de management al securității informației în instituție; 11) participă, cel puțin o dată pe an, la cursuri de formare în domeniul securității cibernetice și, respectiv, organizează cursuri pentru angajații instituției; 12) coordonează elaborarea și implementarea: p) planului de acțiuni pentru asigurarea securității cibernetice al instituției; q) politicilor de securitate cibernetică a instituției; r) politicilor referitoare la analizarea riscurilor și asigurarea securității rețelelor și sistemelor informatice; s) politicilor și procedurilor privind gestionarea incidentelor cibernetice (prevenirea, detectarea și răspunsul la incidentele respective); t) politicilor și procedurilor privind utilizarea criptografiei și a criptării,	8. Persoana (subdiviziunea) responsabilă are următoarele atribuții: 1) coordonează sistemul de management al securității informației în instituție; 2) participă, cel puțin o dată pe an, la cursuri de formare în domeniul securității cibernetice și, respectiv, organizează cursuri pentru angajații instituției; 3) coordonează elaborarea și implementarea: a) planului de acțiuni pentru asigurarea securității cibernetice al instituției; b) politicilor de securitate cibernetică a instituției; c) politicilor referitoare la analizarea riscurilor și asigurarea securității rețelelor și sistemelor informatice; d) politicilor și procedurilor privind gestionarea incidentelor cibernetice (prevenirea, detectarea și răspunsul la incidentele respective);

		în special a criptării de la un capăt la altul; u) politicilor și procedurilor referitoare la evaluarea eficacității măsurilor de securitate implementate; v) măsurilor privind continuitatea activității și privind gestionarea crizelor; w) măsurilor de securitate aplicate în achiziționarea, dezvoltarea și întreținerea rețelelor și sistemelor informatice, inclusiv în divulgarea și gestionarea vulnerabilităților; x) măsurilor de securitate privind resursele umane, politicilor de control al accesului și de gestionare a activelor; y) măsurilor privind asigurarea securității lanțului de aprovizionare, inclusiv aspectele, legate de securitate, referitoare la relațiile furnizorului de servicii cu prestatorii sau cu furnizorii direcți de servicii ai acestuia; z) practicilor de bază în materie de igienă cibernetică și formarea în domeniul securității cibernetice; aa) soluțiilor de autentificare, de comunicații securizate voce, video și text; bb) sistemelor securizate de comunicații de urgență în cadrul furnizorului de servicii;	e) politicilor și procedurilor privind utilizarea criptografiei și a criptării, în special a criptării de la un capăt la altul; f) politicilor și procedurilor referitoare la evaluarea eficacității măsurilor de securitate implementate; g) măsurilor privind continuitatea activității și privind gestionarea crizelor; h) măsurilor de securitate aplicate în achiziționarea, dezvoltarea și întreținerea rețelelor și sistemelor informatice, inclusiv în divulgarea și gestionarea vulnerabilităților; i) măsurilor de securitate privind resursele umane, politicilor de control al accesului și de gestionare a activelor; j) măsurilor privind asigurarea securității lanțului de aprovizionare, inclusiv aspectele, legate de securitate, referitoare la relațiile furnizorului de servicii cu prestatorii sau cu furnizorii direcți de servicii ai acestuia; k) practicilor de bază în materie de igienă cibernetică și formarea în domeniul securității cibernetice; l) soluțiilor de autentificare, de comunicații securizate voce, video și text;

		cc) planului de instruire și responsabilizare în securitatea cibernetică a personalului; dd) reglementările interne pentru domeniul securității cibernetice; 13) asigură actualitatea documentației privind măsurile de securitate; 14) asigură monitorizarea situației privind securitatea rețelelor și sistemelor sale informatice, inclusiv în scopul detectării serviciilor TIC, proceselor TIC sau produselor TIC care compromit rețelele sau sistemele respective; 15) întreprinde măsuri orientate spre reducerea impactului și răspândirii incidentelor cibernetice, inclusiv, dacă este necesar, restricționează utilizarea sau accesul la rețelele și sistemele informatice; 16) verifică plenitudinea și conformitatea aplicării măsurilor de securitate, inclusiv prin efectuarea auditurilor de securitate, și documentează rezultatele verificării respective; 17) evaluează vulnerabilitățile și riscurile de securitate ale rețelelor și sistemelor informatice, determină gravitatea impactului unui eventual incident cibernetic survenit ca urmare a materializării riscurilor, descrie măsurile pentru soluționarea	m) sistemelor securizate de comunicații de urgență în cadrul furnizorului de servicii; n) planului de instruire și responsabilizare în securitatea cibernetică a personalului; o) reglementările interne pentru domeniul securității cibernetice; 4) asigură actualitatea documentației privind măsurile de securitate; 5) asigură monitorizarea situației privind securitatea rețelelor și sistemelor sale informatice, inclusiv în scopul detectării serviciilor TIC, proceselor TIC sau produselor TIC care compromit rețelele sau sistemele respective; 6) întreprinde măsuri orientate spre reducerea impactului și răspândirii incidentelor cibernetice, inclusiv, dacă este necesar, restricționează utilizarea sau accesul la rețelele și sistemele informatice; 7) verifică plenitudinea și conformitatea aplicării măsurilor de securitate, inclusiv prin efectuarea auditurilor de securitate, și documentează rezultatele verificării respective; 8) evaluează vulnerabilitățile și riscurile de securitate ale rețelelor și sistemelor informatice, determină gravitatea impactului

		unui incident cibernetic și întocmește un raport de evaluare în acest sens; 18) informează continuu conducerea cu privire la situația actuală a securității cibernetice.”.	unui eventual incident cibernetic survenit ca urmare a materializării riscurilor, descrie măsurile pentru soluționarea unui incident cibernetic și întocmește un raport de evaluare în acest sens; 9) informează continuu conducerea cu privire la situația actuală a securității cibernetice.
5.	9. Setul de documente se aprobă de conducătorul instituției și trebuie să fie revizuit cel puțin o dată pe an, dacă: … 2) au fost descoperite noi amenințări la securitatea sistemului; 3) s-a constatat o creștere bruscă a incidentelor de securitate asupra sistemului sau s-a depistat cel puțin un incident semnificativ de securitate a sistemului; …	la pct.9: a) cuvântul *„, dacă”* se substituie cu textul „*în următoarele cazuri, fără însă a se limita la acestea*”. b) la subpunctul 2) sintagma *„la securitatea sistemului”* se substituie cu sintagma „*cibernetice la sisteme*”. c) la subpunctul 3) sintagma *„semnificativ de securitate a sistemului”* se substituie cu sintagma „*cibernetic cu impact semnificativ asupra sistemului și asupra continuității serviciului ori asupra securității rețelei și/sau sistemului informatic*”. în tot textul, cuvintele „*incidente de securitate cibernetică*” și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele „*incidente*	9. Setul de documente se aprobă de conducătorul instituției și trebuie să fie revizuit cel puțin o dată pe an, în următoarele cazuri, fără însă a se limita la acestea: … 2) au fost descoperite noi amenințări cibernetice la sistem; 3) s-a constatat o creștere bruscă a incidentelor de securitate asupra sistemului sau s-a depistat cel puțin un incident cibernetic cu impact semnificativ asupra sistemului și asupra continuității serviciului ori asupra securității rețelei și/sau sistemului informatic; …

		cibernetice” la forma gramaticală corespunzătoare.	
6.	11. Politica de securitate cibernetică, în calitate de document instituțional, include: 1) scopul și obiectivele; 2) principiile de organizare internă a managementului de securitate cibernetică; ….	la pct. 11: a) subpunctul 1), după cuvântul „*obiectivele*” se completează cu textul „ *,corelate cu standardele în domeniul securității informației și în cel al securității cibernetice și cele mai bune practici pentru gestionarea incidentelor cibernetice și a riscurilor*;”. b) subpunctul 2), sintagma *„securitate cibernetică”* se substituie cu sintagma „*securitate a informației*”.	11. Politica de securitate cibernetică, în calitate de document instituțional, include: 1) scopul și obiectivele, corelate cu standardele în domeniul securității informației și în cel al securității cibernetice și cele mai bune practici pentru gestionarea incidentelor cibernetice și a riscurilor; 2) principiile de organizare internă a managementului de securitate a informației;
7.	12. Planul de instruire și responsabilizare în securitatea cibernetică a personalului instituției include: 1) instruirea în igiena și etica cibernetică (programe/cursuri de formare în domeniul securității cibernetice); 2) măsurile de securitate internă privind activitatea personalului (autorizație de acces, stabilirea drepturilor, obligațiilor, restricțiilor, responsabilizarea angajaților, monitorizarea, proceduri de asistență ale utilizatorilor în cazuri de urgență);	la pct. 12: a) subpunctul 2), după cuvântul *„personalului”* se completează cu textul *„ , inclusiv furnizorului extern de servicii”.* b) subpunctul 3) se abrogă.	12. Planul de instruire și responsabilizare în securitatea cibernetică a personalului instituției include: 1) instruirea în igiena și etica cibernetică (programe/cursuri de formare în domeniul securității cibernetice); 2) măsurile de securitate internă privind activitatea personalului, inclusiv furnizorului extern de servicii (autorizație de acces, stabilirea drepturilor, obligațiilor, restricțiilor, responsabilizarea angajaților, monitorizarea, proceduri de asistență ale utilizatorilor în cazuri de urgență).

	3) măsurile de securitate privind activitatea personalului/companiilor externe cooptate (coordonarea responsabilităților, acorduri de nedivulgare, autorizație de acces, monitorizare, planul de contingență (intervenție) pentru suspendarea operațiunilor de externalizare).		
8.	13. Regulamentele interne de securitate cibernetică prevăd: ...	la pct. 13, textul „*Regulamentele interne de securitate cibernetică*” se substituie cu textul „*Reglementări interne aplicabile în domeniul TIC*”.	13. <u>Reglementări interne aplicabile în domeniul TIC</u> prevăd: ....
9.	14. Procedurile de recuperare includ: 1) stabilirea procedurilor privind copierea de rezervă și de recuperare în cazul unui incident de securitate cibernetică; ...	în tot textul, cuvintele „*incidente de securitate cibernetică*” și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele „*incidente cibernetice*” la forma gramaticală corespunzătoare.	14. Procedurile de recuperare includ: 1) stabilirea procedurilor privind copierea de rezervă și de recuperare în cazul unui incident <u>cibernetic;</u>
10.	15. Controlul accesului se realizează după cum urmează: ... 5) utilizatorul sistemului trebuie să folosească în calitate de parolă o combinaţie din numere (0-9), caractere latine (minuscule şi majuscule) şi simboluri speciale (!#%), constituită din numărul minim de caractere,	în tot textul, cuvintele *„regulament intern de securitate cibernetică”* și *„regulament intern de securitate”* la orice formă gramaticală, se substituie cu cuvintele *„reglementări interne aplicabile”* la forma gramaticală corespunzătoare.	15. Controlul accesului se realizează după cum urmează: ... 5) utilizatorul sistemului trebuie să folosească în calitate de parolă o combinaţie din numere (0-9), caractere latine (minuscule şi majuscule) şi simboluri speciale (!#%), constituită din numărul minim de caractere, stabilit prin <u>reglementări interne aplicabile</u>, dar nu mai puțin de 7 caractere;

	stabilit prin regulamentul intern de securitate, dar nu mai puțin de 7 caractere; ... 9) datele despre activitățile în sistem (jurnalizarea) se stochează în timp real şi se păstrează pe perioada stabilită prin regulamentul intern de securitate, dar nu mai puțin de 6 luni; ... 11) managementul drepturilor de utilizator trebuie să asigure ca fiecare utilizator să poată face uz doar de drepturile sale. Verificarea activităților în sistem se realizează periodic, la etape de timp stabilite conform regulamentului intern de securitate, dar nu mai rar de o dată la 6 luni; ...		... 9) datele despre activitățile în sistem (jurnalizarea) se stochează în timp real şi se păstrează pe perioada stabilită prin <u>reglementări interne apicabile</u>, dar nu mai puțin de 6 luni; ... 11) managementul drepturilor de utilizator trebuie să asigure ca fiecare utilizator să poată face uz doar de drepturile sale. Verificarea activităților în sistem se realizează periodic, la etape de timp stabilite conform <u>reglementărilor interne aplicabile</u>, dar nu mai rar de o dată la 6 luni; ...
11.	16. Securitatea fizică presupune: 1) delimitarea clară a perimetrului rezervat diferitor grupuri de echipamente IT, alcătuirea planurilor camerelor de servere și a rețelelor; ... 3) controlul tehnic se efectuează periodic, conform regulamentului intern de securitate, și vizează:	la pct. 16, subpunctul 1), după sintagma „*grupuri de*” se completează cu sintagma „*angajați și*”. în tot textul, cuvintele *„regulament intern de securitate cibernetică”* și *„regulament intern de securitate”* la orice formă gramaticală, se substituie cu cuvintele *„reglementări interne*	16. Securitatea fizică presupune: 1) delimitarea clară a perimetrului rezervat diferitor grupuri de <u>angajați și</u> echipamente IT, alcătuirea planurilor camerelor de servere și a rețelelor; ...

	a) securitatea rețelelor, nodurilor și liniilor majore de interconectare cu rețele externe; b) evaluarea necesităților de instalare și utilizare a echipamentelor fără fir, conform regulamentului intern de securitate, securizarea conexiunilor fără fir (autorizarea echipamentelor și criptarea datelor); ... 4) aplicarea cerințelor de securitatea cibernetică la utilizarea rețelelor: a) caracteristicile echipamentelor şi produselor program pentru gestionarea fluxului de la/către utilizatori, conform regulamentului intern de securitate; ...	*aplicabile"* la forma gramaticală corespunzătoare.	3) controlul tehnic se efectuează periodic, conform regulamentului intern de securitate, și vizează: a) securitatea rețelelor, nodurilor și liniilor majore de interconectare cu rețele externe; b) evaluarea necesităților de instalare și utilizare a echipamentelor fără fir, conform <u>reglementărilor interne aplicabile,</u> securizarea conexiunilor fără fir (autorizarea echipamentelor și criptarea datelor); ... 4) aplicarea cerințelor de securitatea cibernetică la utilizarea rețelelor: a) caracteristicile echipamentelor şi produselor program pentru gestionarea fluxului de la/către utilizatori, conform <u>reglementărilor interne aplicabile</u>; ...
12.	17. Securitatea operațională stabilește că: .... 4) aplicarea cerințelor de securitatea cibernetică la utilizarea rețelelor: ...	la pct. 17, subpunctul 4), lit. c), textul „*private de rețelele adiacente*" se substituie cu textul „*instituției, precum și segmentarea acesteia în rețele în scopul protejării sistemelor, serviciilor și grupurilor de angajați*".	17. Securitatea operațională stabilește că: .... 4) aplicarea cerințelor de securitatea cibernetică la utilizarea rețelelor: ... c) echipamentele active de rețea trebuie configurate și testate astfel încît să asigure

	c) echipamentele active de rețea trebuie configurate și testate astfel încît să asigure izolarea reţelei private de reţelele adiacente; 5) elaborarea planului de continuitate, care va asigura restaurarea caracteristicilor sistemului și a datelor în caz de incident de securitate, care să includă: ...	în tot textul, cuvintele „*incidente de securitate cibernetică*” și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele „*incidente cibernetice*” la forma gramaticală corespunzătoare.	izolarea reţelei instituției, precum și segmentarea acesteia în rețele în scopul protejării sistemelor, serviciilor și grupurilor de angajați; 5) elaborarea planului de continuitate, care va asigura restaurarea caracteristicilor sistemului și a datelor în caz de incident cibernetic, care să includă: ...
13.	21. Securitatea operațională presupune: … 3) aplicarea regulilor de utilizare de către instituție a dispozitivelor mobile, aprobate ca document tehnic pentru toate autoritățile sus-menționate, care vor include: … 7) analiza riscurilor se efectuează periodic, dar nu mai rar de o dată la doi ani, și servește pentru ajustarea politicii de securitate cibernetică și a regulamentelor interne; … 9) efectuarea auditului intern de securitate anual, pînă la finele lunii ianuarie a anului următor, de către subdiviziunile responsabile de tehnologia informației, pentru a verifica:	la pct. 21: e) subpunctul 3), cuvântul „*autoritățile*” se substituie cu cuvântul „*instituțiile*”. f) subpunctul 7) va avea următorul cuprins: „*7)* analiza riscurilor se efectuează periodic, dar nu mai rar de o dată pe an, și servește pentru ajustarea politicii de securitate cibernetică și a reglementărilor interne aplicabile”. g) subpunctul 9) lit. b), cuvântul „*entități*” se substituie cu cuvântul „*instituției*”. h) subpunctul 10) va avea următorul cuprins: „*10)* efectuarea periodică a testului de penetrare în conformitate cu politica de securitate cibernetică a instituției.	21. Securitatea operațională presupune: … 3) aplicarea regulilor de utilizare de către instituție a dispozitivelor mobile, aprobate ca document tehnic pentru toate instituțiile sus-menționate, care vor include: … 7) analiza riscurilor se efectuează periodic, dar nu mai rar de o dată pe an, și servește pentru ajustarea politicii de securitate cibernetică și a reglementărilor interne aplicabile; … 9) efectuarea auditului intern de securitate anual, pînă la finele lunii ianuarie a anului următor, de către subdiviziunile responsabile de tehnologia informației, pentru a verifica:

	… b) prezența paravanului de protecție. Dacă necesităţile cer conectarea directă la Internet cu riscuri minime, se utilizează includerea în configuraţie a unei protecţii de tip „firewall”, pentru a facilita controlul traficului dintre reţeaua entităţii şi Internet, dar şi pentru a stopa intruziunea pachetelor de date externe, neautorizate; … 10) efectuarea periodică a testului de penetrare a sistemelor informaționale automatizate de importanță majoră se efectuează în conformitate cu politica de securitate cibernetică a instituției. Rezultatele testului sînt prezentate Ministerului Tehnologiei Informației și Comunicațiilor, în termen de o lună, împreună cu planul de remediere a deficiențelor depistate.	Rezultatele testului se prezintă Agenției pentru Securitate Cibernetică, în termen de o lună, împreună cu planul de remediere a deficiențelor depistate.”.	… … b) prezența paravanului de protecție. Dacă necesităţile cer conectarea directă la Internet cu riscuri minime, se utilizează includerea în configuraţie a unei protecţii de tip „firewall”, pentru a facilita controlul traficului dintre reţeaua <u>instituției</u> şi Internet, dar şi pentru a stopa intruziunea pachetelor de date externe, neautorizate; … 10) efectuarea periodică a testului de penetrare a sistemelor informaționale automatizate de importanță majoră se efectuează în conformitate cu politica de securitate cibernetică a instituției. Rezultatele testului sînt prezentate Ministerului Tehnologiei Informației și Comunicațiilor, în termen de o lună, împreună cu planul de remediere a deficiențelor depistate.
14.	**VI. CERINȚE DE SECURITATE LA EXTERNALIZAREA ADMINISTRĂRII/MENTENANŢEI SISTEMELOR** 23. În cazul în care instituția externalizează serviciile de administrare şi mentenanţă a sistemelor informaţionale și încheie un contract cu furnizorul extern de servicii,	capitolul VI va avea următorul cuprins: „**VI. CERINȚE DE SECURITATE ÎN RELAȚIILE CU PRESTATORII DE SERVICII** *23.* În cazul în care instituția încheie un contract cu furnizorul extern de servicii, contractul trebuie să includă și cerințe relevante de securitate,	**<u>VI. CERINȚE DE SECURITATE ÎN RELAȚIILE CU PRESTATORII DE SERVICII</u>** *<u>23.</u>* <u>În cazul în care instituția încheie un contract cu furnizorul extern de servicii, contractul trebuie să includă și cerințe relevante de securitate, convenite cu fiecare furnizor pe baza tipului de</u>

	contractul trebuie să includă și cerințe de securitate. Contractul va stabili, cel puțin: 1) reglementările interne de securitate cibernetică ale instituției pe care trebuie să le urmeze prestatorul de servicii în realizarea prevederilor contractuale; 2) serviciile externalizate; 3) cerințele precise pentru volumul și calitatea serviciilor externalizate documentate ca Service Level Agreement (SLA); 4) drepturile și obligațiile instituției și prestatorului de servicii externalizate: a) dreptul instituției de a monitoriza continuu calitatea serviciilor furnizate; b) dreptul instituției de a înainta prestatorului extern de servicii un titlu executoriu cu privire la aspectele legate de externalizarea de bună-credință, de înaltă calitate, executarea la timp și corectă a legilor și a regulamentelor; c) dreptul instituției de a înainta prestatorului extern de servicii o cerere scrisă motivată pentru încetarea imediată a contractului de externalizare, în cazul în care instituția a constatat că prestatorul extern de servicii nu respectă cerințele contractului de externalizare privind valoarea sau calitatea serviciului;	convenite cu fiecare furnizor pe baza tipului de relație cu acesta. Contractul trebuie să stabilească cel puțin: 4) reglementările interne de securitate cibernetică ale instituției pe care trebuie să le respecte prestatorul de servicii în realizarea prevederilor contractuale; 5) cerințele precise pentru volumul și calitatea serviciilor prestate, după caz documentate ca nivel agreat de servicii; 6) drepturile și obligațiile instituției și prestatorului de servicii: a) dreptul instituției de a monitoriza continuu calitatea serviciilor furnizate; b) dreptul instituției de a înainta prestatorului de servicii o prescripție cu privire la nerespectarea aspectelor legate de prestarea serviciilor de înaltă calitate, executarea la timp și corectă a actelor normative și reglementărilor interne ale instituției în domeniul securității cibernetice; c) dreptul instituției de a înainta prestatorului extern de servicii o cerere scrisă motivată pentru încetarea imediată a contractului de prestări servicii, în cazul în care instituția a constatat că prestatorul de servicii nu	relație cu acesta. Contractul trebuie să stabilească cel puțin: 7) reglementările interne de securitate cibernetică ale instituției pe care trebuie să le respecte prestatorul de servicii în realizarea prevederilor contractuale; 8) cerințele precise pentru volumul și calitatea serviciilor prestate, după caz documentate ca nivel agreat de servicii; 9) drepturile și obligațiile instituției și prestatorului de servicii: a) dreptul instituției de a monitoriza continuu calitatea serviciilor furnizate; b) dreptul instituției de a înainta prestatorului de servicii o prescripție cu privire la nerespectarea aspectelor legate de prestarea serviciilor de înaltă calitate, executarea la timp și corectă a actelor normative și reglementărilor interne ale instituției în domeniul securității cibernetice; c) dreptul instituției de a înainta prestatorului extern de servicii o cerere scrisă motivată pentru încetarea imediată a contractului de prestări servicii, în cazul în care instituția a constatat că prestatorul de servicii nu respectă cerințele contractului privind valoarea sau calitatea serviciului; d) obligația prestatorului de servicii de a furniza instituției informația privind monitorizarea continuă a calității serviciilor prestate;

	d) obligația prestatorului extern de servicii de a furniza instituției informația privind monitorizarea continuă a calității serviciilor de externalizare prestate; e) dreptul de audit al prestatorului de serviciu, dacă au fost notificate nonconformități critice.	respectă cerințele contractului privind valoarea sau calitatea serviciului; d) obligația prestatorului de servicii de a furniza instituției informația privind monitorizarea continuă a calității serviciilor prestate; e) de a pune la dispoziţia entității orice informaţie, ori de câte ori este necesar, privind serviciile externalizate; f) obligația prestatorului de servicii de a asigura că persoanele implicate în executarea contractului sunt instruite în mod corespunzător cu privire la rolurile și responsabilitățile lor înainte de a li se permite accesul la orice informație vizată în realizarea contractului respectiv; g) obligația prestatorului de servicii de a respecta reglementările interne ale instituției; e) dreptul de audit al prestatorului de serviciu, dacă au fost notificate nonconformități critice. *23[1]*. Instituția este responsabilă de măsurile de securitate în ce privește activitatea personalului prestatorilor de servicii, inclusiv coordonarea responsabilităților, acorduri de	e) de a pune la dispoziţia entității orice informaţie, ori de câte ori este necesar, privind serviciile externalizate; f) obligația prestatorului de servicii de a asigura că persoanele implicate în executarea contractului sunt instruite în mod corespunzător cu privire la rolurile și responsabilitățile lor înainte de a li se permite accesul la orice informație vizată în realizarea contractului respectiv; g) obligația prestatorului de servicii de a respecta reglementările interne ale instituției; e) dreptul de audit al prestatorului de serviciu, dacă au fost notificate nonconformități critice. *23[1]*. Instituția este responsabilă de măsurile de securitate în ce privește activitatea personalului prestatorilor de servicii, inclusiv coordonarea responsabilităților, acorduri de nedivulgare a informațiilor, autorizarea accesului și monitorizarea și planul de contingență (intervenție) în caz de întrerupere/încetare a prestării serviciilor.

		nedivulgare a informațiilor, autorizarea accesului și monitorizarea și planul de contingență (intervenție) în caz de întrerupere/încetare a prestării serviciilor.”.	
15.	24. Planul de răspuns la incidente stabilește că: 1) instituția trebuie să elaboreze și să pună în aplicare planul de răspuns de incidente cibernetice; 2) în cazul unor încălcări ale securității cibernetice, persoana responsabilă/subdiviziunea asigură imediata notificare, înregistrare și verificare a incidentelor de securitate cibernetică și punerea în aplicare a măsurilor de contracarare a acestora, conform procedurilor stabilite.	la pct. 24: a) subpunctul 1), sintagma „*răspuns de incidente cibernetice*” se substituie cu textul „*răspuns la incidente cibernetice, respectând măsurile privind continuitatea activității și privind gestionarea crizelor*”; b) subpunctul 2), după cuvântul *„stabilite”* se completează cu textul *„, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică”.*	Planul de răspuns la incidente stabilește că: 1) instituția trebuie să elaboreze și să pună în aplicare planul de răspuns la incidente cibernetice, respectând măsurile privind continuitatea activității și privind gestionarea crizelor; 2) în cazul unor încălcări ale securității cibernetice, persoana responsabilă/subdiviziunea asigură imediata notificare, înregistrare și verificare a incidentelor de securitate cibernetică și punerea în aplicare a măsurilor de contracarare a acestora, conform procedurilor stabilite, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică.
16.	24. Planul de răspuns la incidente stabilește că: 1) instituția trebuie să elaboreze și să pună în aplicare planul de răspuns de incidente cibernetice; 2) în cazul unor încălcări ale securității cibernetice, persoana responsabilă/subdiviziunea asigură imediata notificare, înregistrare și verificare a	în tot textul, cuvintele „*incidente de securitate cibernetică*” și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele „*incidente cibernetice*” la forma gramaticală corespunzătoare.	24. Planul de răspuns la incidente stabilește că: 1) instituția trebuie să elaboreze și să pună în aplicare planul de răspuns de incidente cibernetice; 2) în cazul unor încălcări ale securității cibernetice, persoana responsabilă/subdiviziunea asigură imediata notificare, înregistrare și verificare a incidentelor cibernetice și punerea în

	incidentelor de securitate cibernetică și punerea în aplicare a măsurilor de contracarare a acestora, conform procedurilor stabilite.		aplicare a măsurilor de contracarare a acestora, conform procedurilor stabilite.
Statutul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică" aprobat prin Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat			
17.	**8.** Serviciul are următoarele funcții: … 34) exercitarea rolului de către Centrul guvernamental de reacție la incidente de securitate cibernetică; ….	Punctul 8 5) se completează cu subpunctul „*20[1]*" cu următorul cuprins: „*20[1])* asigură securitatea rețelelor și sistemelor informatice proprietate a statului;". 6) se completează cu subpunctul „*31[1]*" cu următorul cuprins: „*31[1])* informează Agenția pentru Securitate Cibernetică cu privire la incidentele cibernetice notificate de autoritățile și instituțiile publice, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică;". 7) La subpunctul 34) cuvintele *„Centrul guvernamental de reacție la incidente de securitate cibernetică"* se substituie cu	**8.** Serviciul are următoarele funcții: … 20[1]) asigură securitatea rețelelor și sistemelor informatice proprietate a statului; ... 31[1]) informează Agenția pentru Securitate Cibernetică cu privire la incidentele cibernetice notificate de autoritățile și instituțiile publice, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică;". ... 34) exercitarea rolului de către Centrul guvernamental de răspuns la incidentele cibernetice; …

		cuvintele *„Centrul guvernamental de răspuns la incidentele cibernetice”*. 8) se completează cu subpunctul „*34[1]*” cu următorul cuprins: „*34[1])* facilitează interacțiunea dintre autoritățile și instituțiile publice cu Agenția pentru Securitate Cibernetică și echipa de răspuns la incidentele cibernetice la nivel național, inclusiv îndeplinirea de către acestea a obligațiilor privind securitatea cibernetică stabilite de Legea nr. 48/2023 privind securitatea cibernetică;”.	34[1]) facilitează interacțiunea dintre autoritățile și instituțiile publice cu Agenția pentru Securitate Cibernetică și echipa de răspuns la incidentele cibernetice la nivel național, inclusiv îndeplinirea de către acestea a obligațiilor privind securitatea cibernetică stabilite de Legea nr. 48/2023 privind securitatea cibernetică;
Regulamentul cu privire la tipurile şi modul de stabilire a sporurilor cu caracter specific, aprobat prin Hotărârea Guvernului nr. 1231/2018 pentru punerea în aplicare a prevederilor Legii nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar			
18.	-	se completează cu punctul „*5[1]*” cu următorul cuprins: ”*5[1]*. Pentru personalul Agenției pentru Securitate Cibernetică sporul cu caracter specific se acordă pentru exercitarea funcțiilor de: 1) răspuns la incidente și crize cibernetice la nivel național;	Punct nou.

		2) identificarea și evidența furnizorilor de servicii; 3) supravegherea și controlul de stat al respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice; 4) asigurarea cooperării la nivel național și internațional și schimb de informații în materie de securitate cibernetică, inclusiv rolul de punct național unic de contact; 5) orientare metodologică, reglementare, cercetare și dezvoltare în domeniul securității cibernetice, precum și pentru caracterul specific al suportului în realizarea funcțiilor Agenției pentru Securitate Cibernetică.”.	
19.	-	se completează cu punctul „*5[1]*” cu următorul cuprins: ”*5[1]*. Pentru personalul Agenției pentru Securitate Cibernetică sporul cu caracter specific se acordă pentru exercitarea funcțiilor de: 1) răspuns la incidente și crize cibernetice la nivel național;	Punct nou.

		2) identificarea și evidența furnizorilor de servicii; 3) supravegherea și controlul de stat al respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice; 4) asigurarea cooperării la nivel național și internațional și schimb de informații în materie de securitate cibernetică, inclusiv rolul de punct național unic de contact; 5) orientare metodologică, reglementare, cercetare și dezvoltare în domeniul securității cibernetice, precum și pentru caracterul specific al suportului în realizarea funcțiilor Agenției pentru Securitate Cibernetică.”.	
Regulamentul privind modul de utilizare a platformei de interoperabilitate (MConnect) aprobat prin Hotărârea Guvernului nr. 211/2019			
20.	6. Furnizorul de date are următoarele atribuții și responsabilități: ... 14) informează autoritatea competentă despre erorile apărute în procesul schimbului de date,	la pct. 6: a) subpunctul 14), textul *„ , inclusiv”,* se substituie cu cuvântul *„și”.*	6. Furnizorul de date are următoarele atribuții și responsabilități: ... 14) informează autoritatea competentă despre erorile apărute în procesul schimbului de date,

	vulnerabilitățile, inclusiv incidentele de securitate ale sistemelor informaționale conectate la platforma MConnect, imediat, iar dacă aceasta nu este posibil, în termen de cel mult două zile lucrătoare din momentul depistării acestora; 15) prezintă necondiționat autorității competente informația necesară pentru înlăturarea erorilor și vulnerabilităților, precum și pentru soluționarea incidentelor de securitate; …	b) subpunctul 15), după sintagma *„precum și pentru”* se completează cu sintagma *„prevenirea și”*.	vulnerabilitățile și incidentele de securitate ale sistemelor informaționale conectate la platforma MConnect, imediat, iar dacă aceasta nu este posibil, în termen de cel mult două zile lucrătoare din momentul depistării acestora; 15) prezintă necondiționat autorității competente informația necesară pentru înlăturarea erorilor și vulnerabilităților, precum și pentru prevenirea și soluționarea incidentelor de securitate; …
21.	8. Consumatorul de date are următoarele atribuții și responsabilități: ... 19) prezintă necondiționat autorității competente informația necesară pentru înlăturarea erorilor și a vulnerabilităților și pentru soluționarea incidentelor de securitate; ...	la pct. 8, subpunctul 19), după sintagma *„și pentru”* se completează cu sintagma *„prevenirea și”*.	8. Consumatorul de date are următoarele atribuții și responsabilități: ... 19) prezintă necondiționat autorității competente informația necesară pentru înlăturarea erorilor și a vulnerabilităților și pentru prevenirea și soluționarea incidentelor de securitate; ...
Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat			

22.	2. Instituţia Publică "Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" se desemnează în calitate de Centru guvernamental de reacţie la incidente de securitate cibernetică.	în tot textul hotărârii și anexei, cuvintele *„Centrul guvernamental de reacție la incidente de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„Centrul guvernamental de răspuns la incidentele cibernetice”* la forma gramaticală corespunzătoare.	2. Instituţia Publică "Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" se desemnează în calitate de Centrul guvernamental de răspuns la incidentele cibernetice.
23.	3. Centrul guvernamental de reacţie la incidente de securitate cibernetică va constitui punctul unic de contact şi de raportare a incidentelor de securitate cibernetică pentru structurile de tip CERT departamentale ale Guvernului.	în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare. în tot textul hotărârii și anexei, cuvintele *„Centrul guvernamental de reacție la incidente de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„Centrul guvernamental de răspuns la incidentele cibernetice”* la forma gramaticală corespunzătoare.	3. Centrul guvernamental de răspuns la incidentele cibernetice va constitui punctul unic de contact şi de raportare a incidentelor cibernetice pentru structurile de tip CERT departamentale ale Guvernului.
24.	4. Instituţia Publică "Serviciul Tehnologia Informaţiei şi Securitate Cibernetică", în termen de 9 luni, va crea şi va pune în aplicare Registrul de stat al incidentelor de securitate cibernetică.	în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident*	4. Instituţia Publică "Serviciul Tehnologia Informaţiei şi Securitate Cibernetică", în termen de 9 luni, va crea şi va pune în aplicare Registrul de stat al incidentelor cibernetice.

		cibernetic” la forma gramaticală corespunzătoare	
		<u>Anexa la Hotărârea Guvernului nr. 482/2020</u>	
25.	3. În sensul prezentei hotărâri, următoarele noțiuni semnifică: *CERT Gov* – Centru guvernamental de reacţie la incidente de securitate cibernetică, entitate care constituie punctul unic de contact şi de raportare a incidentelor de securitate cibernetică a Guvernului şi dispune de capacitatea necesară pentru prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice la nivel guvernamental; *CERT departamental* – subdiviziune sau persoană responsabilă desemnată în cadrul entităţilor publice care deţin infrastructuri/sisteme de tehnologia informaţiei şi comunicaţii şi care dispun de capacitatea necesară pentru a ţine evidenţa operativă obligatorie şi a raporta incidentele de securitate cibernetică; ...	la pct.3, textul „*incident de securitate cibernetică – eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică*” se substituie cu textul „*incident cibernetic – astfel cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică*”. în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare. în tot textul hotărârii și anexei, cuvintele *„Centrul guvernamental de reacţie la incidente de securitate cibernetică”,* la orice formă	3. În sensul prezentei hotărâri, următoarele noțiuni semnifică: *CERT Gov* – <u>Centrul guvernamental de răspuns la incidentele cibernetice</u>, entitate care constituie punctul unic de contact şi de raportare a <u>incidentelor cibernetice</u> a Guvernului şi dispune de capacitatea necesară pentru prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice la nivel guvernamental; *CERT departamental* – subdiviziune sau persoană responsabilă desemnată în cadrul entităţilor publice care deţin infrastructuri/sisteme de tehnologia informaţiei şi comunicaţii şi care dispun de capacitatea necesară pentru a ţine evidenţa operativă obligatorie şi a raporta <u>incidentele cibernetice</u>; ... *incident cibernetic* – astfel cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică”.

	incident de securitate cibernetică – eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică.	gramaticală, se substituie cu cuvintele *„Centrul guvernamental de răspuns la incidentele cibernetice”* la forma gramaticală corespunzătoare.	
26.	4. În vederea realizării atribuţiilor sale, CERT Gov are dreptul: … 3) să solicite informaţii de la structurile de tip CERT departamentale create în cadrul entităţilor publice privind incidentele de securitate cibernetică identificate în cadrul acestora, precum şi informaţii aferente acestora; …	în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare	4. În vederea realizării atribuţiilor sale, CERT Gov are dreptul: … 3) să solicite informaţii de la structurile de tip CERT departamentale create în cadrul entităţilor publice privind <u>incidentele cibernetice</u> identificate în cadrul acestora, precum şi informaţii aferente acestora; …
27.	5. CERT Gov are următoarele atribuții: ... 4) identifică, înregistrează, clasifică şi analizează incidente de securitate cibernetică şi coordonează, cooperează şi sesizează organele de drept, după caz; 5) oferă consultanţă şi elaborează recomandări de soluţionare şi prevenire a incidentelor de securitate; 6) întocmeşte date statistice şi elaborează rapoarte anuale cu privire la incidentele de	la pct. 5: - subpunctul 12), sintagma „*securitatea sistemelor informaționale și a rețelelor*” se substituie cu sintagma „*securitatea rețelelor și sistemelor informatice*”; - subpunctul 14) va avea următorul cuprins: „*14)* furnizează entităților publice care au notificat un incident cibernetic imediat, însă nu mai târziu de 24 ore de la recepționarea notificării, un răspuns cu privire la incidentul cibernetic care să cuprindă recomandări și instrucțiuni	5. CERT Gov are următoarele atribuții: … 4) identifică, înregistrează, clasifică şi analizează <u>incidentele cibernetice</u> şi coordonează, cooperează şi sesizează organele de drept, după caz; 5) oferă consultanţă şi elaborează recomandări de soluţionare şi prevenire a <u>incidentelor cibernetice</u>; 6) întocmeşte date statistice şi elaborează rapoarte anuale cu privire la <u>incidentele cibernerice</u> înregistrate, precum şi dinamica acestora;

	securitate înregistrate, precum şi dinamica acestora; 7) asigură evidenţa ameninţărilor, vulnerabilităţilor şi incidentelor de securitate cibernetică identificate sau raportate, tehnicilor şi tehnologiilor folosite pentru atacuri, precum şi a bunelor practici pentru protecţia infrastructurilor cibernetice; 8) oferă o platformă informaţională de comunicare strategică prin intermediul paginii sale web oficiale, care conţine informaţii despre incidente de securitate informaţională şi ghiduri de securitate; … 12) emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele către entitățile publice stabilite la punctul 5 din hotărâre, precum și către orice entitate publică căreia îi poate fi afectată securitatea sistemelor informaționale și a rețelelor; … 14) furnizează entităților publice care au făcut raportarea informații relevante în ceea ce privește acțiunile ulterioare raportării; 15) asigură răspunsul la incidente de securitate cibernetică;	operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv;". - subpunctul 16), după sintagma „*cooperează cu*", se completează cu textul „*echipa de răspuns la incidentele cibernetice la nivel național,* ". - după subpunctul 16), se completează cu subpunctele *„16[1]-16[3]*" care vor avea următorul cuprins: „*16[1])* asigură securitatea rețelelor și sistemelor informatice proprietate a statului; *16[2])* notifică echipa de răspuns la incidente cibernetice la nivel național, informează cu privire la incidentele cibernetice notificate de autoritățile și instituțiile publice, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică; *16[3])* facilitează interacțiunea dintre autoritățile și instituțiile publice cu Agenția pentru Securitate Cibernetică și echipa de răspuns la incidentele cibernetice la nivel național, inclusiv îndeplinirea de către acestea a obligațiilor privind securitatea cibernetică stabilite de Legea nr.	7) asigură evidenţa ameninţărilor, vulnerabilităţilor şi incidentelor cibernetice identificate sau raportate, tehnicilor şi tehnologiilor folosite pentru atacuri, precum şi a bunelor practici pentru protecţia infrastructurilor cibernetice; 8) oferă o platformă informaţională de comunicare strategică prin intermediul paginii sale web oficiale, care conţine informaţii despre incidente cibernetice şi ghiduri de securitate; … 12) emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele către entitățile publice stabilite la punctul 5 din hotărâre, precum și către orice entitate publică căreia îi poate fi afectată securitatea rețelelor și sistemelor informatice; … 14) furnizează entităților publice care au notificat un incident cibernetic imediat, însă nu mai târziu de 24 ore de la recepționarea notificării, un răspuns cu privire la incidentul cibernetic care să cuprindă recomandări și instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv; 15) asigură răspunsul la incidente cibernetice;

	16) cooperează cu CERT-urile departamentale și entitățile publice stabilite la punctul 5 din hotărâre, în cadrul unei platforme de management al incidentelor și schimbului de informații; … 18) întocmește și prezintă, trimestrial, către Serviciul de Informații și Securitate al Republicii Moldova un raport privind riscurile și incidentele de securitate cibernetică identificate, măsurile întreprinse și planificate pentru remedierea acestora.	48/2023 privind securitatea cibernetică;”. - subpunctul 18), sintagma „*Serviciul de Informații și Securitate al Republicii Moldova*”, se substituie cu sintagma „*Agenția pentru Securitate Cibernetică*”. în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*incidente de securitate informațională*”, la orice formă gramaticală, se substituie cu cuvintele „*incidente cibernetice*” la forma gramaticală corespunzătoare.	16) cooperează <u>cu echipa de răspuns la incidentele cibernetice la nivel național</u>, CERT-urile departamentale și entitățile publice stabilite la punctul 5 din hotărâre, în cadrul unei platforme de management al incidentelor și schimbului de informații; <u>16[1]) asigură securitatea rețelelor și sistemelor informatice proprietate a statului;</u> <u>16[2]) notifică echipa de răspuns la incidente cibernetice la nivel național informează cu privire la incidentele cibernetice notificate de autoritățile și instituțiile publice, respectând prevederile Legii nr. 48/2023 privind securitatea cibernetică;</u> <u>16[3]) facilitează interacțiunea dintre autoritățile și instituțiile publice cu Agenția pentru Securitate Cibernetică și echipa de răspuns la incidentele cibernetice la nivel național, inclusiv îndeplinirea de către acestea a obligațiilor privind securitatea cibernetică stabilite de Legea nr. 48/2023 privind securitatea cibernetică;</u> … 18) întocmește și prezintă, trimestrial, către <u>Agenția pentru Securitate Cibernetică</u> un raport privind riscurile și <u>incidentele cibernetice</u> identificate, măsurile întreprinse și planificate pentru remedierea acestora.

28.	6. În vederea exercitării rolului de CERT departamental, entităţile publice au următoarele drepturi: 1) să solicite consultanţă şi recomandări de soluţionare şi prevenire a incidentelor de securitate cibernetică; 2) să participe la atelierele de lucru în domeniul securităţii cibernetice; 3) să solicite informaţii cu privire la statutul incidentelor de securitate cibernetică raportate către CERT Gov; …	în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare	6. În vederea exercitării rolului de CERT departamental, entităţile publice au următoarele drepturi: 1) să solicite consultanţă şi recomandări de soluţionare şi prevenire a <u>incidentelor cibernetice</u>; 2) să participe la atelierele de lucru în domeniul securităţii cibernetice; 3) să solicite informaţii cu privire la statutul <u>incidentelor cibernetice</u> raportate către CERT Gov; …
29.	-	după punctul „6”, se completează cu un punct nou „6^1”, care va avea următorul cuprins: „6^1. *Notificarea incidentelor cibernetice cu impact semnificativ de către CERT* Gov către echipa de răspuns la incidente cibernetice la nivel național (*în continuare - CSIRT național*) cu privire la incidentele cibernetice, nu exclude dreptul entităților publice să notifice și CSIRT-ul național cu privire la incidentele cibernetice.”.	Punct nou.

		în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare.	
30.	7. În vederea exercitării rolului de CERT departamental, entitățile publice au următoarele atribuții: 1) desemnează, prin act administrativ, persoana (subdiviziunea) responsabilă de punerea în aplicare în cadrul entității publice a măsurilor necesare pentru asigurarea securității cibernetice; ... 3) raportează şi ţin evidenţa operativă obligatorie a incidentelor de securitate cibernetică în cadrul entităţii publice; 4) elaborează şi aplică metode de prevenire a incidentelor de securitate cibernetică; …	la pct. 7, subpunctul 1), textul *„necesare pentru asigurarea securității cibernetice”* se substituie cu textul *„tehnice și organizatorice pentru a gestiona riscurile de securitate a rețelelor și a sistemelor informatice pe care le utilizează”.* în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare.	7. În vederea exercitării rolului de CERT departamental, entitățile publice au următoarele atribuții: 1) desemnează, prin act administrativ, persoana (subdiviziunea) responsabilă de punerea în aplicare în cadrul entității publice a măsurilor <u>tehnice și organizatorice pentru a gestiona riscurile de securitate a rețelelor și a sistemelor informatice pe care le utilizează;</u> ... 3) raportează şi ţin evidenţa operativă obligatorie a <u>incidentelor cibernetice</u> în cadrul entităţii publice; 4) elaborează şi aplică metode de prevenire a <u>incidentelor cibernetice</u>; …

31.	8. CERT Gov va crea și asigura funcționarea unei platforme de management al incidentelor și schimbului de informații.	la pct. 8, sintagma *„CERT Gov”* se substituie cu sintagma *„Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”.*	8. Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică va crea și asigura funcționarea unei platforme de management al incidentelor și schimbului de informații.
32.	-	la pct. 11, subpunctul 3), după litera a) se completează cu o literă nouă *„a^1”* care va avea următorul cuprins: ”*a^1)* notifică CSIRT-ul național, în condițiile stabilite de Legea nr. 48/2023 privind securitatea cibernetică, cu privire la: - incidentele cibernetice cu impact semnificativ asupra securității rețelelor sau sistemelor informatice ale statului ori asupra continuității serviciilor; - incidentele cibernetice ale căror impact semnificativ asupra securității rețelelor sau sistemelor informatice ale statului ori asupra continuității serviciilor nu este evident, dar poate fi presupus în mod rezonabil, și - impactul semnificativ al unui incident cibernetic, care a afectat un terț, asupra continuității serviciului prestat de persoanele juridice de drept public, în cazul în care serviciului respectiv depinde de serviciile terțului afectat”.	Literă nouă.

33.	9. Interacţiunea privind incidentele de securitate cibernetică şi alte informaţii aferente se realizează prin: ...	în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare.	9. Interacţiunea privind incidentele cibernetice şi alte informaţii aferente se realizează prin: ...
34.	11. Securitatea cibernetică la nivel guvernamental se realizează prin următoarele măsuri întreprinse de către CERT Gov: 1) măsuri de prevenire: … e) formularea recomandărilor de prevenire a incidentelor de securitate cibernetică, inclusiv remiterea avertizărilor operative către entităţile publice supuse riscurilor şi către organele competente; … 2) măsuri de reacţie: a) tratarea incidentelor de securitate cibernetică şi oferirea recomandărilor de soluţionare a acestora; b) investigarea incidentelor de securitate cibernetică şi identificarea cauzei producerii acestora, inclusiv a măsurilor de prevenire	în tot textul hotărârii și anexei, cuvintele *„incident de securitate cibernetică”* și „*incidente de securitate*”, la orice formă gramaticală, se substituie cu cuvintele *„incident cibernetic”* la forma gramaticală corespunzătoare.	11. Securitatea cibernetică la nivel guvernamental se realizează prin următoarele măsuri întreprinse de către CERT Gov: 1) măsuri de prevenire: … e) formularea recomandărilor de prevenire a incidentelor cibernetice, inclusiv remiterea avertizărilor operative către entităţile publice supuse riscurilor şi către organele competente; … 2) măsuri de reacţie: a) tratarea incidentelor cibernetice şi oferirea recomandărilor de soluţionare a acestora; b) investigarea incidentelor cibernetice şi identificarea cauzei producerii acestora, inclusiv a măsurilor de prevenire care vor asigura depistarea la timp a unor incidente similare; c) sesizarea organelor de drept, după caz;

	care vor asigura depistarea la timp a unor incidente similare; c) sesizarea organelor de drept, după caz; 3) măsuri de contracarare: a) notificarea imediată a CERT-urilor departamentale cu privire la depistarea unor incidente de securitate cibernetică; … e) diseminarea rezultatelor analizei incidentelor de securitate cibernetică, cu respectarea prevederilor acordurilor de cooperare încheiate cu partenerii CERT Gov.		3) măsuri de contracarare: a) notificarea imediată a CERT-urilor departamentale cu privire la depistarea unor incidente cibernetice; … e) diseminarea rezultatelor analizei incidentelor cibernetice, cu respectarea prevederilor acordurilor de cooperare încheiate cu partenerii CERT Gov.
35.	12. La exercitarea atribuțiilor sale, în vederea asigurării securității sistemelor informaționale și rețelelor a căror afectare poate cauza daune securității naționale, CERT Gov se consultă și cooperează cu Serviciul de Informații și Securitate al Republicii Moldova.	pct. 12., la sfârșit se completează cu textul „ *și cu Agenția pentru Securitate Cibernetică*”.	12. La exercitarea atribuțiilor sale, în vederea asigurării securității sistemelor informaționale și rețelelor a căror afectare poate cauza daune securității naționale, CERT Gov se consultă și cooperează cu Serviciul de Informații și Securitate al Republicii Moldova și cu Agenția pentru Securitate Cibernetică.
Programul național de securitate în domeniul aviației civile aprobat prin Hotărârea Guvernului nr. 124/2021			
36.		punctul „*557[1]*” va avea următorul cuprins:	557[1]. Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” este responsabilă de asigurarea securității rețelelor și

		,*557[1]*. Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” este responsabilă de asigurarea securității rețelelor și sistemelor informatice proprietate a statului, de facilitarea îndeplinirii de către furnizorii de servicii persoane juridice de drept public a obligațiilor privind asigurarea securității cibernetice prevăzute de prezentul Program, inclusiv a celor privind notificarea, și de facilitarea interacțiunii acestora cu autoritatea competentă și echipa de răspuns la incidentele cibernetice la nivel național.”	sistemelor informatice proprietate a statului, de facilitarea îndeplinirii de către furnizorii de servicii persoane juridice de drept public a obligațiilor privind asigurarea securității cibernetice prevăzute de prezentul Program, inclusiv a celor privind notificarea, și de facilitarea interacțiunii acestora cu autoritatea competentă și echipa de răspuns la incidentele cibernetice la nivel național.
37.	557[2]. Atunci când administratorii de aeroporturi, transportatorii aerieni şi entităţile definite în programul naţional de securitate a aviaţiei civile fac obiectul unor cerinţe de securitate cibernetică naţională, STISC poate înlocui respectarea cerinţelor din prezentul Program cu respectarea prevederilor actelor normative naţionale.	în tot textul, cuvântul *„STISC”,* la orice formă gramaticală, se substituie cu sintagma *„Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”* la forma gramaticală corespunzătoare.	557[2]. Atunci când administratorii de aeroporturi, transportatorii aerieni şi entităţile definite în programul naţional de securitate a aviaţiei civile fac obiectul unor cerinţe de securitate cibernetică naţională, Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică poate înlocui respectarea cerinţelor din prezentul Program cu respectarea prevederilor actelor normative naţionale.
38.	-	după punctul „*560*”, se completează cu punctele „*560[1] și 560[2]*”, care vor avea următorul cuprins:	Puncte noi

		„*560[1]*. Operatorii aeroportuari, transportatorii aerieni, FSNA și alte entități definite în prezentul Program trebuie să asigure securitatea rețelelor și sistemelor informatice utilizate la prestarea serviciilor și, dacă sunt incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile de asigurare a securității cibernetice stabilite de legea respectivă. *560[2]*. Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat al respectării de către operatorii aeroportuari, transportatorii aerieni, FSNA și alte entități definite în prezentul Program, incluși în Lista furnizorilor de servicii, a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică. Aceștia sunt obligați să ofere acces Agenței pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare realizării obiectivelor controlului.”.	

Hotărârea Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”			
39.	**H O T Ă R Â R E** **cu privire la aprobarea Conceptului Sistemului informaţional** **"Registrul de stat al incidentelor de securitate cibernetică"**	în titlu și în textul hotărârii de Guvern cuvintele *„incidentelor de securitate cibernetică”* se substituie cu cuvintele *„incidentelor cibernetice”.*	**H O T Ă R Â R E** **cu privire la aprobarea Conceptului Sistemului informaţional** **"Registrul de stat al incidentelor cibernetice"**
40.	În temeiul art.22 lit.d) din Legea nr.467/2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr.6-12, art.44), cu modificările ulterioare, şi al art.16 din Legea nr.71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314), cu modificările ulterioare, Guvernul…	în clauza de adoptare, după cuvântul „*temeiul*”, se completează cu textul „ *art. 10 alin (1) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225),*”.	În temeiul art. 10 alin (1) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225), art.22 lit.d) din Legea nr.467/2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr.6-12, art.44), cu modificările ulterioare, şi al art.16 din Legea nr.71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314), cu modificările ulterioare, Guvernul…
41.	1. Se aprobă Conceptul Sistemului informaţional "Registrul de stat al incidentelor de securitate cibernetică" (se anexează).	în titlu și în textul hotărârii de Guvern cuvintele *„incidentelor de securitate cibernetică”* se substituie cu cuvintele *„incidentelor cibernetice”.*	1. Se aprobă Conceptul Sistemului informaţional "Registrul de stat al incidentelor cibernetice" (se anexează).

42.	2. Se instituie Registrul de stat al incidentelor de securitate cibernetică, proprietate a statului.	în titlu și în textul hotărârii de Guvern cuvintele *„incidentelor de securitate cibernetică”* se substituie cu cuvintele *„incidentelor cibernetice”.*	2. Se instituie Registrul de stat al incidentelor cibernetice, proprietate a statului.
43.	3. Crearea, implementarea, funcţionarea şi dezvoltarea Sistemului informaţional "Registrul de stat al incidentelor de securitate cibernetică" vor fi asigurate de către Instituţia Publică Serviciul Tehnologia Informaţiei şi Securitate Cibernetică.	în titlu și în textul hotărârii de Guvern cuvintele *„incidentelor de securitate cibernetică”* se substituie cu cuvintele *„incidentelor cibernetice”.*	3. Crearea, implementarea, funcţionarea şi dezvoltarea Sistemului informaţional "Registrul de stat al incidentelor cibernetice" vor fi asigurate de către Instituţia Publică Serviciul Tehnologia Informaţiei şi Securitate Cibernetică.
Anexă la Hotărârea Guvernului nr. 388/2022			
44.	**CONCEPTUL** **Sistemului informaţional *"Registrul de stat al incidentelor de securitate cibernetică"***	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare.	**CONCEPTUL** **Sistemului informaţional *"Registrul de stat al incidentelor cibernetice"***
45.	În conformitate cu prevederile art.10 alin.(1) din Legea nr.467/2003 cu privire la informatizare şi la resursele informaţionale de stat, ale Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul	cuvintele „*Centrul guvernamental de reacţie la incidente de securitate cibernetică*” se substituie cu cuvintele „*Centru guvernamental de răspuns la incidentele cibernetice*”. în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă	În conformitate cu prevederile art.10 alin.(1) din Legea nr.467/2003 cu privire la informatizare şi la resursele informaţionale de stat, ale Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării

	public şi de raţionalizare a administrării sistemelor informaţionale de stat, Instituţia Publică Serviciul Tehnologia Informaţiei şi Securitate Cibernetică (în continuare – STISC), în calitatea sa de Centru guvernamental de reacţie la incidente de securitate cibernetică (în continuare – CERT Gov), ce constituie punctul unic de contact şi de raportare a incidentelor de securitate cibernetică al Guvernului, asigură securitatea cibernetică a sistemelor şi resurselor informaţionale de stat. Una dintre atribuţiile STISC în calitate de CERT Gov este de a crea şi a pune în aplicare Registrul de stat al incidentelor de securitate cibernetică. De asemenea, conform pct.5 subpct. 7) şi 8) din Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020, CERT Gov are atribuţia de a oferi o platformă informaţională de comunicare strategică cu entităţile publice, precum şi de a asigura evidenţa ameninţărilor, vulnerabilităţilor în spaţiul cibernetic şi a incidentelor de securitate cibernetică identificate sau raportate. În prezent, pentru raportarea incidentelor de securitate cibernetică şi alte date aferente acestora se utilizează procese semiautomatizate, ceea ce presupune	gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	sistemelor informaţionale de stat, Instituţia Publică Serviciul Tehnologia Informaţiei şi Securitate Cibernetică (în continuare – STISC), în calitatea sa de Centru guvernamental de răspuns la incidentele cibernetice (în continuare – CERT Gov), ce constituie punctul unic de contact şi de raportare a incidentelor cibernetice ale Guvernului, asigură securitatea cibernetică a sistemelor şi resurselor informaţionale de stat. Una dintre atribuţiile STISC în calitate de CERT Gov este de a crea şi a pune în aplicare Registrul de stat al incidentelor cibernetice. De asemenea, conform pct.5 subpct. 7) şi 8) din Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020, CERT Gov are atribuţia de a oferi o platformă informaţională de comunicare strategică cu entităţile publice, precum şi de a asigura evidenţa ameninţărilor, vulnerabilităţilor în spaţiul cibernetic şi a incidentelor cibernetice identificate sau raportate. În prezent, pentru raportarea incidentelor cibernetice şi alte date aferente acestora se utilizează procese semiautomatizate, ceea ce presupune numeroase riscuri privind: securitatea informaţiei, integritatea datelor, istoricul modificărilor etc. Incidentele raportate sunt documentate conform unui şablon predefinit (formular de raportare a

	numeroase riscuri privind: securitatea informaţiei, integritatea datelor, istoricul modificărilor etc. Incidentele raportate sunt documentate conform unui şablon predefinit (formular de raportare a incidentelor de securitate cibernetică) şi remise prin poşta electronică, fiind înregistrate manual într-o bază de date în format .xls. Metoda actuală nu asigură realizarea unei analize comprehensive, care ar permite identificarea cauzelor şi a ariilor expuse riscului de securitate. Înregistrarea şi monitorizarea tuturor tipurilor de incidente de securitate cibernetică ar îmbunătăţi aspecte ce ţin de: definiţia, clasificarea, învăţarea din incidente. Astfel, apare necesitatea creării şi implementării Sistemului informaţional "Registrul de stat al incidentelor de securitate cibernetică" (în continuare – *SI RSISC*). Prin aceasta se urmăreşte îmbunătăţirea proceselor existente în cadrul CERT Gov, a modului de gestiune a incidentelor de securitate cibernetică, precum şi facilitarea raportării acestora pentru structurile de tip CERT departamentale ale Guvernului. Prezentul Concept stabileşte scopurile, sarcinile şi funcţiile SI RSISC, structura organizaţională şi baza normativă necesare		incidentelor de securitate cibernetică) şi remise prin poşta electronică, fiind înregistrate manual într-o bază de date în format .xls. Metoda actuală nu asigură realizarea unei analize comprehensive, care ar permite identificarea cauzelor şi a ariilor expuse riscului de securitate. Înregistrarea şi monitorizarea tuturor tipurilor de incidente cibernetice ar îmbunătăţi aspecte ce ţin de: definiţia, clasificarea, învăţarea din incidente. Astfel, apare necesitatea creării şi implementării Sistemului informaţional "Registrul de stat al incidentelor de securitate cibernetică" (în continuare – *SI RSIC*). Prin aceasta se urmăreşte îmbunătăţirea proceselor existente în cadrul CERT Gov, a modului de gestiune a incidentelor cibernetice, precum şi facilitarea raportării acestora pentru structurile de tip CERT departamentale ale Guvernului. Prezentul Concept stabileşte scopurile, sarcinile şi funcţiile SI RSIC, structura organizaţională şi baza normativă necesare pentru crearea şi exploatarea lui, obiectele informaţionale şi lista datelor care se păstrează în acesta, infrastructura tehnologică şi măsurile de securitate informaţională. În cadrul implementării şi exploatării SI RSIC, se va respecta Reglementarea tehnică "Procesele ciclului de viaţă ale software-ului RT 38370656-002:2006,

	pentru crearea şi exploatarea lui, obiectele informaţionale şi lista datelor care se păstrează în acesta, infrastructura tehnologică şi măsurile de securitate informaţională. În cadrul implementării şi exploatării SI RSISC, se va respecta Reglementarea tehnică "Procesele ciclului de viaţă ale software-ului RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaţionale nr.78/2006. Beneficiile implementării SI RSISC sunt: … 3) consolidarea unei baze de date electronice aferente incidentelor de securitate cibernetică; … 5) înregistrarea şi evidenţa totalităţii documentelor aferente incidentelor de securitate cibernetică; … 8) simplificarea procesului de introducere, modificare, actualizare a informaţiilor aferente incidentelor de securitate cibernetică; …		aprobată prin Ordinul ministrului dezvoltării informaţionale nr.78/2006. Beneficiile implementării SI RSIC sunt: … 3) consolidarea unei baze de date electronice aferente incidentelor cibernetice; … 5) înregistrarea şi evidenţa totalităţii documentelor aferente incidentelor cibernetice; … 8) simplificarea procesului de introducere, modificare, actualizare a informaţiilor aferente incidentelor cibernetice; … 11) asigurarea schimbului de date cu privire la incidentele cibernetice, în format electronic, între CERT Gov şi CERT departamentale, conform legislaţiei; 12) reducerea timpului mediu de raportare şi răspuns la incidentele cibernetice; …

	11) asigurarea schimbului de date cu privire la incidentele de securitate cibernetică, în format electronic, între CERT Gov şi CERT departamentale, conform legislaţiei; 12) reducerea timpului mediu de raportare şi răspuns la incidentele de securitate cibernetică; …		
46.	1.SI RSISC reprezintă totalitatea sistematizată de date privind incidentele cibernetice raportate prin punctul unic de contact CERT Gov, deţinătorii resurselor informaţionale afectate, precum şi privind documentele şi mijloacele de identificare a incidentelor de securitate cibernetică raportate.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	1.SI RSIC reprezintă totalitatea sistematizată de date privind incidentele cibernetice raportate prin punctul unic de contact CERT Gov, deţinătorii resurselor informaţionale afectate, precum şi privind documentele şi mijloacele de identificare a incidentelor cibernetice raportate.
47.	2. SI RSISC este parte componentă a resurselor informaţionale de stat ale Republicii Moldova.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	2. SI RSIC este parte componentă a resurselor informaţionale de stat ale Republicii Moldova.
48.	3. SI RSISC creează un spaţiu informaţional unitar, care reprezintă sursa oficială de	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă	3. SI RSIC creează un spaţiu informaţional unitar, care reprezintă sursa oficială de informaţie cu

	informaţie cu privire la ameninţările, vulnerabilităţile în spaţiul cibernetic şi incidentele de securitate cibernetică identificate sau raportate la nivel guvernamental.	gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	privire la ameninţările, vulnerabilităţile în spaţiul cibernetic şi incidentele cibernetice identificate sau raportate la nivel guvernamental.
49.	4. SI RSISC reprezintă un ansamblu de resurse şi tehnologii informaţionale, de mijloace de program şi metodologii, aflate în interconexiune şi destinate evidenţei şi gestionării incidentelor de securitate cibernetică în conformitate cu atribuţiile STISC în calitate de CERT Gov, care sunt prevăzute în Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	4. SI RSIC reprezintă un ansamblu de resurse şi tehnologii informaţionale, de mijloace de program şi metodologii, aflate în interconexiune şi destinate evidenţei şi gestionării incidentelor cibernetice în conformitate cu atribuţiile STISC în calitate de CERT Gov, care sunt prevăzute în Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020.
50.	5. Destinaţia SI RSISC constă în formarea Registrului de stat al incidentelor de securitate cibernetică, automatizarea procesului de înregistrare a incidentelor de securitate cibernetică, precum şi în documentarea şi gestionarea incidentelor de securitate cibernetică conform actelor normative.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	5. Destinaţia SI RSIC constă în formarea Registrului de stat al incidentelor cibernetice automatizarea procesului de înregistrare a incidentelor cibernetice, precum şi în documentarea şi gestionarea incidentelor cibernetice conform actelor normative.
51.	6. Crearea SI RSISC contribuie la soluţionarea unei probleme polivalente: pe de	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă	6. Crearea SI RSIC contribuie la soluţionarea unei probleme polivalente: pe de o parte, se elaborează

	o parte, se elaborează mecanismul care asigură automatizarea proceselor de identificare, înregistrare, clasificare şi analiză a incidentelor de securitate cibernetică, monitorizarea şi evidenţa alertelor, vulnerabilităţilor în spaţiul cibernetic şi incidentelor de securitate cibernetică identificate sau raportate, iar pe de altă parte, se constituie interacţiunea CERT departamentale cu CERT Gov privind incidentele de securitate cibernetică şi alte informaţii aferente securităţii cibernetice.	gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	mecanismul care asigură automatizarea proceselor de identificare, înregistrare, clasificare şi analiză a incidentelor de securitate cibernetică, monitorizarea şi evidenţa alertelor, vulnerabilităţilor în spaţiul cibernetic şi incidentelor cibernetice identificate sau raportate, iar pe de altă parte, se constituie interacţiunea CERT departamentale cu CERT Gov privind incidentele cibernetice şi alte informaţii aferente securităţii cibernetice.
52.	10. Scopul SI RSISC rezidă în: 1) asigurarea formării resurselor informaţionale de stat aferente incidentelor de securitate cibernetică; … 3) formarea bazei de date a incidentelor de securitate cibernetică la nivel guvernamental; 4) asigurarea evidenţei ameninţărilor, vulnerabilităţilor în spaţiul cibernetic şi a incidentelor de securitate cibernetică identificate sau raportate, a tehnicilor şi tehnologiilor folosite pentru atacuri, precum şi a bunelor practici pentru protecţia infrastructurilor cibernetice; …	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	10. Scopul SI RSIC rezidă în: 1) asigurarea formării resurselor informaţionale de stat aferente incidentelor cibernetice; … 3) formarea bazei de date a incidentelor cibernetice la nivel guvernamental; 4) asigurarea evidenţei ameninţărilor, vulnerabilităţilor în spaţiul cibernetic şi a incidentelor cibernetice identificate sau raportate, a tehnicilor şi tehnologiilor folosite pentru atacuri, precum şi a bunelor practici pentru protecţia infrastructurilor cibernetice; …

53.	11. Sarcinile de bază realizate la exploatarea SI RSISC sunt cele menţionate în pct.5 subpct. 1), 2), 4), 6) şi 8) din Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020, precum şi: 1) crearea şi menţinerea unei baze de date a incidentelor de securitate cibernetică şi a măsurilor întreprinse pentru înlăturarea şi contracararea acestora; ... 3) promovarea bunelor practici între specialiştii CERT Gov şi persoanele responsabile de răspuns la incidente de securitate cibernetică din cadrul entităţilor publice.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	11. Sarcinile de bază realizate la exploatarea SI RSIC sunt cele menţionate în pct.5 subpct. 1), 2), 4), 6) şi 8) din Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020, precum şi: 1) crearea şi menţinerea unei baze de date a incidentelor cibernetice şi a măsurilor întreprinse pentru înlăturarea şi contracararea acestora; ... 3) promovarea bunelor practici între specialiştii CERT Gov şi persoanele responsabile de răspuns la incidente cibernetice din cadrul entităţilor publice.
54.	12. Principiile de bază ale SI RSISC sunt: …	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	12. Principiile de bază ale SI RSIC sunt: …
55.	**III. SPAŢIUL JURIDICO-NORMATIV AL FUNCŢIONĂRII SI RSISC**	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	**III. SPAŢIUL JURIDICO-NORMATIV AL FUNCŢIONĂRII SI RSIC**
56.	13. Cadrul normativ aferent creării şi implementării SI RSISC include următoarele acte normative: …	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	13. Cadrul normativ aferent creării şi implementării SI RSIC include următoarele acte normative: …

57.	14. La elaborarea şi implementarea SI RSISC se vor respecta următoarele standarde tehnice: …	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	14. La elaborarea şi implementarea SI RSIC se vor respecta următoarele standarde tehnice: …
58.	**IV. SPAŢIUL FUNCŢIONAL AL SI RSISC**	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	**IV. SPAŢIUL FUNCŢIONAL AL SI RSIC**
59.	15. Contururile funcţionale principale ale SI RSISC sunt prezentate în figura 1, acestea fiind: … 2) conturul "Platformă de management al incidentelor şi schimb de informaţii" – platforma preia informaţiile aferente incidentelor de securitate cibernetică din documentele de intrare sau din cadrul conturului funcţional "Sistem de alertă timpurie şi reacţie în timp real privind incidentele cibernetice". Informaţiile respective sunt prelucrate ulterior prin intermediul instrumentelor automatizate de analiză şi încorporate în platforma de management. Conturul realizează următoarele funcţii: a) formarea bazei de date a SI RSISC. Se asigură evidenţa primară a incidentelor de securitate cibernetică şi actualizarea sistematică a bazei de date a incidentelor de	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	**15.** Contururile funcţionale principale ale SI RSIC sunt prezentate în figura 1, acestea fiind: … 2) conturul "Platformă de management al incidentelor şi schimb de informaţii" – platforma preia informaţiile aferente incidentelor cibernetice din documentele de intrare sau din cadrul conturului funcţional "Sistem de alertă timpurie şi reacţie în timp real privind incidentele cibernetice". Informaţiile respective sunt prelucrate ulterior prin intermediul instrumentelor automatizate de analiză şi încorporate în platforma de management. Conturul realizează următoarele funcţii: a) formarea bazei de date a SI RSIC. Se asigură evidenţa primară a incidentelor cibernetice şi actualizarea sistematică a bazei de date a incidentelor cibernetice, la modificarea sau completarea datelor obiectelor de evidenţă; b) asigurarea informaţională. Informaţia se pune la dispoziţia autorităţilor competente. Nivelul de acces al beneficiarilor SI RSIC va fi stabilit în

	securitate cibernetică, la modificarea sau completarea datelor obiectelor de evidenţă; b) asigurarea informaţională. Informaţia se pune la dispoziţia autorităţilor competente. Nivelul de acces al beneficiarilor SI RSISC va fi stabilit în Regulamentul privind modul de ţinere a Registrului de stat al incidentelor de securitate cibernetică format de SI RSISC; c) gestionarea incidentelor de securitate. Se asigură înregistrarea, clasificarea, analiza incidentelor de securitate cibernetică. De asemenea, are loc evidenţa ameninţărilor şi vulnerabilităţilor în spaţiul cibernetic şi a incidentelor de securitate cibernetică identificate sau raportate, a tehnicilor şi tehnologiilor folosite pentru atacuri cibernetice; d) asigurarea răspunsului la incidente de securitate cibernetică. Conturul respectiv recepţionează raportări privind incidentele de securitate cibernetică care afectează sistemele informaţionale şi reţelele entităţilor publice, precum şi furnizează entităţilor care au făcut raportarea informaţii relevante în ceea ce priveşte acţiunile ulterioare raportării; e) întocmirea datelor statistice şi elaborarea rapoartelor aferente incidentelor de securitate cibernetică;		Regulamentul privind modul de ţinere a Registrului de stat al incidentelor cibernetice format de SI RSIC; c) gestionarea incidentelor de securitate. Se asigură înregistrarea, clasificarea, analiza incidentelor cibernetice. De asemenea, are loc evidenţa ameninţărilor şi vulnerabilităţilor în spaţiul cibernetic şi a incidentelor cibernetice identificate sau raportate, a tehnicilor şi tehnologiilor folosite pentru atacuri cibernetice; d) asigurarea răspunsului la incidentelor cibernetice. Conturul respectiv recepţionează raportări privind incidentelor cibernetice care afectează sistemele informaţionale şi reţelele entităţilor publice, precum şi furnizează entităţilor care au făcut raportarea informaţii relevante în ceea ce priveşte acţiunile ulterioare raportării; e) întocmirea datelor statistice şi elaborarea rapoartelor aferente incidentelor cibernetice; f) publicarea alertelor şi atenţionărilor privind apariţia unor activităţi premergătoare atacurilor cibernetice; g) asigurarea securităţii informaţiei. Securitatea informaţiei se asigură la toate etapele de colectare, păstrare şi utilizare a resurselor informaţionale de stat; 3) conturul "Platformă informaţională de comunicare strategică" – asigură comunicarea

	f) publicarea alertelor şi atenţionărilor privind apariţia unor activităţi premergătoare atacurilor cibernetice; g) asigurarea securităţii informaţiei. Securitatea informaţiei se asigură la toate etapele de colectare, păstrare şi utilizare a resurselor informaţionale de stat; 3) conturul "Platformă informaţională de comunicare strategică" – asigură comunicarea măsurilor necesare pentru prevenirea şi răspunsul la incidente de securitate cibernetică pentru entităţile publice. Materialele furnizate de platforma informaţională de comunicare strategică, precum ghidurile de securitate, bunele practici şi recomandările, sunt publicate în scopul diseminării informaţiilor privind riscurile de securitate cibernetică care pot afecta sistemele informaţionale şi reţelele. În baza informaţiilor furnizate de contururile funcţionale "Sistem de alertă timpurie şi reacţie în timp real privind incidentele cibernetice" şi "Platformă de management al incidentelor şi schimb de informaţii", specialiştii CERT Gov vor identifica şi vor promova informaţii relevante în scopul consolidării capacităţii de reacţie la atacuri cibernetice. Conturul realizează următoarele funcţii:		măsurilor necesare pentru prevenirea şi răspunsul la incidentelor cibernetice pentru entităţile publice. Materialele furnizate de platforma informaţională de comunicare strategică, precum ghidurile de securitate, bunele practici şi recomandările, sunt publicate în scopul diseminării informaţiilor privind riscurile de securitate cibernetică care pot afecta sistemele informaţionale şi reţelele. În baza informaţiilor furnizate de contururile funcţionale "Sistem de alertă timpurie şi reacţie în timp real privind incidentele cibernetice" şi "Platformă de management al incidentelor şi schimb de informaţii", specialiştii CERT Gov vor identifica şi vor promova informaţii relevante în scopul consolidării capacităţii de reacţie la atacuri cibernetice. Conturul realizează următoarele funcţii: a) promovarea acţiunilor de sensibilizare şi informare privind ameninţările, vulnerabilităţile în spaţiul cibernetic, riscurile de securitate cibernetică şi măsurile de protecţie necesare; b) diseminarea informaţiilor de securitate cibernetică, inclusiv a rezultatelor analizei incidentelor cibernetice, cu respectarea prevederilor acordurilor de cooperare; c) informarea privind desfăşurarea exerciţiilor şi a atelierelor de lucru în domeniul securităţii cibernetice;

	a) promovarea acţiunilor de sensibilizare şi informare privind ameninţările, vulnerabilităţile în spaţiul cibernetic, riscurile de securitate cibernetică şi măsurile de protecţie necesare; b) diseminarea informaţiilor de securitate cibernetică, inclusiv a rezultatelor analizei incidentelor de securitate cibernetică, cu respectarea prevederilor acordurilor de cooperare; c) informarea privind desfăşurarea exerciţiilor şi atelierelor de lucru în domeniul securităţii cibernetice; d) publicarea ghidurilor de securitate cibernetică şi a recomandărilor de soluţionare a incidentelor de securitate cibernetică. … **Figura 1.** *Contururile funcţionale de bază ale SI RSISC*		d) publicarea ghidurilor de securitate cibernetică şi a recomandărilor de soluţionare a <u>incidentelor cibernetice</u>. … **Figura 1.** *Contururile funcţionale de bază ale <u>SI RSIC</u>*
60.	16. SI RSISC stabileşte interconexiunea modulelor de lucru şi urmează să îndeplinească, în primul rând, funcţiile specifice determinate de obiectivele, scopurile şi destinaţia prezentului Concept. Pe lângă funcţiile de bază, SI RSISC va asigura realizarea unor funcţii auxiliare necesare bunei funcţionări a acestuia.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	16. <u>SI RSIC</u> stabileşte interconexiunea modulelor de lucru şi urmează să îndeplinească, în primul rând, funcţiile specifice determinate de obiectivele, scopurile şi destinaţia prezentului Concept. Pe lângă funcţiile de bază, <u>SI RSIC</u> va asigura realizarea unor funcţii auxiliare necesare bunei funcţionări a acestuia.

61.	18. SI RSISC va recunoaşte cel puţin 3 tipuri de utilizatori, după cum sunt indicaţi în figura 2: 1) utilizatori interni – utilizatori cu drepturi depline asupra datelor şi funcţionalităţilor disponibile ale SI RSISC; 2) registrator – utilizator care operează, introduce sau modifică datele din cadrul SI RSISC, dar nu configurează însuşi funcţionalităţile sistemului; 3) vizitator – utilizator care are acces la vizualizarea informaţiei, fără drepturi de a introduce/modifica/şterge date din cadrul sistemului. … **Figura 2.** *Utilizatorii sistemului SI RSISC*	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	18. SI RSIC va recunoaşte cel puţin 3 tipuri de utilizatori, după cum sunt indicaţi în figura 2: 1) utilizatori interni – utilizatori cu drepturi depline asupra datelor şi funcţionalităţilor disponibile ale SI RSIC; 2) registrator – utilizator care operează, introduce sau modifică datele din cadrul SI RSIC, dar nu configurează însuşi funcţionalităţile sistemului; 3) vizitator – utilizator care are acces la vizualizarea informaţiei, fără drepturi de a introduce/modifica/şterge date din cadrul sistemului. … **Figura 2.** *Utilizatorii sistemului SI RSIC*
62.	19. Registratorul sistemului va avea acces la principalele funcţionalităţi ale SI RSISC, în concordanţă cu atribuţiile oferite de către posesor, conform figurii 3.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	19. Registratorul sistemului va avea acces la principalele funcţionalităţi ale SI RSIC, în concordanţă cu atribuţiile oferite de către posesor, conform figurii 3.
63.	**V. STRUCTURA ORGANIZAŢIONALĂ A SI RSISC**	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	**V. STRUCTURA ORGANIZAŢIONALĂ A SI RSIC**
64.	21. Proprietarul SI RSISC este statul.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	21. Proprietarul SI RSIC este statul.

65.	22. Posesorul SI RSISC este STISC, în calitate de CERT Gov, care are drept de gestionare şi de utilizare a datelor şi a resurselor informaţionale şi exercită atribuţiile deţinătorului şi administratorului tehnic al sistemului.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	22. Posesorul SI RSIC este STISC, în calitate de CERT Gov, care are drept de gestionare şi de utilizare a datelor şi a resurselor informaţionale şi exercită atribuţiile deţinătorului şi administratorului tehnic al sistemului.
66.	23. Registratorii SI RSISC sunt entităţile publice declarate conform Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat, precum şi specialiştii CERT Gov.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	23. Registratorii SI RSIC sunt entităţile publice declarate conform Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat, precum şi specialiştii CERT Gov.
67.	24. Furnizorii datelor în SI RSISC sunt STISC, în calitate de CERT Gov, entităţile publice declarate conform Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat şi entităţile	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	23. Registratorii SI RSIC sunt entităţile publice declarate conform Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat, precum şi specialiştii CERT Gov.

	publice care au atribuţii de asigurare a securităţii statului, cu următoarele funcţii: …		
68.	25. Destinatari şi utilizatori ai datelor din SI RSISC sunt angajaţii CERT Gov, entităţile publice, precum şi cele care au atribuţii de asigurare a securităţii statului. Drepturile şi obligaţiile destinatarului datelor registrului se stabilesc de legislaţia privind accesul la informaţie şi de legislaţia cu privire la schimbul de date şi interoperabilitate.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	25. Destinatari şi utilizatori ai datelor din SI RSIC sunt angajaţii CERT Gov, entităţile publice, precum şi cele care au atribuţii de asigurare a securităţii statului. Drepturile şi obligaţiile destinatarului datelor registrului se stabilesc de legislaţia privind accesul la informaţie şi de legislaţia cu privire la schimbul de date şi interoperabilitate.
69.	**VI. CLASIFICAREA DOCUMENTELOR SI RSISC**	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	**VI. CLASIFICAREA DOCUMENTELOR SI RSIC**
70.	26. În cadrul SI RSISC sunt folosite următoarele categorii de documente: 1) documente de intrare – în baza cărora sunt înregistrate incidentele de securitate cibernetică raportate; … 3) documente de ieşire – documente obţinute în urma funcţionării sistemului, precum rapoarte, statistici, diagrame aferente incidentelor de securitate cibernetică înregistrate; …	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	24. Furnizorii datelor în SI RSIC sunt STISC, în calitate de CERT Gov, entităţile publice declarate conform Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat şi entităţile publice care au atribuţii de asigurare a securităţii statului, cu următoarele funcţii: …

71.	28. Fiecare incident de securitate cibernetică înregistrat va stoca istoria modificărilor, documentele interne ale CERT Gov aferente prelucrării informaţiilor de intrare, precum şi documentele de ieşire generate în final de SI RSISC.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	28. Fiecare incident de securitate cibernetică înregistrat va stoca istoria modificărilor, documentele interne ale CERT Gov aferente prelucrării informaţiilor de intrare, precum şi documentele de ieşire generate în final de SI RSIC.
72.	29. Din categoria documentelor interne fac parte rapoartele de analiză a incidentelor de securitate cibernetică generate de instrumentele de lucru ale conturului funcţional "Platformă de management al incidentelor de securitate informaţională şi schimb de informaţii", ale cărui informaţii sunt ulterior folosite ca bază în gestionarea incidentului de securitate raportat.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare.	29. Din categoria documentelor interne fac parte rapoartele de analiză a incidentelor cibernetice generate de instrumentele de lucru ale conturului funcţional "Platformă de management al incidentelor de securitate informaţională şi schimb de informaţii", ale cărui informaţii sunt ulterior folosite ca bază în gestionarea incidentului cibernetic raportat.
73.	30. Sistemul include o serie de documente şi mijloace tehnologice, precum: imagini scanate ale documentelor, cuvinte-cheie ce facilitează căutarea incidentelor, lista utilizatorilor şi drepturilor acestora, versiunile documentelor şi modificările acestora; rapoartele şi statisticile agregate privind utilizarea SI RSISC.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	30. Sistemul include o serie de documente şi mijloace tehnologice, precum: imagini scanate ale documentelor, cuvinte-cheie ce facilitează căutarea incidentelor, lista utilizatorilor şi drepturilor acestora, versiunile documentelor şi modificările acestora; rapoartele şi statisticile agregate privind utilizarea SI RSIC.
74.	31. Documentele de ieşire ale SI RSISC sunt: informaţiile privind statutul incidentelor cibernetice, scrisorile de notificare aferente statutului incidentelor de securitate cibernetică către raportorii incidentului de securitate cibernetică şi recomandările emise	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare.	31. Documentele de ieşire ale SI RSIC sunt: informaţiile privind statutul incidentelor cibernetice, scrisorile de notificare aferente statutului incidentelor cibernetice către raportorii incidentelor cibernetice şi recomandările emise de

	de către specialiştii CERT Gov (ex.: bune practici, anexe aferent incidentelor notificate).	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	către specialiştii CERT Gov (ex.: bune practici, anexe aferent incidentelor notificate).
75.	**VII. SPAŢIUL INFORMAŢIONAL AL SI RSISC**	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	**VII. SPAŢIUL INFORMAŢIONAL AL SI RSIC**
76.	33. Obiectele informaţionale de bază ale SI RSISC sunt: ...	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	33. Obiectele informaţionale de bază ale SI RSIC sunt: ...
77.	34. Totalitatea identificatorilor obiectelor informaţionale sunt determinate de scopul şi destinaţia SI RSISC şi includ colectarea următoarelor informaţii: ... 3) date aferente incidentelor de securitate cibernetică; ... 6) date de identificare a utilizatorilor autorizaţi ai SI RSISC împrumutate din alte sisteme informaţionale de stat, conform pct.46.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	34. Totalitatea identificatorilor obiectelor informaţionale sunt determinate de scopul şi destinaţia SI RSIC şi includ colectarea următoarelor informaţii: ... 3) date aferente incidentelor cibernetice; ... 6) date de identificare a utilizatorilor autorizaţi ai SI RSIC împrumutate din alte sisteme informaţionale de stat, conform pct.46.
78.	35. Obiectul informaţional "Incident de securitate cibernetică" va conţine 2 scenarii de bază: 1) incident de securitate cibernetică tipic – se referă la un caz de incident de securitate cibernetică înregistrat şi gestionat în cadrul SI	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	35. Obiectul informaţional "Incident de securitate cibernetică" va conţine 2 scenarii de bază: 1) incident de securitate cibernetică tipic – se referă la un caz de incident de securitate cibernetică înregistrat şi gestionat în cadrul SI RSISC, care, în baza datelor colectate, este

	RSISC, care, în baza datelor colectate, este analizat în scopul oferirii suportului şi remedierii după posibilitate. Cazul poate fi închis de către persoana desemnată responsabilă după ce au fost luate toate măsurile prevăzute în procedurile operaţionale de rigoare; 2) incident de securitate escaladat – se referă la un caz de incident de securitate cibernetică deschis în cadrul SI RSISC, care, în urma datelor colectate, se constată a fi în afara atribuţiilor CERT Gov şi necesită escaladarea către entităţile publice care au atribuţii de asigurare a securităţii statului. În scenariul respectiv, persoana responsabilă de acest caz în cadrul SI RSISC desemnează o altă persoană responsabilă şi consemnează prin comentariu motivul escaladării. Cazul incidentului de securitate poate fi închis de reprezentanţii entităţilor publice desemnate responsabile de gestiunea ulterioară a incidentului de securitate cibernetică sau de către registratorul iniţial al incidentului de securitate cibernetică, în cazul în care s-a depăşit termenul-limită de analiză a incidentului fără prezentarea unui raport.		analizat în scopul oferirii suportului şi remedierii după posibilitate. Cazul poate fi închis de către persoana desemnată responsabilă după ce au fost luate toate măsurile prevăzute în procedurile operaţionale de rigoare; 2) incident de securitate escaladat – se referă la un caz de incident de securitate cibernetică deschis în cadrul SI RSIC, care, în urma datelor colectate, se constată a fi în afara atribuţiilor CERT Gov şi necesită escaladarea către entităţile publice care au atribuţii de asigurare a securităţii statului. În scenariul respectiv, persoana responsabilă de acest caz în cadrul SI RSIC desemnează o altă persoană responsabilă şi consemnează prin comentariu motivul escaladării. Cazul incidentului de securitate poate fi închis de reprezentanţii entităţilor publice desemnate responsabile de gestiunea ulterioară a incidentului de securitate cibernetică sau de către registratorul iniţial al incidentului de securitate cibernetică, în cazul în care s-a depăşit termenul-limită de analiză a incidentului fără prezentarea unui raport.
79.	36. Obiectul informaţional "Alertă de securitate cibernetică" va conţine 3 scenarii de bază:	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	36. Obiectul informaţional "Alertă de securitate cibernetică" va conţine 3 scenarii de bază:

	1) alertă pozitivă – se referă la activităţi anomalice recepţionate sau raportate prin căile de comunicare aprobate, care au potenţial de a degenera în vulnerabilitate cibernetică sau incident de securitate cibernetică. În scenariul respectiv, utilizatorii desemnaţi responsabili de această alertă în cadrul SI RSISC vor emite notificări în cadrul platformei de gestiune a incidentelor cibernetice şi vor analiza activitatea anomalică în scopul identificării potenţialelor riscuri de securitate cibernetică asociate alertei respective; 2) alertă fals-pozitivă – se referă la cazul în care alertele recepţionate prezintă activităţi anomalice, dar care nu reprezintă risc de securitate sau care nu au potenţial de a deveni vulnerabilitate în spaţiul cibernetic sau incident de securitate cibernetică. În acest scenariu, actorii desemnaţi responsabili de alerta respectivă în cadrul SI RSISC vor închide alerta de securitate în cadrul SI RISC, cu menţiunile de rigoare în comentariu; 3) alertă degenerată în incident de securitate cibernetică – se referă la cazul în care activitatea anomalică raportată este rezultatul desfăşurării unui atac cibernetic în timp real, ce devine incident de securitate cibernetică. În acest scenariu, responsabilii de incidentul de securitate cibernetică identificat vor gestiona alertele, asociind, în cadrul SI RSISC, datele		1) alertă pozitivă – se referă la activităţi anomalice recepţionate sau raportate prin căile de comunicare aprobate, care au potenţial de a degenera în vulnerabilitate cibernetică sau incident de securitate cibernetică. În scenariul respectiv, utilizatorii desemnaţi responsabili de această alertă în cadrul SI RSIC vor emite notificări în cadrul platformei de gestiune a incidentelor cibernetice şi vor analiza activitatea anomalică în scopul identificării potenţialelor riscuri de securitate cibernetică asociate alertei respective; 2) alertă fals-pozitivă – se referă la cazul în care alertele recepţionate prezintă activităţi anomalice, dar care nu reprezintă risc de securitate sau care nu au potenţial de a deveni vulnerabilitate în spaţiul cibernetic sau incident de securitate cibernetică. În acest scenariu, actorii desemnaţi responsabili de alerta respectivă în cadrul SI RSIC vor închide alerta de securitate în cadrul SI RSIC, cu menţiunile de rigoare în comentariu; 3) alertă degenerată în incident de securitate cibernetică – se referă la cazul în care activitatea anomalică raportată este rezultatul desfăşurării unui atac cibernetic în timp real, ce devine incident de securitate cibernetică. În acest scenariu, responsabilii de incidentul de securitate cibernetică identificat vor gestiona alertele, asociind, în cadrul SI RSIC, datele stocate despre alertă către cazul incidentului de securitate

	stocate despre alertă către cazul incidentului de securitate cibernetică deschis. Ca urmare, alerta respectivă va obţine statutul de alertă închisă, cu menţionarea în comentarii a identificatorului cazului incidentului de securitate cibernetică asociat.		cibernetică deschis. Ca urmare, alerta respectivă va obţine statutul de alertă închisă, cu menţionarea în comentarii a identificatorului cazului incidentului de securitate cibernetică asociat.
80.	40. Registratorii din cadrul CERT Gov vor opera cu informaţiile colectate în cadrul SI RSISC, în scopul: 1) corelării datelor aferente activităţilor anomale (alertelor) raportate spre identificarea prealabilă a unor potenţiale incidente de securitate cibernetică; 2) diagnosticării specifice problemelor securităţii cibernetice a entităţilor publice şi oferirii serviciilor de consultanţă, precum şi al elaborării recomandărilor de soluţionare şi prevenire a incidentelor de securitate cibernetică; 3) întocmirii datelor statistice şi a rapoartelor privind alertele, riscurile şi incidentele de securitate cibernetică; 4) promovării bunelor practici aferente prevenţiei şi minimizării impactului potenţialelor incidente de securitate cibernetică.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	40. Registratorii din cadrul CERT Gov vor opera cu informaţiile colectate în cadrul SI RSIC, în scopul: 1) corelării datelor aferente activităţilor anomale (alertelor) raportate spre identificarea prealabilă a unor potenţiale incidente cibernetice; 2) diagnosticării specifice problemelor securităţii cibernetice a entităţilor publice şi oferirii serviciilor de consultanţă, precum şi al elaborării recomandărilor de soluţionare şi prevenire a incidentelor cibernetice; 3) întocmirii datelor statistice şi a rapoartelor privind alertele, riscurile şi incidentele cibernetice; 4) promovării bunelor practici aferente prevenţiei şi minimizării impactului potenţialelor incidente cibernetice.

81.	41. După înregistrarea incidentului sau a alertei de securitate cibernetică în cadrul SI RSISC, angajaţii CERT Gov: ... 4) coordonează, la nivel guvernamental, reacţia la incidente de securitate cibernetică, în colaborare cu celelalte entităţi publice, conform domeniului de activitate şi responsabilitate.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	41. După înregistrarea incidentului sau a alertei de securitate cibernetică în cadrul SI RSIC, angajaţii CERT Gov: ... 4) coordonează, la nivel guvernamental, reacţia la incidente cibernetice, în colaborare cu celelalte entităţi publice, conform domeniului de activitate şi responsabilitate.
82.	44. SI RSISC este proiectat ca sistem modular compatibil cu tehnologii de "cloud computing" (nor informaţional), care asigură posibilitatea dezvoltării sale fără perturbarea continuităţii funcţionării.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	44. SI RSIC este proiectat ca sistem modular compatibil cu tehnologii de "cloud computing" (nor informaţional), care asigură posibilitatea dezvoltării sale fără perturbarea continuităţii funcţionării.
83.	45. Arhitectura SI RSISC este concepută după schema-tip a infrastructurii informaţionale a sistemului informaţional şi este găzduit pe platforma tehnologică guvernamentală comună (MCloud).	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	45. Arhitectura SI RSIC este concepută după schema-tip a infrastructurii informaţionale a sistemului informaţional şi este găzduit pe platforma tehnologică guvernamentală comună (MCloud).
84.	46. SI RSISC va conţine şi obiectele informaţionale împrumutate din alte sisteme informaţionale de stat, precum: 1) Registrul de stat al unităţilor de drept – pentru recepţionarea datelor de identificare a persoanelor juridice, utilizatori autorizaţi ai SI RSISC;	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	46. SI RSIC va conţine şi obiectele informaţionale împrumutate din alte sisteme informaţionale de stat, precum: 1) Registrul de stat al unităţilor de drept – pentru recepţionarea datelor de identificare a persoanelor juridice, utilizatori autorizaţi ai SI RSIC;

	2) Registrul de stat al populaţiei – pentru recepţionarea datelor de identificare a persoanelor fizice, utilizatori autorizaţi ai SI RSISC.		2) Registrul de stat al populaţiei – pentru recepţionarea datelor de identificare a persoanelor fizice, utilizatori autorizaţi ai SI RSIC.
85.	47. SI RSISC va fi integrat cu următoarele sisteme informaţionale partajate relevante: ... 7) portalul guvernamental unic de date deschise (PDGD) – pentru publicarea seturilor publice de date produse în cadrul fluxurilor de lucru ale SI RSISC.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	47. SI RSIC va fi integrat cu următoarele sisteme informaţionale partajate relevante: ... 7) portalul guvernamental unic de date deschise (PDGD) – pentru publicarea seturilor publice de date produse în cadrul fluxurilor de lucru ale SI SI RSIC.
86.	8. Pentru asigurarea funcţionalităţii eficiente şi neîntrerupte a SI RSISC, schimbul informaţional de date din cadrul sistemului informaţional este asigurat în regim nonstop.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	8. Pentru asigurarea funcţionalităţii eficiente şi neîntrerupte a SI RSIC, schimbul informaţional de date din cadrul sistemului informaţional este asigurat în regim nonstop.
87.	**III. SPAŢIUL TEHNOLOGIC AL SI RSISC**	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	**III. SPAŢIUL TEHNOLOGIC AL SI RSIC**
88.	49. Spaţiul tehnologic al SI RSISC reprezintă un complex informaţional. Toate datele sistemului se depozitează într-o bază de date centralizată. Prezenţa componentelor software şi a mijloacelor tehnologice în complexul informaţional respectiv este stabilită la etapa elaborării sarcinii tehnice şi a proiectului tehnic al sistemului.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	49. Spaţiul tehnologic al SI RSIC reprezintă un complex informaţional. Toate datele sistemului se depozitează într-o bază de date centralizată. Prezenţa componentelor software şi a mijloacelor tehnologice în complexul informaţional respectiv este stabilită la etapa elaborării sarcinii tehnice şi a proiectului tehnic al sistemului.

89.	50. Arhitectura complexului software-hardware se determină la etapa elaborării caietului de sarcini al SI RSISC. Această soluţie constructivă a sistemului reprezintă viziunea strategică managerială asupra proceselor de activitate în domeniu. Pentru arhitectura SI RSISC se insistă asupra respectării următoarelor principii: ... 6) asigurarea confidenţialităţii şi integrităţii datelor sistemului prin limitarea accesului în 2 etape: asigurarea accesului doar prin autentificare, precum şi stabilirea individuală a drepturilor de acces al utilizatorului la atributele sistemului de către administratorul SI RSISC.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	50. Arhitectura complexului software-hardware se determină la etapa elaborării caietului de sarcini al SI RSIC. Această soluţie constructivă a sistemului reprezintă viziunea strategică managerială asupra proceselor de activitate în domeniu. Pentru arhitectura SI RSIC se insistă asupra respectării următoarelor principii: ... 6) asigurarea confidenţialităţii şi integrităţii datelor sistemului prin limitarea accesului în 2 etape: asigurarea accesului doar prin autentificare, precum şi stabilirea individuală a drepturilor de acces al utilizatorului la atributele sistemului de către administratorul SI RSIC.
90.	53. În scenariul de bază privind gestiunea unui incident de securitate cibernetică în cadrul SI RSISC se vor parcurge câteva etape principale, prezentate în figura 5: 1) identificarea şi raportarea evenimentelor/incidentelor de securitate cibernetică conform modului de interacţiune stabilite în Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020; ...	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	53. În scenariul de bază privind gestiunea unui incident de securitate cibernetică în cadrul SI RSIC se vor parcurge câteva etape principale, prezentate în figura 5: 1) identificarea şi raportarea evenimentelor/ incidentelor cibernetice conform modului de interacţiune stabilite în Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020; ...

	3) investigarea incidentelor de securitate cibernetică şi identificarea cauzei producerii acestora, inclusiv a măsurilor de prevenire care să asigure depistarea la timp a unor incidente similare; ... 5) escaladarea incidentelor de securitate cibernetică ce nu vizează domeniul de competenţă al CERT Gov şi furnizarea de către entităţile publice care au făcut raportarea a informaţiei relevante în ceea ce priveşte acţiunile ulterioare escaladării; 6) tratarea incidentelor de securitate cibernetică şi oferirea recomandărilor de soluţionare a acestora; 7) evidenţa şi stocarea informaţiilor aferente incidentelor de securitate cibernetică; ...		3) investigarea incidentelor cibernetice şi identificarea cauzei producerii acestora, inclusiv a măsurilor de prevenire care să asigure depistarea la timp a unor incidente similare; ... 5) escaladarea incidentelor cibernetice ce nu vizează domeniul de competenţă al CERT Gov şi furnizarea de către entităţile publice care au făcut raportarea a informaţiei relevante în ceea ce priveşte acţiunile ulterioare escaladării; 6) tratarea incidentelor cibernetice şi oferirea recomandărilor de soluţionare a acestora; 7) evidenţa şi stocarea informaţiilor aferente incidentelor cibernetice; ...
91.	54. Fluxurile informaţionale ale SI RSISC sunt redate în figura 6.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	54. Fluxurile informaţionale ale SI RSIC sunt redate în figura 6.
92.	**Figura 6.** Fluxurile informaţionale ale SI RSISC	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	**Figura 6.** Fluxurile informaţionale ale SI RSIC
93.	55. Prin securitatea informaţiei se înţelege protecţia resurselor şi a infrastructurii informaţionale a SI RSISC împotriva acţiunilor premeditate sau accidentale cu	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	55. Prin securitatea informaţiei se înţelege protecţia resurselor şi a infrastructurii informaţionale a SI RSIC împotriva acţiunilor premeditate sau accidentale cu caracter natural

	caracter natural sau artificial, care au ca rezultat cauzarea prejudiciului participanţilor la procesul de schimb informaţional.		sau artificial, care au ca rezultat cauzarea prejudiciului participanţilor la procesul de schimb informaţional.
94.	56. Noţiunea de securitate informaţională a SI RSISC include o serie de termeni, cum ar fi: măsuri de prevenţie, măsuri de reacţie şi măsuri de contracarare, politici, tehnologii, structură organizaţională, atribuţii şi funcţii în sistem. Este necesară identificarea acestor mijloace de control pentru a asigura şi a implementa securitatea informaţională în SI RSISC.	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	56. Noţiunea de securitate informaţională a SI RSIC include o serie de termeni, cum ar fi: măsuri de prevenţie, măsuri de reacţie şi măsuri de contracarare, politici, tehnologii, structură organizaţională, atribuţii şi funcţii în sistem. Este necesară identificarea acestor mijloace de control pentru a asigura şi a implementa securitatea informaţională în SI RSIC.
95.	58. Mecanismele tehnologice de bază pentru asigurarea protecţiei şi securităţii datelor sunt: 1) accesul la date doar prin interfaţa unică de obiect; 2) delimitarea accesului utilizatorilor la date în conformitate cu rolurile acestora în SI RSISC;	în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	58. Mecanismele tehnologice de bază pentru asigurarea protecţiei şi securităţii datelor sunt: 1) accesul la date doar prin interfaţa unică de obiect; 2) delimitarea accesului utilizatorilor la date în conformitate cu rolurile acestora în SI RSIC;
96.	64. Prelucrarea de date în cadrul registrului de stat al incidentelor de securitate cibernetică trebuie să garanteze respectarea următoarelor reguli privind protecţia datelor cu caracter personal: ...	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare.	64. Prelucrarea de date în cadrul registrului de stat al incidentelor cibernetice trebuie să garanteze respectarea următoarelor reguli privind protecţia datelor cu caracter personal: ...
97.	66. Prezentul Concept conţine descrierea principalelor aspecte organizaţionale ce ţin de crearea SI RSISC şi vine să contribuie la	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele	66. Prezentul Concept conţine descrierea principalelor aspecte organizaţionale ce ţin de crearea SI RSIC şi vine să contribuie la

	soluţionarea unei probleme polivalente: pe de o parte, se elaborează mecanismul care asigură automatizarea proceselor de identificare, înregistrare, clasificare şi analiză a incidentelor de securitate cibernetică, monitorizarea şi evidenţa alertelor, vulnerabilităţilor şi incidentelor de securitate cibernetică identificate sau raportate, iar pe de altă parte, se constituie interacţiunea CERT departamentale cu CERT Gov privind incidentele de securitate cibernetică şi alte informaţii aferente.	*„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	soluţionarea unei probleme polivalente: pe de o parte, se elaborează mecanismul care asigură automatizarea proceselor de identificare, înregistrare, clasificare şi analiză a incidentelor cibernetice, monitorizarea şi evidenţa alertelor, vulnerabilităţilor şi incidentelor cibernetice identificate sau raportate, iar pe de altă parte, se constituie interacţiunea CERT departamentale cu CERT Gov privind incidentelor cibernetice şi alte informaţii aferente.
98.	67. Beneficiile statului ca urmare a creării şi implementării SI RSISC sunt următoarele: 1) consolidarea capacităţii de răspuns la incidente de securitate cibernetică; 2) ameliorarea imaginii Republicii Moldova pe plan extern; 3) monitorizarea incidentelor de securitate cibernetică la nivel guvernamental.	în tot textul, cuvintele *„incidentelor de securitate cibernetică”,* la orice formă gramaticală, se substituie cu cuvintele *„incidentelor cibernetice”* la forma gramaticală corespunzătoare. în tot textul, cuvintele „*SI RSISC*” se substituie cu cuvintele „*SI RSIC*”.	67. Beneficiile statului ca urmare a creării şi implementării SI RSIC sunt următoarele: 1) consolidarea capacităţii de răspuns la incidentele cibernetice; 2) ameliorarea imaginii Republicii Moldova pe plan extern; 3) monitorizarea incidentelor cibernetice la nivel guvernamental.
Regulamentul sanitar privind supravegherea și monitorizarea calității apei potabile aprobat prin Hotărârea Guvernului nr. 651/2023			
99.	-	se completează cu punctele *„72[1] și 72[2]”* cu următorul cuprins:	Puncte noi.

		„72[1]. Furnizorii de apă potabilă, trebuie să asigure securitatea rețelelor și sistemelor informatice utilizate la prestarea serviciilor și, dacă sunt incluși în Lista furnizorilor de servicii în sectoarele și subsectoarele critice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, să îndeplinească obligațiile de asigurare a securității cibernetice stabilite de legea respectivă. 72[2]. Agenția pentru Securitate Cibernetică exercită funcția de supraveghere și control de stat al respectării de către furnizorii de apă potabilă, incluși în Lista furnizorilor de servicii, a obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică. Furnizorii de apă potabilă sunt obligați să ofere acces Agenției pentru Securitate Cibernetică la informațiile, bunurile și încăperile deținute de aceștia, care sunt necesare realizării obiectivelor controlului.”.	

SINTEZA

obiecțiilor și propunerilor/recomandărilor la proiectul Guvernului pentru modificarea unor hotărâri ale Guvernului (aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Ministerul Finanțelor** *(07/3-12-100 din 14.05.2024)*	*Referitor la proiectul hotărârii Guvernului*		
		1.	La punctul 1, subpunctul 1), cuvântul *„informatice”* se va substitui cu cuvântul *„informaționale”*, iar după cuvintele „prestarea serviciilor” se va adăuga cuvântul *„poștale”*, în scopul uniformizării terminologiei utilizate în Hotărârea Guvernului nr.1457/2016 pentru aprobarea regulilor privind prestarea serviciilor poștale.	**Se acceptă parțial.** A fost adăugat cuvântul „*poștale*”. În același timp, așa cum este menționat și în nota informativă, obiectivul de bază al prezentei hotărâri de Guvern este aducerea în concordanță a hotărârilor de Guvern cu Legea nr. 48/2023 privind securitatea cibernetică, inclusiv din punct de vedere terminologic. În acest sens, sintagma “*securitatea rețelelor și sistemelor informatice*” este în conformitate cu terminologia cu care operează Legea nr. 48/2023 privind securitatea cibernetică, precum și Directiva NIS 2. Suplimentar, art. 3 din Legea nr. 48/2023 definește noțiunea de “*securitatea rețelelor și sistemelor informatice*”.
		2.	La punctul 2, subpunctul 15) din proiect, în punctul 23 subpunctul 3) lit.b) din textul capitolului VI, cuvintele *„executarea la timp și corectă a legilor și a regulamentelor”* se va substitui cu cuvintele *„executarea la timp și corectă a actelor normative și reglementărilor interne ale instituției în domeniul securității cibernetice”*, întru excluderea	**Se acceptă.** În versiunea actualizată a proiectului este punctul 2, subpunctul 16).

			cuvintelor ce lasă loc de interpretare (nu este clar ce „legi și regulamente” se are în vedere în această normă) în conformitate cu prevederile art. 54 din Legea nr.100/2017 cu privire la actele normative.	
		3.	La punctul 3, subpunctul 2) și subpunctul 4) urmează a fi reamplasate, ținând cont că conținutul normei propuse la pct.31[1] din statutul IP STISC nu se încadrează în capitolul ”Finanțarea și Patrimoniul Serviciului”, nici la pct.34[1] – în capitolul ”Evidența și dările de seamă.”	**Precizare.** Modificările propuse în proiectul de hotărâre de Guvern se referă la punctul 8 din Statutul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică”, aprobat prin Hotărârea Guvernului nr. 414/2018, cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat. Aceste modificări completează funcțiile Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică” stabilite la pct. 8 din Statut, și nu se referă la capitolul „Finanțarea și Patrimoniul Serviciului” sau capitolul „Evidența și dările de seamă”.
		4.	La punctul 8, subpunctul 1) lit. b) se propune de exclus, deoarece Legea nr.48/2023 a fost aprobată și a intrat în vigoare mai târziu decât Hotărârea Guvernului nr.388/2022 cu privire la aprobarea Conceptului Sistemului informaţional „Registrul de stat al incidentelor de securitate cibernetică” și nu poate servi drept temei de adoptare a unui act aprobat anterior.	**Nu se acceptă.** Potrivit indicațiilor metodologice privind regulile de tehnică legislativă la indicarea temeiului juridic se face referință la norma juridică concretă care stabilește competența autorității emitente să adopte/aprobe actul normativ respectiv. Aceasta nu stabilește restricții cu privire la momentul adoptării actului normativ ierarhic superior.

		Referitor la nota informativă		
		5.	Capitolul 5 „Fundamentarea economico-financiară” urmează a fi completat cu estimarea eventualelor cheltuieli care pot surveni în rezultatul adoptării proiectului, inclusiv implementarea prevederilor punctului 4 al proiectului privind acordarea sporului specific personalului Agenției pentru Securiatete Cibernetică. Totodată, autorul proiectului urmează să aducă claritate dacă pentru acoperirea costurilor sunt prevăzute resurse financiare suficiente în Legea bugetului de stat pentru anul 2024 nr.418/2023, luînd în considerație data intrării în vigoare a prevederilor punctului 4 din proiect. În context, informăm că în bugetul de stat pentru anul curent, la subprogramul 1504 „Tehnologii informaționale” au fost aprobate cheltuieli în sumă de 15 000,0 mii lei dintre care cheltuieli de personal 12 449,2 mii lei.	**Se acceptă.**
		6.	De asemenea, atenționăm că potrivit modificărilor propuse la Statului IP Serviciul Tehnologia Informației și Securitate Cibernetică (STISC), aprobat prin Hotărârea Guvernului nr.414/2018, STISC va menține funcția de exercitare a rolului Centrului guvernamental de răspuns la incidentele cibernetice, precum și va exercita o funcție nouă privind asigurarea securității rețelelor și sistemelor informatice proprietate a statului. Respectiv, urmează a fi indicate costurile și subprogramul bugetar pentru acoperirea cheltuielilor în acest sens.	**Nu se acceptă.** Asigurarea securității rețelelor și sistemelor informatice proprietate a statului nu este o funcție nouă, este o funcție pe care Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” o realizează la momentul actual. Modificările propuse vin să ofere un spor de precizie juridică și să alinieze prevederile Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat la prevederile art. 8 din Legea nr. 48/2023 privind securitatea cibernetică.

				Adițional, urmează a fi remarcat că în procesul de promovare a proiectului de Lege nr. 48/2023 privind securitatea cibernetică acesta a fost însoțit de analiză de impact.
		7.	Suplimentar, din dosarul de însoțire a actului normativ remis spre consultare prealabilă lipsește tabelul comparativ în care trebuie să fie reflectate reglementările în vigoare și modificările propuse, avînd în vedere că în conformitate cu art. 40 lit. g) din Legea nr. 100/2017 cu privire la actele normative, reiese că un asemenea act este necesar a fi întocmit pentru proiectele care conțin modificări la actele normative în vigoare. Urmare a analizei înfăptuite pe marginea proiectului, Ministerul Finanțelor este dispus să examineze repetat proiectul de hotărîre în cauză, conținutul acestuia urmând a fi ajustat în conformitate cu obiecțiile și propunerile sus-menționate.	**Se acceptă.**
2.	**IP „Agenția de Guvernare Electronică”** *(Nr. 24/3007 – 80 din 15.05.2024)*	8.	În **pct.2 (modificări la Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr.201/2017)**, la **sbp.5)**, textul *„și Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică”* propunem de exclus pornind de la faptul că ar dubla prevederile pct.7 sbp.2) din Măsurile necesare pentru asigurarea securității cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr.482/2020, conform cărora este stabilită deja atribuția entităților publice, în calitatea lor CERT departamentale, de a interacționa privind modalitatea de raportare, stocare și prelucrare a informațiilor aferente incidentelor și amenințărilor securității cibernetice cu Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, în calitatea acesteia de CERT Gov.	**Nu se acceptă.** Punctul 7 alin. (2) se limitează la raportarea, stocarea și prelucrarea informațiilor aferente incidentelor și amenințărilor de securitate cibernetică, fără a include obligația de a informa cu privire la persoana (sau subdiviziunea) responsabilă de implementarea sistemului de management al securității informației.

		9.	În **pct.4 (modificări la Regulamentul cu privire la tipurile și modul de stabilire a sporurilor cu caracter specific, aprobat prin Hotărârea Guvernului nr. 1231/2018 pentru punerea în aplicare a prevederilor Legii nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar),** considerăm oportun să fie examinată suplimentar ***redacția noului pct.51 sbp.4)****, în special în partea ce ține de funcția personalului Agenției pentru Securitate Cibernetică (ASC) de schimb de informații în materie de securitate cibernetică*. Astfel, considerăm că după aprobarea, prin Hotărârea Guvernului nr.1028/2023, a Regulamentului cu privire la organizarea și funcționarea ASC, deocamdată, nu există o claritate în ceea ce privește realizarea de către Agenție a atribuției respective. În context, facem trimitere la art.16 din Legea nr.48/2023, care conține o normă primară referitor la schimbul transfrontalier de informații privind prevenirea și soluționarea incidentelor cibernetică, iar la art.17 alin.(2) prevede că ASC, în calitate de autoritate competentă în domeniul securității cibernetice, intermediază schimbul de informații între furnizorii de servicii și, după caz, alte persoane juridice care intră în domeniul de aplicare a legii în cauză *„prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și a comunităților de încredere”*, ceia ce ar putea presupune necesitatea dezvoltării unui instrument tehnic pentru realizarea acestei atribuții care, din câte cunoaștem, la moment, nu există. Pe de altă parte, nu există o certitudine cum aceste atribuții de schimb transfrontalier de informații și, respectiv, de schimb voluntar de informații relevate în materie de schimb de date vor corela cu obligațiile ASC și a furnizorilor de servicii ce le revin conform Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate, și anume de a efectua schimbul de date, inclusiv cel transfrontalier, prin intermediul platformei de	**Nu se acceptă.** Aspectele invocate de autorul obiecției nu intră în obiectul de reglementare al acestui proiect de act normativ. Modalitatea de exercitare de către personalul Agenției pentru Securitate Cibernetică a atribuției de schimb de informații în materie de securitate cibernetică la nivel național și internațional (transfrontalier) urmează a fi reglementată în contextul executării prevederilor art. 23 alin. (2) și (3) din Legea nr. 48/2023 privind securitatea cibernetică.

			interoperabilitate (MConnect) și de a asigura condițiile tehnice necesare realizării schimbului de date. În această ordine de idei, recomandăm autorului să completeze nota informativă la proiect cu explicațiile de rigoare în privința modalității de exercitare de către personalul ASC a atribuției de schimb de informații în materie de securitate cibernetică la nivel național și internațional (transfrontalier).	
		10.	În **pct.5 (modificări la Regulamentul privind modul de utilizare a platformei de interoperabilitate (MConnect), aprobat prin Hotărârea Guvernului nr. 211/2019)**, la **sbp.3)** considerăm că noile pct.10^1 și 10^2 necesită a fi excluse, deoarece nu se integrează armonios în Secțiunea a 2-a din Regulamentul în speță, care reglementează responsabilitățile participanților la schimbul de date prin intermediul platformei MConnect (furnizori de date și consumatori de date) la pct.6 și, respectiv, pct.8 din Regulament. Dar și mai important, considerăm că, soluțiile juridice produse de autor excedează prevederile Regulamentului privind modul de utilizare a platformei de interoperabilitate (MConnect) și, în principiu, se regăsesc deja în art.8 din Legea nr.142/2018 cu privire la schimbul de date și interoperabilitate, care reglementează, la nivel normelor primare, securitatea și confidențialitatea schimbului de date, dar și în Secțiunea a 12-a din același Regulament, care este dedicată integral reglementării aspectelor privind securitatea informației și protecția datelor cu caracter personal în contextul schimbului de date prin platforma MConnect.	**Se acceptă.**
		11.	Totodată, referindu-ne în special la formularea propusă de autor la pct.10^2 , considerăm că aceasta nu aduce valoare normativă suplimentară dispozițiilor Capitolului IV din Legea nr.48/2023 privind securitatea cibernetică și Legii nr.131/2012 privind controlul de stat asupra activității de	**Se acceptă.**

			întreprinzător, care, în opinia AGE, reglementează exhaustiv competențele ASC în domeniul supravegherii și controlului de stat.	
3.	**IP „Serviciul Tehnologia Informației și Securitate Cibernetică”** *(Nr. 1.4/819/24 din 15.05.2024)*	Comunică susținerea de principiu a acestuia, intervenind cu următoarele propuneri.		
		12.	Considerăm necesară revizuirea temeiului de aprobare, întrucât potrivit regulilor de tehnică legislativă referințele la dispozițiile finale ale unui act normativ, prin care o autoritate publică se obligă să amendeze actele sale în conformitate cu noile reglementări, nu constituie temei juridic.	**Se acceptă.**
		13.	La pct. 2 sbp. 2), substituirea textului *„sistemul de management al securității cibernetice”* cu textul *„sistemul de management al securității informației”*, creează interpretări din punct de vedere al percepției și atribuțiilor diverselor instituții ce au tangență la proces. Noțiunea de *securitate informațională* are un sens mult mai larg decât cea de *securitate cibernetică*, iar accentul trebuie pus anume pe *securitate cibernetică*, conform noțiunilor cu care operează Legea nr. 48/2023 privind securitatea cibernetică precum și prezentul proiect.	**Nu se acceptă.** Așa cum este menționat și în nota informativă, unul din obiectivele de bază al prezentei hotărâri de Guvern este alinierea cadrului normativ secundar la Legea nr. 48/2023 privind securitatea cibernetică, inclusiv aspectele care vizează standardele în domeniul securității informației și al securității cibernetice. În acest sens, terminologia cu care se propune a opera în cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr. 201/2017 este aliniată la Standardul ISO 27001.
		14.	La pct. 2 sbp. 3), textul *„la pct. 1, textul: „1) echipamentele (hardware) și produsele de program (software) existente în cadrul fiecărei instituţii; 2) sistemele informatice, resursele și sistemele informaționale existente în instituție (în continuare – sisteme), precum și cele aflate la etapa de elaborare, testare și implementare.” se substituie cu sintagma „rețele și sisteme informatice (în continuare – sisteme).”,* se va indica într-un subpunct distinct.	**Se acceptă.**

		15.	Cu referire la pct. 3 sbp. 1), respectiv la pct. 6 sbp. 3) lit. c), atragem atenția că acestea se contrazic cu prevederile pct. 3 din Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat. Or, potrivit Măsurilor necesare pentru asigurarea securităţii cibernetice la nivel guvernamental aprobate prin aceeași hotărâre, CERT-urile departamentale sunt create în cadrul **ministerelor, altor autorităţi administrative centrale subordonate Guvernului, Cancelariei de Stat şi structurilor organizaţionale din sfera lor de competenţă (autorităţilor administrative din subordine, serviciilor publice desconcentrate şi celor aflate în subordine, precum şi instituţiilor publice şi întreprinderilor de stat în care ministerul, Cancelaria de Stat sau altă autoritate administrativă centrală are calitatea de fondator) şi organizaţiilor de stat autonome înfiinţate de Guvern.**	**Nu se acceptă.** Competența privind asigurarea securității rețelelor și sistemelor informatice proprietate a statului de către Centrul guvernamental de răspuns la incidentele cibernetice este stabilită la nivel de normă primară în art. 8 alin. (3) din Legea nr. 48/2023 privind securitatea cibernetică.
		16.	În ceea ce privește sbp. 3) lit. d) de la pct. 6, considerăm că notificarea directă a CSIRT-ului național de către entitățile publice, fără a notifica CERT Gov, ar cauza pierderea informațiilor de către ultima, ținerea evidenței inexacte și prezentarea unor date eronate în raportul trimestrial prezentat către CSIRT național.	**Se acceptă.** Textul normei a fost modificat pentru a evita interpretările ambigue privind posibilitatea excluderii notificării către CERT Gov. Astfel, notificarea obligatorie a incidentelor cibernetice de către entitățile publice către CERT Gov nu exclude dreptul acestora de a notifica și CSIRT național cu privire la același incident cibernetic.
		17.	La pct. 7 sbp. 2), sintagma *„prevăzute de prezenta lege”* creează confuzii și din acest considerent considerăm că trebuie substituită cu *„prevăzute de prezentul Program”*.	**Se acceptă.**

		18.	Pe această cale, în vederea clarificării aspectelor contradictorii, solicităm respectuos organizarea unei ședințe cu participarea reprezentanților Ministerului Dezvoltării Economice și Digitalizării și a Agenției de Securitate Cibernetică. Totodată trebuie puse în discuție și anumite aspecte privind Registrul de stat al incidentelor de securitate cibernetică. Or, considerăm oportună modificarea Hotărârii Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” inclusiv în partea de substituire a IP STISC, din calitatea de responsabil de crearea, implementarea, funcționarea și dezvoltarea Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”, precum și posesor și deținător al acestuia, cu Agenția de Securitate Cibernetică.	

Secretar de stat **Cătălina PLINSCHI**

Ministerul Dezvoltării
Economice și Digitalizării
al Republicii Moldova

Nr. 13/2-2099 din 05.07.2024

Cancelaria de Stat

În temeiul prevederilor pct.179 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr.610/2018, se transmite cererea privind înregistrarea în lista proiectelor care urmează a fi examinate în cadrul ședinței secretarilor generali, a proiectului hotărârii Guvernului pentru modificarea unor hotărâri ale Guvernului (aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe).

CERERE

privind înregistrarea de către Cancelaria de Stat a proiectului hotărârii Guvernului pentru modificarea unor hotărâri ale Guvernului (aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)

Nr. crt.	**Criterii de înregistrare**	**Nota autorului**
1.	Categoria şi denumirea proiectului	Proiectul hotărârii Guvernului pentru modificarea unor hotărâri ale Guvernului (aducerea actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe)
2.	Autoritatea care a elaborat proiectul	Ministerul Dezvoltării Economice și Digitalizării
3.	Justificarea depunerii cererii	Proiectul hotărârii Guvernului a fost elaborat în scopul aducerii actelor normative subsidiare în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și legile conexe.
4.	Lista autorităţilor şi instituţiilor a căror avizare este necesară	1. Cancelaria de Stat 2. Aparatul Președintelui Republicii Moldova 3. Ministerul Infrastructurii și Dezvoltării Regionale 4. Ministerul Energiei 5. Ministerul Finanțelor 6. Ministerul Mediului 7. Ministerul Sănătății 8. Ministerul Agriculturii și Industriei Alimentare 9. Ministerul Apărării 10. Ministerul Afacerilor Interne

		11. Ministerul Afacerilor Externe și Integrării Europene 12. Ministerul Educației și Cercetării 13. Ministerul Muncii și Protecției Sociale 14. Serviciul de Informații și Securitate 15. IP Agenția de Guvernare Electronică 16. IP Serviciul Tehnologia Informației și Securitate Cibernetică 17. Agenția pentru Securitate Cibernetică 18. Agenția Națională pentru Reglementare în Energetică a Republicii Moldova 19. Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei 20. Banca Națională a Moldovei 21. Ministerul Justiției – *expertiza juridică* 22. Centrul Național Anticorupție - *expertiza anticorupție*
5.	Termenul-limită pentru depunerea avizelor/expertizelor	10 zile
6.	Persoana responsabilă de promovarea proiectului	Melnic Mihaela, consultant principal, Secția politici în domeniul securității cibernetice, tel.: 022 232 327, e-mail: mihaela.melnic@mded.gov.md
7.	Anexe	1. Proiectul hotărârii Guvernului – *11 file;* 2. Nota informativă – *6 file;* 3. Tabelul comparativ – *64 file*; 4. Sinteza obiecțiilor și propunerilor – *9 file.*
8.	Data şi ora depunerii cererii	
9.	Semnătura	

Secretar de stat **Cătălina PLINSCHI**

Ex. Mihaela Melnic,
022-232-327