Ministerul Economiei
și Infrastructurii
al Republicii Moldova

nr. 08/1-7748
23.07 2018

La nr. 18/701 din 10.07.2018

Serviciul de Informații și Securitate

Ministerul Economiei și Infrastructurii a examinat *proiectul Hotărârii de Guvern privind aprobarea proiectului de lege pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și a Planului de acțiuni pentru implementarea acesteia* și ținând cont de prevederile Legii nr.100 din 22.12.2017 cu privire la actele normative, precum și în corespundere cu competențele funcționale, comunică următoarele.

Cu referință la proiectul Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023:

1. La pct. 4, sintagma „Uniunea Informațională a Telecomunicațiilor" de modificat cu sintagma „Uniunea Internațională a Telecomunicațiilor", iar sintagma „industriale în domeniul electronic" - cu sintagma „sectoriale în domeniul Tehnologiei Informației";

2. La pct. 7, de modificat cuvântul „interferenței" cu cuvântul „interacțiunii";

3. La pct. 10, de modificat cuvântul „remediere" cu cuvântul „implementare";

4. La pct. 15, sintagma „spațiului informațional-cibernetic" se propune a fi modificată cu sintagma „spațiului cibernetic", iar sintagma „spațiului informațional-mediatic" – cu cuvântul „informaționale". Denumirea pilonului III se recomandă a fi completată la sfârșit cu cuvintele „în domeniul securității informaționale".

5. La pct. 17, cuvântul „pertinente" se recomandă a fi exclus.

6. În pct. 19 este oportun de utilizat cuvântul „îngrădirea" în locul cuvântului „împiedicarea";

7. În pct. 21, sintagmele „organizarea protecției" și „protecția" nu reflectă scopul punctului de asigurare a securități informaționale. Astfel, se recomandă revenirea la textul agreat în ultima ședință a grupului de lucru: „asigurarea securității" și „asigurarea securității informaționale";

8. Punctul 29 considerăm necesar a fi reformulat sau exclus, întrucât nu Legea 299/2017 constituie punctul de pornire în domeniul menționat în acest punct. Anterior acestei legi au mai fost aprobate o serie de acte normative ce reglementează acest domeniu (Legea 20/2009, HG 857/2013, HG 811/2015, etc.).

9. În pct. 35 din textul Strategiei după sintagma „atacurile informatice" de inclus sintagma „acțiunile hibride de destabilizare a ordinii publice a statului";

10. Totodată, luând în considerație că tema amenințărilor hibride a fost mai puțin abordată în documentele de politici, Capitolul II al Strategiei propunem a fi

Piața Marii Adunări Naționale nr. 1, Chișinău, MD-2012, tel. 022 250107, fax 022 234064
E-mail: mineconcom@mei.gov.md Pagina web: www.mei.gov.md

completat cu mai multe informații ce descriu situația din domeniul amenințărilor hibride de destabilizare a ordinii publice și a statului.

11. În pct. 36, sintagma „sutelor de miliarde" de expus în redacția „miliardelor", și dacă e posibil de indicat sursa acestei informații;

12. În pct. 40, sintagma „unei entități" de expus în următoarea redacție „unei viziuni privind crearea unei entități";

13. În pct. 43 subpunctul 7), sintagma „teritoriul necontrolat efectiv de autoritățile Republicii Moldova" de expus în următoarea redacție „teritoriul Republicii Moldova necontrolat efectiv de autoritățile constituționale";

14. Punctul 45 poate fi exclus, întrucât problematica dată este expusă deja în pct. 42 subpct. 1).

15. Punctul 48 din textul Strategiei este necesar de reformulat astfel încât să se identifice problematica situației existente. Însăși aprobarea Directivei UE nu constituie o problemă;

16. În pct. 51 sintagma „dezvoltării sale" de expus în redacția „dezvoltării sale statale";

17. În pct. 52 sintagma „crearea unei stări de revoltă socială" de expus în redacția „crearea și exploatarea unei stări de nemulțumire socială";

18. Punctele 66 și 67 din textul Strategiei se recomandă a fi unificate într-un singur punct și expuse într-o formă depersonalizată, precum este prezentată situația din pct. 63. Totodată, Republica Moldova își are propriile pericole, precum acapararea de teritorii, separatism, subminarea statalității, ș.a., care considerăm că, la moment, încă nu sunt suficient reflectate în documentele de politici, și totuși, acestea vizează tangențial și spațiul informațional;

19. Considerăm oportun completarea Capitolului III cu un punct nou cu referire la protecția datelor cu caracter personal: descrierea problemelor, lipsurilor/deficiențelor, necesitatea cadrului normativ aprobat sau a convenției ratificate.

20. La Cap. IV, denumirile pilonilor este necesar a fi reformulate conform propunerilor expuse în punctul 4 al prezentului aviz.

21. Considerăm că, actuala redacție a pct. 81 alin. 4) și, respectiv, a pct. 2 acțiunea 4) din Planul de acțiuni contravine practicii internaționale. Aducem la cunoștință că, în astfel de țări precum Statele Unite ale Americii, Uniunea Europeană, Republica Populară Chineză, Federația Rusă accesul la codul sursă este solicitat pentru astfel de aplicații, precum antivirus și software care conțin elemente de criptare înaltă. În Statele Unite, companiile tehnologice le permit Guvernului să verifice codul sursă în situații limită ca parte a unor contracte din domeniul apărării sau altor activități foarte importante ale Guvernului. Astfel, în pct. 81 alin. 4) din Strategie și, respectiv, a pct. 2 acțiunea 4) din Planul de acțiuni se recomandă de a include în finalul propoziției următoarea sintagmă: „pentru autoritățile publice".

22. În pct. 85, alin. 3), în finalul acțiunii de adăugat următoarea paranteză: „(atragerea companiilor private și experților independenți, a hackerilor albi, dezvoltarea laboratoarelor, etc.)";

23. Acțiunile din pct. 86 de expus în următoarea redacție:

„1) promovarea unui Internet mai sigur pentru copii prin intermediul consilierii on-line și încurajarea raportării prin proiecte informaționale specializate;

2) organizarea campaniilor de informare și instruire a părinților în scopul responsabilizării și creșterii gradului de conștientizare a riscurilor la care se expun copiii pe Internet;

3) combaterea fenomenului de pornografie infantilă în Internet;

4) combaterea fenomenelor de grooming și hărțuire sexuală a copiilor în Internet.";

24. Se recomandă pe tot parcursul textului Strategiei și a Planului de acțiuni, după caz, de substituit abrevierea „CERT" cu „CSIRT", deoarece CERT (Computer Emergency Response Team) este o marcă comercială înregistrată și pentru utilizarea acesteia va fi nevoie de o autorizare oficială, iar pentru utilizarea CSIRT (Computer Security Incident Response Team) nu sunt necesare autorizări;

25. Pct. 93 subpunctul 2) în finalul acțiunii de suplinit cu sintagma „în conformitate cu recomandările Comisiei Europene și bunele practici europene";

26. În pct. 107 alin 4), sintagma „asigurarea investigării" de expus în următoarea redacție: „asigurarea prevenirii și investigării", iar după alin. 16) de inclus un aliniat cu următorul conținut: „17) protecția datelor cu caracter personal precum și a persoanelor, în special a copiilor, în mediul online";

27. Pct. 112 în final de suplinit cu un aliniat cu următorul cuprins: „7) vor fi asigurate măsuri de prevenire și combatere a criminalității informatice";

28. Punctele 115 și 116 propunem a fi expuse în următoarea redacție:

„115. Monitorizarea și coordonarea procesului de realizare a Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și Planului de acțiuni privind implementarea Strategiei se pune în sarcina Cancelariei de Stat.

116. Ministerele, instituțiile și alte autorități administrative centrale, conform competențelor atribuite:

1) vor asigura întreprinderea măsurilor necesare în vederea realizării integrale și în termenele stabilite a acțiunilor incluse în Planul menționat;

2) vor prezenta anual, până la data de 1 martie, Cancelariei de Stat, rezultatele acțiunilor prevăzute în Plan.

117. Cancelaria de Stat va generaliza informația recepționată și, până la data de 1 aprilie, va plasa pe pagina-web oficială proprie raportul privind rezultatele implementării Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023.";

Cu referință la proiectul Planului de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023, se recomandă următoarele:

29. La obiectivul 1 acțiunile 1) și 2), în rubrica „Instituțiile responsabile" de inclus Cancelaria de Stat – ca fiind prima instituție responsabilă, întrucât este fondatorul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică";

30. La obiectivul 2 acțiunea 1), la instituțiile responsabile de inclus CSIRT-N, deoarece executarea acțiunii poate fi efectuată doar de CSIRT național;

31. La obiectivul 2 acțiunea 2), la instituțiile responsabile de substituit „MEI" cu „AGE", deoarece, în conformitate cu HG 760/2010, Agenția de Guvernare Electronică este responsabilă pentru efectuarea auditului de securitate cibernetică în autoritățile publice și monitorizarea implementării rezultatelor auditului. La acțiunea 4) din instituțiile partenere de exclus „MEI";

32. La obiectivul 11 acțiunea 5), din instituțiile responsabile de exclus „MEI" și de transferat la instituțiile partenere, iar la acțiunea 7) de exclus „MEI" din instituțiile partenere, deoarece Ministerul nu are astfel de atribuții funcționale;

33. La obiectivul 12 acțiunea 3), trebuie specificat care resursă informațională este necesar a fi creată.

34. La obiectivul 18 acțiunea 2), din instituțiile partenere de exclus „MEI", deoarece Ministerul nu are astfel de atribuții funcționale;

35. La obiectivul 19 acțiunea 3), instituțiile partenere de completat cu: „SIS, MAI, PG", deoarece considerăm că doar aceste instituții pot contribui la astfel de acțiuni;

36. La obiectivul 22 acțiunea 1), în calitate de instituție responsabilă urmează a fi inclus SIS, iar instituții partenere – AAP, MECC, CCA, MEI, MA, MAI, PG, SIS, ONG. La acțiunea 4), instituții responsabile – INJ, MAI (Academia Ștefan cel Mare), PG, MA, iar instituții partenere – MECC, CCA, SIS, AȘM, ONG din domeniul media.

37. Totodată, considerăm oportun a completa Planul de acțiuni cu costurile estimative pe fiecare acțiune.

Ministru **Chiril GABURICI**

Iurie Ursu, 022 250630

Ministerul Afacerilor Interne al Republicii Moldova
Ministry of Internal Affairs of the Republic of Moldova

MD 2012, mun. Chişinău, bd. Ştefan cel Mare, 75, tel. (373-22) 255-324, fax: 25-53-24

nr. 38/165 din „18" iulie 2018

Domnului Vasile BOTNARI
Director al Serviciului de
Informații și Securitate

Stimate Domnule Director,

Am onoarea să vă informez în legătură cu solicitarea dumneavoastră nr. 18/701 din 10.07.2018, referitoare la avizarea proiectului Strategiei securității informaționale pentru anii 2018 – 2023 și a Planului de acțiuni pentru implementarea acesteia, că Ministerul Afacerilor Interne nu are observații și propuneri cu privire la documentele menționate.

Folosesc acest prilej, pentru a reitera satisfacția privind cooperarea și dialogul din cadrul grupului de lucru interinstituțional în contextul elaborării proiectului Strategiei.

Cu respect,

Secretar de stat **Dorin PURICE**

SIS al RM
nr. 18/701
20 07 2018

MINISTERUL AFACERILOR EXTERNE ŞI INTEGRĂRII EUROPENE
AL REPUBLICII MOLDOVA
MINISTRY OF FOREIGN AFFAIRS AND EUROPEAN INTEGRATION
OF THE REPUBLIC OF MOLDOVA

Str. 31 August 1989 80, MD-2012 Chişinău • Tel: (373 22) 233940 • Fax: (373 22) 232302 • http://www.mfa.gov.md

Nr. DM/4/363.2/ 8218 din 19 iulie 2018

La nr. 18/701 din 10 iulie 2018

Serviciul de Informaţii şi Securitate

Cu referire la solicitarea SIS privind avizarea proiectului Strategiei securităţii informaţionale a RM (2018-2023) şi a Planului de acţiuni pentru implementarea acesteia, MAEIE, urmare a examinării, remite anexat propunerile/obiecţiile la proiectele în speţă.

Varianta electronică a anexei a fost remisă la adresa jurist@sis.md

Tatiana Molcean
Secretar de stat

Anexă: 25 file

Red.: Victor Verejan
victor.verejan@mfa.md
022 578 268

SIS al RM
La nr. 18/701
20 07 20 18

MINISTERUL APĂRĂRII
AL REPUBLICII MOLDOVA
MD-2021, mun. Chişinău, şoseaua Hînceşti, 84

MINISTRY OF DEFENCE
OF REPUBLIC OF MOLDOVA
84, Hincesti Highway, Chisinau, MD 2021

Serviciul de Informaţii şi Securitate

11/950
14.04.2018

La nr. 18/701
din 10.07.2018

Ministerul Apărării a examinat proiectele Strategiei securităţii informaţionale al Republicii Moldova pentru anii 2018-2023 şi a Planului de acţiuni pentru implementarea Strategiei şi comunică, în limita competenţelor funcţionale, lipsa propunerilor şi obiecţiilor pe marginea proiectelor nominalizate.

Ministru Eugeniu STURZA

SIS al RM
Nr. 18/701
20 04 2018

Ministerul Educaţiei, Culturii şi Cercetării al Republicii Moldova

2033-MD, or. Chişinău, Piaţa Marii Adunări Naţionale, tel. (37322) 227620, fax (3722) 232388

Ministry of Education, Culture and Research of the Republic of Moldova

2033-MD, Chişinău, 1, Piaţa Marii Adunări Naţionale tel. (37322) 227620, fax (3722) 232388

Nr. 07-09/9389 din 27.07.18
La 18/701 din 10.07.2018

Serviciul de Informaţii şi Securitate

Ministerul Educaţiei, Culturii şi Cercetării a examinat proiectul de lege pentru aprobarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 şi a Planului de acţiuni pentru implementarea acesteia şi-l susţine cu următoarele obiecţii şi propuneri:

1) pilonul I, obiectivul 10, acţiunea 1, coloana *Instituţii responsabile* după sintagma "AŞM" se va suplimenta cu sintagmele "Agenţia Naţională de Dezvoltare şi Cercetare" şi "Serviciul de Informare şi Securitate", iar în coloana *Termen de realizare* sintagma *"2019-2022"* se va substitui cu sintagma *"2020-2023";*
2) pilonul I, obiectivul 10, acţiunea 2 se va expune în următoarea redacţie: "Crearea/consolidarea laboratoarelor de securitate cibernetică";
3) pilonul I, obiectivul 11, acţiunea 5 este improprie Ministerului Educaţiei, Culturii şi Cercetării;
4) pilonul IV, obiectivul 22, acţiunea 1, coloana "*Parteneri"* se va completa cu sintagma "MECC" şi, respectiv, din coloana "*Instituţii responsabile"* se va exclude sintagma "MECC" atât la acţiunea 1, cât şi la acţiunile 3 şi 4, ca fiind improprii.

Igor ŞAROV,
Secretar general de stat

G. Gavriliţă, 022 23 34 02
galina.gavrilita@mecc.gov.md

SIS al RM
Nr. 18/701
01 08 2018

MINISTERUL SĂNĂTĂȚII, MUNCII ȘI PROTECȚIEI SOCIALE AL REPUBLICII MOLDOVA

MD-2009, Chișinău, str. Vasile Alecsandri, 2
Tel./Fax. + 373 22268818
e-mail: office@msmps.gov.md
www.msmps.gov.md

MINISTRY OF HEALTH, LABOUR AND SOCIAL PROTECTION OF THE REPUBLIC OF MOLDOVA

2, Vasile Alecsandri Street, Chișinău, MD-2009
Tel./Fax. + 373 22268818
e-mail: office@msmps.gov.md
www.msmps.gov.md

01-5168 din 18.07.2018
La nr. 18/701 din 10.07.2018

Serviciul de Informații și Securitate

Ministerul Sănătății, Muncii și Protecției Sociale a examinat setul proiectului de lege "pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și a Planului de acțiuni pentru implementarea acesteia" și propune următoarele:

La capitolul *VII. Proceduri de Monitorizare și Evaluare* al Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023, deși în titlul capitolului este menționat cuvîntul "evaluare", în text nu este specificat ce presupune și cum va avea loc acest proces. Prin urmare, se propune completarea acestui capitol în ceea ce privește procesul de evaluare a Strategiei.

Cu privire la Planul de acțiuni, unde este specificat ca partener Ministerul Sănătății, Muncii și Protecției Sociale, la abrevierea autorității a fost omisă ultima literă "S", respectiv se solicită completarea, conform Listei de abrevieri expuse la proiectul Strategiei.

Totodată la Pilonul I, punctul 6, subpunct 4) *perfecționarea cadrului legal ce reglementează salarizarea efectivului specializat în combaterea criminalității informatice și investigarea infracțiunilor informatice*, ca responsabili sunt menționați Ministerul Finanțelor și Ministerul Afacerilor Interne, iar ca parteneri, la fel este menționat MF și MSMPS. Luînd în considerație că, după reforma administrației publice centrale, politica salarială în sectorul bugetar a fost preluată de Ministerul Finanțelor (HG nr. 696 din 30.08.2017), această autoritatea trebuie să fie responsabilă de acțiunea respectivă, iar la parteneri trebuie exclus MSMPS și de inclus MAI.

Boris GÎLCA
Secretar general de stat

Ex. Iulia Mihalachi
tel. 022-268-868
e-mail: iulia.mihalachi@msmps.gov.md

SIS al RM
la nr. 18/701
20 07 2018

MINISTERUL FINANȚELOR
AL REPUBLICII MOLDOVA

МИНИСТЕРСТВО ФИНАНСОВ
РЕСПУБЛИКИ МОЛДОВА

MD-2005, mun.Chișinău, str.Constantin Tănase, 7
www.mf.gov.md, tel. (373 22) 26 26 00, fax: (373 22) 26 25 17

06.08.2018 nr. 32/1416

La nr. *18/701 din 10 iulie 2018*

Serviciul de Informații și Securitate
MD-2004 Chișinău, bd. Ștefan cel Mare și Sfînt 166

Ministerul Finanțelor a examinat proiectul de hotărâre de Guvern pentru aprobarea proiectului de lege pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018 – 2023 și a Planului de acțiuni pentru implementarea acesteia și, în limitele competențelor funcționale, Vă comunică următoarele.

Nerespectarea prevederilor art. 30 din Legea nr.100 din 22 decembrie 2017 privind actele normative, conform cărora la proiectul de act prezentat spre examinare și avizare, se întocmește o notă informativă care urmează să includă *fundamentarea economico-financiară*, face dificilă expunerea privind impactul financiar asupra bugetului de stat. Prin urmare considerăm necesar, completarea notei informative.

Totodată, proiectul Hotărârii Guvernului se propune de completat cu un punct nou în redacția următoare:

"Finanțarea acțiunilor prevăzute în Planul de acțiuni privind implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 se va efectua din contul și în limita mijloacelor aprobate în bugetele instituțiilor responsabile de implementare.".

La *proiectul Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023* menționăm că, obiectivele Strategiei trebuie astfel formulate, ca acestea să fie simple, măsurabile, accesibile, realiste și încadrate în timp.

Totodată, proiectul Strategiei urmează a fi adus în concordanță cu prevederile stipulate în pct. 9 lit. e) Hotărârea Guvernului nr. 33 din 11 ianuarie 2007 cu privire la regulile de elaborare și cerințele unificate față de documentele de politici, în special atragem atenția că. Strategia trebuie să include evaluarea impactului financiar, normă care nu a fost respectată de autor.

În același timp, pct. 109 și pct. 110 urmează a fi excluse și substituite cu un punct nou în următoarea redacție:

"Finanțarea Strategiei se va realiza din bugetul de stat(resurse generale, venituri colectate și resurse ale proiectelor finanțate din surse externe) și din alte surse conform legislației.".

La *anexa nr. 2 "Planul de acțiuni privind implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023".*

Potrivit Planului, realizarea unor obiective/acțiuni urmează a fi asigurată din contul surselor financiare externe. Totodată, nu este clar dacă sunt sau nu deja încheiate angajamente financiare externe pentru implementarea obiectivelor/acțiunilor propuse, Astfel, conform prevederilor pct. 6, subpct.6) din anexa nr. 1 la Hotărârea Guvernului nr. 696 din 30 august 2017 "Cu privire la organizarea și funcționarea Ministerului Finanțelor", ministerul este responsabil de coordonarea asistenței financiare externe, respective orice decizie care poate avea impact financiar asupra bugetului public national, urmează a fi consultată preliminar cu Ministerul Finanțelor.

În consecință, Ministerul Finanțelor consideră necesar revizuirea proiectului hotărârei Guvernului prin prizma obiecțiilor expuse.

Secretar general de stat **Ion CHICU**

Executor: Cornel Jaloba
Tel: 022 262873

CANCELARIA DE STAT A REPUBLICII MOLDOVA

Nr. 21-06-6442 Chişinău 6. 08. 2018

Serviciul de Informaţii şi Securitate

Referitor la proiectul hotărîrii Guvernului „Privind aprobarea proiectului de lege pentru aprobarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 şi a Planului de acţiuni pentru implementarea acesteia", prezentat prin demersul nr.18/700 din 10 iulie 2018, comunicăm următoarele.

La proiectul hotărîrii de Guvern:

1. Întrucît, conform prevederilor art.24 din Legea 100/2017 cu privire la actele normative, documentele de politici nu sînt acte normative, considerăm oportună aprobarea Strategiei sus-menţionate şi a Planului de acţiuni prin hotărîre de Parlament, dar nu prin lege.

La proiectul de lege:

2. La art.2 considerăm judicios de a exclude responsabilitatea Cancelariei de Stat de a prezenta rapoarte privind implementarea Strategiei şi Planului de acţiuni, precum şi de a transfera obligaţia respectivă Serviciului de Informaţii şi Securitate. Menţionăm că, în conformitate cu prevederile pct. 30 al Concepţiei securităţii informaţionale a Republicii Moldova, aprobată prin Legea nr.299/2017, Serviciul de Informaţii şi Securitate, în limita competenţelor, exercită atribuţiile autorităţii naţionale de coordonare a activităţii autorităţilor publice desfăşurate în domeniul securităţii informaţionale. Mai mult decît atît, în pct.28 al Concepţiei menţionate, care listează autorităţile statului cu atribuţii de asigurare a securităţii informaţionale, Cancelaria de Stat nu este menţionată.

La proiectul Strategiei:

3. Se propune extinderea termenului de implementare a Strategiei în 2019-2024, pentru a evita situaţia în care, la momentul adoptării Strategiei, primul an de implementare să fi expirat deja.

4. Capitolul I „Descrierea situaţiei" necesită a fi revizuit după cum urmează:

a) la pct.23 se va specifica tipul de „politici interne" ce urmează a fi adoptate de către operatorul de date cu caracter personal. Menţionăm că domeniul protecţiei datelor cu caracter personal este reglementat corespunzător de către legislaţia în vigoare şi că este în proces de implementare Strategia naţională în domeniul protecţiei datelor cu caracter personal pentru anii 2013–2018 şi Planul de acţiuni pentru implementarea acesteia;

Casa Guvernului,
MD-2033, Chişinău,
Republica Moldova

Telefon:
+ 373 22 250 104

Fax:
+ 373 22 242696

b) la pct.26, pe lîngă enumerarea documentelor de politici valabile până în anul 2020, tangențiale dimensiunii securității informaționale, urmează a fi inclusă o prezentare succintă a realizărilor de bază obținute prin implementarea documentelor respective, identificate problemele care împiedică implementarea corespunzătoare a acestora, precum și descrisă modalitatea prin care prezenta Strategie va dezvolta în continuare realizările obținute, pentru a asigura atingerea obiectivelor stabilite. La fel, este necesară includerea informației privind mecanismele ce vor fi utilizate pentru neadmiterea dublărilor de obiective și acțiuni ale prezentului document de politici cu documentele aflate deja în proces de implementare. Sintagma „Strategia propune reglementarea și abordarea unor segmente ale securității informaționale neelucidate anterior" de la pct.28 al proiectului nu clarifică suficient felul în care autorul va evita potențialele dublări de activități și resurse pentru realizarea acestora;

c) la pct.31 urmează a fi incluse date adiționale, care să confirme constatarea autorului privind „reglementarea insuficientă a componentei de protecție a spațiului mediatic".

5. La capitolul IV:

a) Pentru evitarea dublării neargumentate a acțiunilor de realizare a obiectivelor specifice, acestea vor fi prevăzute doar în Planul de acțiuni;

b) obiectivele specifice ale fiecărui Pilon urmează a fi formulate după principiul SMART – pentru a fi specifice, măsurabile, accesibile, realiste și determinate în timp. Mai mult decît atît, pentru fiecare obiectiv specific urmează a fi identificați indicatorii care vor permite evaluarea nivelului de atingere a obiectivului respectiv. Cu titlu de exemplu, menționăm că gradul de realizare a obiectivului nr.2 al Pilonului I, „Monitorizarea permanentă şi evaluarea periodică a nivelului securității spațiului cibernetic" în formularea actuală nu va putea fi evaluat;

c) obiectivul nr.7 al Pilonului I urmează a fi reformulat pentru a exclude caracterul declarativ al acestuia;

d) propunem înlocuirea tabelelor cu acțiuni din fiecare Pilon cu un tabel cu indicatori de impact care ar permite evaluarea rezultatelor obținute în cadrul fiecărui pilon;

e) Obiectivul nr.3 al Pilonului III repetă Obiectivul nr.3 al Pilonului I, de aceea propunem comasarea lor.

6. La capitolul V este oportună estimarea costurilor implementării Strategiei. Menționăm că estimarea necesarului de resurse pentru implementarea unui document de politici este o condiție obligatorie pentru aprobarea acestuia, care, în același timp, va contribui la implementarea lui eficientă.

7. La capitolul VI urmează a fi incluși indicatorii de progres care lipsesc. Indicatorii respectivi vor permite monitorizarea eficientă, precum și estimarea gradului de implementare a Strategiei.

8. În cadrul capitolului VII se impune includerea informației privind procedura de evaluare a implementării Strategiei.

La proiectul Planului de acțiuni:

9. Pentru fiecare acțiune planificată vor fi indicate termenul de realizare și costul estimativ de implementare.

10. Totodată, propunem examinarea suplimentară a acțiunilor planificate în raport cu acțiunile incluse în Planul de acțiuni pentru implementarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, în vederea excluderii dublărilor sau neconcordanțelor dintre acestea. Spre exemplu, Acțiunea 1 a Obiectivului 1, în conformitate cu pct.3.1. al Programului, urma a fi realizată încă în anul 2016. Situație similară este și în cazul acțiunilor 4 și 6 ale acestui obiectiv, care urmau a fi realizate în anul 2017.

11. La obiectivul nr. 1, acțiunea nr. 1 – *„crearea/desemnarea entității care va exercita rolul de Centru național de reacție...”*, la obiectivul nr. 10 acțiunea nr. 2 – *„crearea/ consolidarea laboratoarelor de securitate cibernetică...”*, la obiectivul nr. 11 acțiunea nr. 5 – *„certificarea specialiștilor în domeniul securității cibernetice ...”*, la obiectivul nr. 14 acțiunea nr. 1 – *„evaluarea spațiului Internet...”*, la obiectivul nr. 16 acțiunea nr. 1 – *„crearea la nivel național a entității...”*, se propune excluderea din rubrica „instituțiile responsabile” a I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” și includerea acesteia în rubrica „parteneri”.

12. La obiectivul nr. 2, acțiunea nr. 1 urmează a fi reformulată în corespundere cu acțiunile descrise la obiectivul nr. 2 „Monitorizarea permanentă și evaluarea periodică a nivelului securității spațiului cibernetic” al Pilonului I al Strategiei.

13. Acțiunea 1 a obiectivul nr. 6, precum și acțiunile 1,2 și 3 ale obiectivului 7 din cadrul Pilonului urmează a fi revizuite, deoarece sînt formulate drept obiective.

14. La obiectivul nr. 11 acțiunea nr. 6 – *„crearea platformelor web de sensibilizare și informare privind pericolele în spațiul cibernetic și măsurile de protecție ce pot fi luate de către persoanele fizice și juridice”*, se propune la rubrica „termen de realizare” substituirea sintagmei „2019-2020” cu sintagma „2019-2021”, avînd în vedere că realizarea acțiunii ține inclusiv de Cert-ul național, crearea căruia este stabilită pentru perioada 2018-2020.

15. Acțiunea 3 a obiectivului 12, cu excepția literei c), repetă acțiunile 2 și 3 de la obiectivul 9 al Pilonului I și, prin urmare, urmează a fi revizuită.

16. La obiectivul nr. 14 acțiunea nr. 1, se propune completarea rubricii „instituțiile responsabile” cu Ministerul Afacerilor Interne.

Totodată, oportunitatea acțiunii 1 a obiectivului 16 al Pilonului III necesită a fi argumentată suplimentar, în textul Strategiei fiind prezentată informația privind potențialul statut, precum și sarcinile și atribuțiile de bază ce urmează a fi atribuite entității care urmează a fi create. În același timp, propunem excluderea acțiunii 3 a aceluiași obiectiv, dat fiind faptul că un complex de măsuri de informare a publicului sînt deja menționate la acțiunile 6 și 7 ale Obiectivului 11 al Pilonului I.

17. La acțiunea 2 a obiectivului 21 al Pilonului III se impune a fi revizuită lista responsabililor de implementare prin excluderea SIS în calitate de responsabil și includerea tuturor instituțiilor ce urmează a remite rapoarte în adresa SIS despre starea de risc de la instituțiile statului cu competență în domeniul securității informaționale.

18. La obiectivul nr. 25 acțiunea nr. 1 și acțiunea nr. 2 este oportună substituirea sintagmei „CTS” cu sintagma „STISC”, avînd în vederea reorganizarea Î.S. „Centrul de telecomunicații speciale”.

19. În subsidiar, comunicăm că susținem opinia Agenției de Guvernare Electronică referitoare la proiectele vizate, enunțată în scrisoarea adresată Serviciului de Informații și Securitate și Cancelariei de Stat cu nr.3007-50 din 20.07.2018.

CANCELARIA DE STAT A REPUBLICII MOLDOVA
DIRECȚIA MANAGEMENTUL DOCUMENTELOR ȘI PETIȚII
3

Secretar general adjunct al Guvernului **Roman CAZAN**

Ex.: N. Sandu
Tel.: 0 22 250 579

SERVICIUL TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

MD-2012 mun. Chișinău, Piața Marii Adunări Naționale, 1 IDNO 1003600096694
tel.: + 373 22 820 900, fax: + 373 22 250 522 e-mail: stisc@stisc.gov.md, itsec@itsec.gov.md

Nr. 132 din 20.07. 2018

La nr. 18/701 din 10.07. 2018

Domnului Vasile BOTNARI,
Director al Serviciului de Informații și Securitate al Republicii Moldova

Stimate domnule director,

Examinînd proiectul Hotărîrii Guvernului privind aprobarea proiectului de lege pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și a Planului de acțiuni pentru implementarea acesteia, comunicăm susținerea acestuia, precum și necesitatea modificării/completării planului de acțiuni pentru implementarea Strategiei Securității informaționale a Republicii Moldova pentru anii 2018-2023, după cum urmează:

- la obiectivul nr. 1, acțiunea nr. 1– „*crearea/desemnarea entității care va exercita rolul de Centru național de reacție la incidentele de securitate cibernetică și care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autoritățile publice competente și persoanele fizice și juridice: elaborarea și promovarea cadrului normativ; crearea Centrului național de reacție la incidentele de securitate cibernetică*”, se propune excluderea din rubrica „instituțiile responsabile” a I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”, și includerea acesteia în rubrica „parteneri”, precum și completarea rubricii „instituțiile responsabile” cu Cancelaria de Stat.

- la obiectivul nr. 1, acțiunea nr. 2, „*desemnarea entității care va exercita rolul de Centru Guvernamental de reacție la incidentele de securitate cibernetică, și care va constitui punctul de raportare al incidentelor de securitate cibernetică al Guvernului, și stabilirea interacțiunii acestuia cu Centrul național de reacție la incidentele de securitate cibernetică*”, se propune completarea rubricii „instituțiile responsabile” cu Cancelaria de Stat.

- la obiectivul nr. 2, acțiunea nr. 1 urmează a fi modificată și expusă în corespundere cu acțiunile descrise la obiectivul nr. 2 „Monitorizarea permanentă și evaluarea periodică a nivelului securității spațiului cibernetic” al Pilonului I al Strategiei.

SIS al RM
Ho nr. 18/701
24 07 2018

- la obiectivul nr. 10, acțiunea nr. 2, „*crearea/consolidarea laboratoarelor de securitate cibernetică din cadrul instituțiilor de învățământ superior și instituțiile de cercetare științifică*” se propune excluderea din rubrica „instituțiile responsabile” a I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”, și includerea acesteia în rubrica „parteneri”;

- la obiectivul nr. 11, acțiunea nr. 5, „*certificarea specialiștilor în domeniul securității cibernetice de către organizațiile/companiile specializate reieșind din standardele aplicate și cerințele minime obligatorii de securitate cibernetică aprobate*” se propune excluderea din rubrica „instituțiile responsabile” a I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”, și includerea acesteia în rubrica „parteneri”;

- la obiectivul nr. 11, acțiunea nr. 6, „*crearea platformelor web de sensibilizare și informare privind pericolele în spațiul cibernetic și măsurile de protecție ce pot fi luate de către persoanele fizice și juridice*” se propune la rubrica „termen de realizare” substituirea sintagmei „2019- 2020” cu sintagma „2019-2021”, avînd în vedere faptul că realizarea acțiunii ține inclusiv de Cert-ul național, crearea căruia este stabilită pentru perioada 2018-2020.

- la obiectivul nr. 14, acțiunea nr. 1, „*evaluarea spațiului Internet din perspectiva identificării actorilor implicați în producerea și diseminarea conținutului media on-line și alți intermediari și servicii auxiliare ce au impact pentru securitatea informațională;*” se propune excluderea din rubrica „instituțiile responsabile” a I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”, și includerea acesteia în rubrica „parteneri”, precum și completarea rubricii „instituțiile responsabile” cu Ministerul Afacerilor Interne.

- la obiectivul nr. 16, acțiunea nr. 1, „*crearea la nivel național a entității ce va avea competențe de promovare și coordonare a politicilor de securitate informațională într-o societate democratică, în funcție de dezvoltarea tehnologiei, raporturile juridice și de altă natură din sectorul societății informaționale la nivel național și internațional (Consiliul coordonator pentru asigurarea securității informaționale)*” se propune excluderea din rubrica „instituțiile responsabile” a I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”, și includerea acesteia în rubrica „parteneri”.

- la obiectivul nr. 25, acțiunea nr. 1 și acțiunea nr. 2 este oportună substituirea sintagmei „CTS” cu sintagma „STISC”, avînd în vederea reorganizarea Î.S. „Centrul de telecomunicații speciale”.

Cu respect,

Director **Serghei POPOVICI**

AGENȚIA DE GUVERNARE ELECTRONICĂ

E-GOVERNANCE AGENCY

Republic of Moldova, Chisinau, MD-2012, 42 B, Alexandr Puskin st.
Phone: +373 22 820 026, email: office@egov.md, web: http://www.egov.md

Nr. 3007-50 din 20.07.2018
La nr. 18/701 din 10.07.2018

Serviciul de Informații și Securitate

Copie: **Cancelaria de Stat**

Agenția de Guvernare Electronică a examinat **proiectul de Lege pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și a Planului de acțiuni pentru implementarea acesteia** *(prezentat spre examinare de către Serviciul de Informații și Securitate prin scrisoarea nr.18/701 și nr.18/700 din data de 10.07.2018)* și bazându-se pe atribuțiile funcționale ale Instituției stabilite în Statutul acesteia, aprobat prin Hotărârea Guvernului nr.760 din 18.08.2010, și atribuțiile delegate de către Guvern în temeiul altor acte normative aferente domeniilor modernizării serviciilor publice și e-Transformării Guvernării, comunică următoarele.

Acțiunile prevăzute la **pct.81** din Strategia securității informaționale a Republicii Moldova pentru anii 2018-2023 (*Obiectivul nr.2. Monitorizarea permanentă și evaluarea periodică a nivelului securității spațiului cibernetic*), și anume **lit.b) pct.1** și **pct.2** urmează a fi excluse, deoarece depășesc competența Agenției de Guvernare Electronică în domeniul auditului de securitate cibernetică.

În acest context, recomandăm consultarea suplimentară a pct.11 sbpct.11)-17) din Statutul Instituției Publice „Agenția de Guvernare Electronică", aprobat prin HG nr.760/2010, cu modificările și completările ulterioare.

Totodată, aceeași situație se referă și la Planul de acțiuni pentru implementarea Strategiei nominalizate, și anume urmează a fi excluse **sbpct.1)** și **lit.b)** din pct.2 (*Monitorizarea permanentă și evaluarea periodică a nivelului securității spațiului cibernetic*), deoarece depășesc competența Agenției de Guvernare Electronică în domeniul auditului de securitate cibernetică.

În același timp, atragem atenția asupra riscului dublării unor acțiuni în domeniul securității cibernetice între proiectul de lege prezentat pentru avizare și prevederile actelor normative existente, în special inițiativa Ministerului Economiei și Infrastructurii privind modificarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020.

Reiterăm recunoștința pentru atenția și atitudinea manifestată de Dumneavoastră în conlucrare cu Agenția de Guvernare Electronică.

Director Semnat electronic **Eugeniu URSU**

Ex.: Veaceslav Pușcașu, Viorel Zabolotnic,
tel.: 022 820024, 820021
email: veaceslav.puscasu@egov.md
viorel.zabolotnic@egov.md

SIS al RM
la nr. 18/701
23 07 2018

Digitally signed by Ursu Eugeniu
Date: 2018.07.20 17:23:06 EEST
Reason: MoldSign Signature
Location: Moldova

AGENŢIA SERVICII PUBLICE A REPUBLICII MOLDOVA
PUBLIC SERVICES AGENCY OF THE REPUBLIC OF MOLDOVA

MD-2012, municipiul Chişinău, str. Aleksandr Puşkin, nr.42 42, Aleksandr Pushkin str., MD-2012 Chisinau
Tel.: +373 22 50 46 54 Fax: +373 22 21 22 59 e-mail: asp@asp.gov.md, web: asp.gov.md

30.07.18 nr. 01/4546

La nr. 18/701 din 10 iulie 2018

Serviciul de Informaţii şi Securitate

Agenţia Servicii Publice a examinat *proiectul de lege pentru aprobarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 şi a Planului de acţiuni pentru implementarea acesteia* şi vă comunică despre lipsa propunerilor şi obiecţiilor la proiectul dat.

Director **Serghei RAILEAN**

Dorina Ursu, 022 504 084

SIS al RM
Le nr. 18/701
31 07 2018

AGENŢIA DE STAT
PENTRU PROPRIETATEA INTELECTUALĂ
A REPUBLICII MOLDOVA

Str. Andrei Doga nr. 24/1, MD-2024, Chişinău, Republica Moldova
Tel: (+373-22) 400-508, (+373-22) 400-583, Fax: (+373-22) 440-119
www.agepi.gov.md, e-mail: office@agepi.gov.md

IDNO 1015601000112

STATE AGENCY
ON INTELLECTUAL PROPERTY
OF THE REPUBLIC OF MOLDOVA

24/1 Andrei Doga str., MD-2024, Chisinau, Republic of Moldova
Tel: (+373-22) 400-508, (+373-22) 400-583, Fax: (+373-22) 440-094
www.agepi.gov.md, e-mail: office@agepi.gov.md

nr. 1761
din 2018 SEP. 12.

Serviciul de Informaţii şi Securitate
al Republicii Moldova
bd. Ştefan cel Mare şi Sfînt, 166,
MD – 2004, Chişinău, Republica Moldova

la nr. 18/701 din 10.07.2018

Agenţia de Stat pentru Proprietatea Intelectuală (AGEPI) a examinat proiectul de lege pentru aprobarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 şi a Planului de acţiuni pentru implementarea acesteia şi, reieşind din limitele competenţelor funcţionale, comunică lipsa de obiecţii şi propuneri pe marginea acestora.

Lilia BOLOCAN,
Director General

SIS al RM
18/701
10 09 2018

Ex: D. Morari
tel. 022 400 652

Procuratura Republicii Moldova

Republica Moldova, MD-2005, mun.Chișinău, str.Mitropolit Bănulescu-Bodoni, 26,
tel.(022) 22-50-75, fax (022) 21-20-32, e-mail: proc-gen@procuratura.md

23.07.2018 nr. 28- 2d/18-451
la nr. 18/701 din 10.07.2018

Domnului Vasile BOTNARI,
Director al Serviciului de
Informații și Securitate

Stimate Domnule director,

Procuratura Generală a examinat proiectul de lege pentru aprobarea *Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și a Planului de acțiuni pentru implementarea acesteia.*

Susținem proiectul propus spre avizare, totodată, în scopul îmbunătățirii acestuia, înaintăm unele propuneri, inclusiv sub aspect redacțional, după cum urmează:

1. La pct.111 din proiect, după cuvintele *„organizațiile internaționale"* considerăm oportun de a completa cu sintagma *„și regionale"*.

2. La pct.112, subpct.3) din proiect, propunem substituirea sintagmei *„datelor personale"* cu sintagma *„datelor cu caracter personal"*, în vederea corelării terminologiei utilizate cu prevederile cadrului juridic existent *(Legea nr.133 din 08.07.2011 privind protecția datelor cu caracter personal)*.

3. Întru respectarea prevederilor art.54 alin. (1) lit.a) din Legea nr.100 din 22.12.2017 cu privire la actele normative, propunem revizuirea proiectului în integritate, din motiv că în textul acestuia sunt unele greșeli gramaticale (spre exemplu:la pct.92 subpct.1) lit.b) *mass media*; la pct.104 subpct. 1) *inter-instituționale* etc.).

Alte obiecții și propuneri nu sunt.

Cu respect,

Adjunct al Procurorului General **Iurii GARABA**

Ex.: Cealic Zinaida
Tel:022-223077

SIS al RM
la nr 18/701
26 07 2018

Banca Națională a Moldovei

Nr. 31-002/16/2951 "27" iulie 2018

Serviciul de Informații și Securitate al Republicii Moldova
Bd.Ștefan cel Mare și Sfânt, 166
mun.Chișinău, MD-2004

Cu referire la proiectul de lege pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și a Planului de acțiuni pentru implementarea acesteia, remis spre examinare prin scrisoarea nr.18/701 din 10 iulie 2018, Banca Națională a Moldovei Vă comunică următoarele:

Considerăm că în calitate de *"Instituție responsabilă"* pentru acțiunea 8.3 *"Identificarea mecanismelor comune de combatere a fraudelor card-present și card not-present"* din Planul de acțiuni urmează a fi reținute doar organele abilitate cu atribuții de urmărire penală, care dețin competențe nemijlocite în cercetarea infracțiunilor.

Opinăm că, eventual, Banca Națională a Moldovei ar putea fi indicată la coloana *„Parteneri"* a acțiunii 8.3, având în vedere că anumite cerințe, ce țin de identificarea de către prestatorii de servicii de plată a utilizării frauduloase a cardurilor emise şi/sau acceptate, ținerea evidenței cazurilor de fraudă, luarea măsurilor necesare pentru minimizarea fraudelor şi descurajarea tentativelor de fraudă cu carduri ale personalului propriu, deținătorilor de carduri, comercianților şi altor persoane, elaborarea unor proceduri interne relevante în acest sens, sunt reglementate în actele normative ale acesteia (*spre exemplu, a se vedea pct.7, 9, 51 din Regulamentului cu privire la cardurile de plată, aprobat prin Hotărârea Consiliului de Administrație al Băncii Naționale a Moldovei nr.157 din 01 august 2013*).

Totodată, ținem să menționăm că reglementările respective sunt emise în vederea exercitării unei atribuții de bază a Băncii Naționale a Moldovei – supravegherea sistemelor de plăți în Republica Moldova (*art.49[1] din Legea nr.548-XIII din 21 iulie 1995 cu privire la Banca Națională a Moldovei*), atribuție din care derivă - întru asigurarea funcționării stabile și eficiente a acestora, promovarea încrederii publicului în efectuarea plăților fără numerar - dreptul emiterii unor recomandări referitoare la prevenirea cazurilor de fraudă aferente utilizării cardurilor de plată (*a se vedea Anexa la Regulamentului cu privire la cardurile de plată, aprobat prin Hotărârea Consiliului de Administrație al Băncii Naționale a Moldovei nr.157 din 01 august 2013*) și nu abilitează cu competențe care să contribuie direct la identificarea mecanismelor de combatere a fraudelor.

SIS al RM
nr. 18/701
01 08 2018

Adresa: Bulevardul Grigore Vieru nr. 1,MD-2005, Chişinău, Republica Moldova
Tel: (+373) 22 822 606, Fax: (+373) 22 220 591, email: official@bnm.md, web: www.bnm.md

Adițional, recomandăm uniformizarea noțiunilor cu care se operează în proiect *(pct.87.1) din Strategie; pct.8.1) – 3) din Planul de acțiuni - "instituții bancare"; "băncile și instituțiile financiare")*, cu luarea în considerare a prevederilor art.148 alin.(4) din Legea nr.202 din 6 octombrie 2017 privind activitatea băncilor (în vigoare din 1 ianuarie 2018) – *"Orice referire sau trimitere, în actele normative existente, la data intrării în vigoare a prezentei legi, la termenul de "instituție financiară" se va considera ca referire și/sau trimitere la termenul de "bancă" prevăzut la art.3 din prezenta lege."*.

Cu respect,

Cristina HAREA
Viceguvernator

ex. S.Aghenie
tel. (+373) 22 822 493

CENTRUL NAȚIONAL PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL AL REPUBLICII MOLDOVA

MD-2004, mun. Chișinău, str. Serghei Lazo, 48, tel: +373-22-820801, fax: +373-22-820807, www.datepersonale.md

Nr. 04-06/1690
La nr. 18/701 din 10 iulie 2018

„31" iulie 2018

Serviciul de Informații și Securitate al Republicii Moldova

Centrul Național pentru Protecția datelor cu Caracter Personal al Republicii Moldova (CNPDCP) a examinat proiectul de lege pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și a Planului de acțiuni pentru implementarea acesteia și comunică despre susținerea acestuia.

Totodată, propunem includerea CNPDCP, în calitate de autoritate partener la următoarele acțiuni din Planul de acțiuni pentru implementarea Strategiei:

1. Obiectivul 1.: *Crearea unui sistem integrat de comunicare și evaluare a amenințărilor la adresa securității informaționale și de elaborare a măsurilor operative de răspuns,* acțiunea 2);

2. Obiectivul 2.: *Monitorizarea permanentă și evaluarea periodică a nivelului securității spațiului cibernetic*, acțiunea 3);

3. Obiectivul 3.: *Consolidarea capacităților de apărare cibernetică*, acțiunile 2) și 3);

4. Obiectivul 9.: *Dezvoltarea capacităților instituționale în combaterea criminalității informatice,* acțiunile 2), 3) și 4);

5. Obiectivul 11.: *Dezvoltarea capacităților de reziliență cibernetică și ridicarea nivelului de cultură în domeniul TIC*, acțiunile 2), 3) și 4);

6. Obiectivul 22.: *Dezvoltarea sistemului de pregătire a resurselor umane în domeniul securității informaționale*, acțiunile 3) și 4).

De asemenea, reieșind din importanța asigurării securității datelor cu caracter personal în contextul asigurării securității cibernetice, solicităm ca la acțiunea 5) din Obiectivul 4. *Protecția rețelelor de comunicații speciale ale Republicii Moldova și a informației cu accesibilitate limitată, pentru menținerea funcțiilor vitale ale statului*, să fie incluse în calitate de autorități partenere: MAI, SIS PG și STISC.

Eduard RĂDUCAN
Director

SIS al RM
la nr. 18/701
07 08 2018

Ex: Angela Colomiicenco
Tel: (022) 820 804

COMISIA ELECTORALĂ CENTRALĂ
A REPUBLICII MOLDOVA

str.Vasile Alecsandri nr.119, MD 2012 Chişinău, Republica Moldova
tel. (+373 22) 251-451, fax (+373 22) 234-047
www.cec.md, e-mail: info@cec.md

Nr. CEC 8/ 2662 **din** 12 septembrie **20** 18

La nr. 18/701 din 10 iulie 2018

Domnului Vasile BOTNARI,
Director al Serviciului de Informaţii şi Securitate

Cu referire la solicitarea de a da un aviz asupra proiectului de lege pentru aprobarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023, vă informăm că nu avem obiecţii la acesta.

Cu respect,

Preşedintele
Comisiei Electorale Centrale **Alina RUSSU**

Ex.: Alexandru Balmoş
Tel.: 022-201-895

ACADEMIA DE ŞTIINŢE A MOLDOVEI

bd. Ştefan cel Mare , 1
MD-2028 Chişinău,
Republica Moldova
Tel: +373-22-27-40-47
Fax: +373-22-54-28-23
E-mail: tiginyanu@asm.md

ACADEMY OF SCIENCES OF MOLDOVA

Stefan cel Mare Ave., 1
MD-2001 Chisinau,
Republic of Moldova
Tel: +373-22-27-40-47
Fax: +373-22-54-28-23
E-mail: tiginyanu@asm.md

Nr. 193-01/5 din 09.08. 2018

Dlui Vasile BOTNARI,
Director al Serviciului de Informaţii şi Securitate al Republicii Moldova

Stimate dle Director,

Prin prezenta, Academia de Ştiinţe a Moldovei Vă informează că a examinat proiectul *Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023* şi *Planul de acţiuni pentru implementarea acesteia* şi avizează pozitiv conţinutul acestora. Totodată, în asigurarea (i) respectării cadrului naţional de elaborare a documentelor de politici şi (ii) unor soluţii eficiente de contracarare a riscurilor şi ameninţărilor la adresa securităţii informaţionale, intervenim cu unele remarci şi sugestii:

1. În cadrul notei informative la proiectul Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 şi Planului de acţiuni pentru implementarea acesteia se menţionează că „*Capitolul I – Introducere* descrie evoluţia curentă a tehnologiilor informaţionale ..., precum şi evidenţiază principalele vulnerabilităţi, riscuri şi ameninţări la adresa societăţii informaţionale şi a mediului naţional şi general de securitate". De regulă, descrierea problemei în evoluţie sau contextul care determină necesitatea elaborării unei strategii trebuie să se regăsească în cadrul compartimentului „Descrierea situaţiei" (A se vedea: Ghid metodologic cu privire la procesul decizional, www.rapc.gov.md/file/Ghid%20procesul%20decizional_revi), iar în conţinutul „Introducerii" se indică deciziile care au dus la elaborarea strategiei, de exemplu conexiunea cu Concepţia securităţii informaţionale, perioada propusă de implementare, părţile implicate în elaborarea strategiei. În mare parte, aceasta va contribui la asigurarea unui conţinut succint şi explicit al introducerii (volum: 1 - 1,5 pag.).
2. În acelaşi timp, ţinem să remarcăm că deşi se menţionează că sunt evidenţiate „principalele vulnerabilităţi, riscuri şi ameninţări la adresa societăţii informaţionale şi a mediului naţional şi general de securitate", totuşi în proiectul Strategiei nu se regăseşte o clasificare a acestora din perspectiva securităţii informaţionale sau au un caracter haotic.
3. Reieşind din faptul că proiectul Strategiei respective se referă la una din dimensiunile securităţii – securitatea informaţională –, este binevenit ca în cadrul compartimentului „Descrierea situaţiei" contextul care determină necesitatea şi importanţa elaborării şi

adoptării unei astfel de strategii de structurat la nivel național, regional și internațional. Aceasta ar permite de accentuat situația privind asigurarea securității informaționale la nivel național, fundamentând necesitatea compartimentării acțiunilor prin prisma celor patru piloni menționați în introducerea Strategiei (punctul 15). În același timp, aceasta ar asigura evitarea generalizărilor sau constatărilor și focusarea pe argumente în baza unor analize sau cercetări. De exemplu, la pagina 8, punctul 31 se menționează că „Analiza evoluției fenomenului social-media și presei electronice reliefează reglementarea insuficientă a componentei de protecție a spațiului mediatic de la amenințări cu caracter hibrid și a componentei de securitate. ..." Aici apare întrebarea „Conform cărei analize?". Dacă este vorba de o analiză efectuată, atunci rezultatul problemelor identificate trebuie să se regăsească în cadrul compartimentului „Descrierea problemelor". În același timp, sensul propoziției/constatării trebuie revăzut, căci nu este clar despre ce „componentă de securitate" este vorba.

4. Referindu-ne la capitolul III „Definirea problemei", constatăm lipsa unui fundament metodologic de identificare a problemelor, de exemplu efectuarea unei analize calitative și cantitative cu referire strictă la Republica Moldova. Cadrul național privind elaborarea de politici evidențiază că analiza problemei este importantă pentru a înțelege cauzele, efectele, amploarea, categoriile afectate și cum ar putea evolua problema în timp.

Cu respect,

Președinte interimar

Academician

Ion TIGHINEANU

Ex: Vicedirector, doctor habilitat în științe politice,
profesor universitar, Victor JUC Tel (022) 54-66-92.

CONSILIUL COORDONATOR AL AUDIOVIZUALULUI AL REPUBLICII MOLDOVA

MD-2012, Chişinău, str. V. Pârcălab nr. 46
Tel.: (+373 22) 27-75-51, fax: (+373 22) 27-74-71
e-mail: office@cca.md, http://www.cca.md

THE COORDINATING COUNCIL OF AUDIOVISUAL OF THE REPUBLIC OF MOLDOVA

MD-2012, Chisinau, V. Pârcălab str., № 46
Tel: (+373 22) 27-75-51, fax: (+373 22) 27-74-71
e-mail: office@cca.md, http://www.cca.md

nr. 535 din 18 iulie 2018
la nr. 18/7 din 10 iulie 2018

Dlui Vasile BOTNARI,
Director al Serviciului de Informaţii şi Securitate
al Republicii Moldova
(MD-2004, mun. Chişinău, bd. Ştefan cel Mare şi Sfânt, nr. 166)

Stimate Domnule Director,

AVIZ

Consiliul Coordonator al Audiovizualului expediază Avizul la proiectul de Lege pentru aprobarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 şi al Planului de acţiuni pentru implementarea acesteia, urmare a examinării solicitării nr. 18/7 din 10 iulie 2018.

Consiliul Coordonator al Audiovizualului este o autoritate publică autonomă, reprezentantul şi garantul interesului public în domeniul audiovizualului.

În limitele competenţelor sale legale, prevăzute de Codul audiovizualului, autoritatea este responsabilă pentru implementarea şi respectarea legislaţiei audiovizuale, precum şi participarea la negocieri internaţionale, exclusiv în domeniul mijloacelor de informare şi comunicare audiovizuală.

Menţionăm că, la data de 20 aprilie curent, în Parlamentul Republicii Moldova a fost votat, în prima lectură, Codul Serviciilor Media Audiovizuale al Republicii Moldova asupra căruia au parvenit recomandări din partea reprezentantului OSCE pentru libertatea presei al Organizaţiei pentru Securitate şi Cooperare în Europa şi avizul Direcţiei Generale Dreptului Omului şi Statul de Drept al Consiliului Europei în sfera audiovizuală, prin care autorităţii regulatorii nu i-au fost extinse limitele competenţelor existente. Totodată, remarcăm că acestea nu se regăsesc printre competenţele autorităţilor omoloage din majoritatea statelor UE şi CSI.

Este de specificat că, actorii implicaţi în mass-media fac parte din diverse domenii, precum: media scrisă, media on-line şi media audiovizuală. Acestea, cu excepţia celei din urmă, reprezintă un obiect al altor reglementări legislative, care stabilesc nu doar modul de organizare şi funcţionare, dar şi competenţele în cazul nerespectării prevederilor legale.

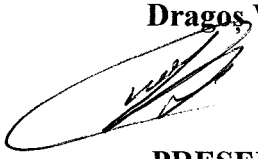
În acest sens, revendicarea drepturilor şi libertăţilor fundamentale ale omului încălcate de posturile de televiziune sau radio, în cadrul emisiunilor, nu pot fi exercitate decât pe cale judiciară, iar autoritatea de reglementare este responsabilă de examinarea sesizărilor cu privire la neacordarea dreptului la replică solicitantului de către postul de radio/TV.

Ca urmare a examinării proiectului de Lege pentru aprobarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 şi al Planului de acţiuni pentru implementarea acesteia, CCA prezintă lipsa de obiecţii şi propuneri asupra actelor sus-menţionate, **cu condiţia exercitării atribuţiilor în limitele competenţelor exclusiv pe dimensiunea media audiovizuală, aşa cum este stipulat în actualul Cod al Audiovizualului, cât şi în proiectul Codului Serviciilor Media Audiovizuale.**

În contextul unei colaborări eficiente, Vă asigurăm de toată considerațiunea noastră.

Cu respect,

Dragoș VICOL



PREȘEDINTE

Compania "Teleradio – Moldova"
instituţia publică naţională a audiovizualului
str. Mioriţa, 1, MD-2028, Chişinău, Republica Moldova; www.trm.md; trm@trm.md
tel: +373 22 72-10-47, +373 22 22-82-84; fax: +373 22 72-33-52

Data 12.08.18 nr. 01-10/493

Serviciul de Informare şi Securitate
Dlui Vasile Botnari, director

Cu referire la scrisoarea nr.18/~~701~~c din 10 iulie 2018 Vă comunicăm următoarele: IPNA Compania „Teleradio-Moldova" avizează pozitiv proiectul de lege privind aprobarea Strategiei securităţii informaţionalea a Republicii Moldova pentru anii 2018 – 2023 şi a Planului de acţiuni pentru implementarea acesteia.

Cu respect,
Preşedintele Companiei **Olga BORDEIANU**

Ex: Vulpe C
069151854

SIS al RM
nr. 18/701
13 07 2018

MINISTERUL JUSTIȚIEI
AL REPUBLICII MOLDOVA

str. 31 August 1989, nr. 82
MD- 2012, mun. Chișinău,
tel.: 0 22 23 47 95, fax: 0 22 23 47 97
www.justice.gov.md

04/9854 din 17.08.2018
La nr. 18/801 din 03.08.2018

Serviciul de Informații și Securitate

Ministerul Justiției a examinat proiectul legii pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-20203 și a Planului de acțiuni pentru implementarea acesteia, și comunică următoarele.

La proiectul hotărârii Guvernului:

1. Sursa publicării actelor normative se va indica după formula „(Monitorul Oficial al Republicii Moldova, anul publicării, numărul Monitorului, numărul articolului)".

2. În temeiul art. 41 din *Legea 136 din 7 iulie 2017 cu privire la Guvern*, precum și a pct. 6 din *Regulamentul privind organizarea și funcționarea Ministerului Justiției*, aprobat prin *Hotărârea Guvernului nr. 698 din 30 august 2017,* care stabilesc exercitarea funcției de reprezentant al Guvernului în Parlament de către Ministerul Justiției, în lista contrasemnatarilor se va include ministrul justiției.

La proiectul legii:

3. În scopul asigurări clarității prevederilor actului normativ, art. 1 se va expune conform următoarei redacții: „Art. 1. – Se aprobă:

Strategia securității informaționale a Republicii Moldova pentru anii 2018-2023, conform anexei nr. 1;

Planul de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023, conform anexei nr. 2."

La proiectul Strategiei (anexa nr. 1):

4. La pct. 16 se vor revedea cuvintele „Anexă la prezenta Strategie", întrucât conform art. 1 din proiectul legii, Planul de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova reprezintă anexa nr. 2 la aceasta.

5. Pct. 17 este unul inutil, și prin urmare, se va exclude.

6. Pct. 18 se va completa cu referința la *Legea nr. 122 din 2 iulie 2014 pentru ratificarea Acordului de Asociere între Republica Moldova, pe de o parte, și Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de altă parte.*

7. La pct. 44 în virtutea caracterului obligatoriu al actelor normative, cuvintele „în vigoare" se vor exclude (obiecție valabilă și pentru restul referințelor la legislația în vigoare din proiect).

8. La capitolul VII Proceduri de monitorizare și evaluare se va ține cont de prevederile pct. 38 din *Regulile de elaborare și cerințele unificate față de*

documentele de politici, aprobate prin Hotărârea Guvernului nr. 33 din 11 ianuarie 2007, potrivit căruia, raportul de monitorizare trebuie să identifice cel puţin următoarele aspecte: remanierile instituţionale care au survenit în urma implementării; modificarea situaţiei grupurilor-ţintă vizate de document, atît pe parcursul implementării, cît şi la finalizarea acesteia; impactul în urma implementării (economic, juridic, social, ecologic etc.); costurile implementării; gradul de respectare de către responsabilii pentru implementare a termenelor, costurilor şi conţinutului acţiunilor din cadrul planului de implementare; motivele neexecutării sau executării parţiale.

9. La pct. 116, cuvintele „pe pagina-web oficială" se vor substitui cu cuvintele „pe pagina oficială", în conformitate cu *Regulamentul cu privire la paginile oficiale ale autorităţilor administraţiei publice în reţeaua Internet*, aprobat prin *Hotărârea Guvernului nr. 188 din 3 aprilie 2012*.

La proiectul Planului de acţiuni (anexa nr. 2):

10. La obiectivul 1 nu este clar stabilită denumirea acţiunii 3), iar sistematizarea datelor statistice la capitolul securităţii cibernetice, analiza şi evaluarea acestora se va expune ca o acţiune aparte sau o subacţiune.

11. La obiectivul 2 acţiunea 1) litera b) nu este stabilit indicatorul de progres, iar la obiectivul 2, acţiunea 2) necesită precizare indicatorul stabilit (obiecţie valabilă şi pentru obiectivele/acţiunile 5. 1), 5. 2), 5. 5), 8. 1), 12. 2), etc).

12. La obiectivul 2 acţiunea 3) cu referire la *Consiliul coordonator pentru asigurarea securităţii informaţionale*, atenţionăm că nu poate fi desemnat în calitate de instituţie responsabilă de realizarea unor acţiuni o entitate care nu este creată.

13. La obiectivul 3 acţiunile 2) şi 3) se vor corela indicatorii de progres, întrucât ambele prevăd elaborarea unor măsuri de protecţie.

14. La obiectivul 4 acţiunea 1) indicatorul de progres nu corespunde acţiunii prevăzute, în acest sens se vor reanaliza obiectivele/acţiunile 4. 6), 9. 3), 10. 1), 12. 3), 16. 1), 17. 3) şi 17. 6).

15. La obiectivul 4 acţiunea 2) se va revedea indicatorul în sensul că acesta trebuie să fie măsurabil (ex. numărul controalelor efectuate). Sub acest aspect se vor reexamina obiectivele/acţiunile 6. 1), 6. 2), 7. 1), 7. 2), 7. 3), precum şi altele similare.

16. La obiectivul 13 acţiunea 1) societatea civilă şi organizaţii mass-media nu sunt subiecţi de drept subordonaţi Guvernului şi nu pot fi obligate să preia anumite sarcini. Din acest considerent, acestea vor fi menţinute în plan, în calitate de parteneri, în colaborare cu care se va atinge rezultatul scontat (obiecţie valabilă şi pentru restul cazurilor similare din proiect).

17. La obiectivul 14 acţiunea 2) menţionăm că, potrivit pct.6 din *Hotărârea Guvernului nr.698 din 30 august 2017 cu privire la organizarea şi funcţionarea Ministerului Justiţiei*, acesta este responsabil de elaborarea politicilor în domeniul justiţiei, drepturilor omului, profesiilor şi serviciilor juridice, precum şi politicile punitive ale statului. Acesta nu este responsabil de elaborarea politicilor în domeniul securităţii spaţiului mediatic.

Conform art. 40 alin. (1) lit. d[1]) din *Codul audiovizualului nr. 260-XVI din 27 iulie 2006*, Consiliului Coordonator al Audiovizualului monitorizează și supraveghează respectarea de către radiodifuzorii și distribuitorii de servicii a prevederilor prezentului cod privind asigurarea securității. Totodată, având în vedere prevederile art. 1 alin. (1) din *Legea nr. 753-XIV din 23 decembrie 1999 privind Serviciul de Informații și Securitate al Republicii Moldova*, Serviciul de Informații și Securitate este organul de stat specializat în domeniul asigurării securității de stat, inclusiv a securității informaționale.

Prin urmare, luând în considerare competențele funcționale, Ministerul Justiției nu poate fi instituția responsabilă de executarea acțiunii respective.

18. În partea ce ține de atribuirea în competența Ministerului Justiției a unor acțiuni privind elaborarea politicilor ce țin de *asigurarea transparenței financiare în activitatea autorităților publice, asociațiilor obștești și societăților comerciale în contextul asigurării securității informaționale*, stabilite la acțiunea 15, se reiterează poziția enunțată supra.

Mai mult, având în vedere faptul că în prezent cadrul legislativ instituie principiul transparenței în gestionarea resurselor financiare publice, nu este clar ce măsuri legislative urmează a fi întreprinse în acest sens. Menționăm că, *Legea finanțelor publice și responsabilității bugetar-fiscale nr. 181 din 25 iulie 2014* stabilește la art. 12 alin. (2) că, bugetele se elaborează, se aprobă și se administrează în mod transparent, având la bază: a) procesul bugetar, bazat pe un calendar bugetar și pe proceduri transparente; b) roluri și responsabilități bine definite în procesul bugetar; c) informație bugetară cuprinzătoare, elaborată și prezentată publicului într-o manieră clară și accesibilă.

De asemenea, art. 38 alin. (2) din *Legea nr. 837-XIII din 17 mai 1996 cu privire la asociațiile obștești* prevede că controlul asupra surselor de venit, cuantumului mijloacelor obținute, plății impozitelor și asupra altei activități financiare a asociației obștești îl exercită organele de control financiar și administrare fiscală.

Adițional, în partea ce ține de obiectivul 15, acțiunile 1) și 2) comunicăm că acestea au un conținut ambiguu fiind lipsite de previzibilitate, prin urmare în eventualitatea adoptării acestora va fi dificil de identificat măsurile legislative care urmează a fi întreprinse. Mai mult, în partea ce ține de *elaborarea sub egida Consiliului creat sau existent* nu este clar dacă respectiva entitate la care se face referire există sau nu.

În contextul celor enunțate, obiectivul 15 precum și acțiunile incluse urmează a fi revizuite și în același timp exclus Ministerul Justiției în calitate de executor principal.

19.La obiectivul 19:

la acțiunea 1) în partea ce ține de prevenirea dezinformării și răspândirii știrilor false și/sau a informațiilor manipulatorii prin platformele media, atragem atenția că prin *Legea nr.257 din 22 decembrie 2017 cu privire la completarea Codului audiovizualului al Republicii Moldova nr. 260/2006*, a fost definită „securitate informațională" și instituite sancțiuni pentru prejudicierea securității informaționale, care implică măsuri pentru asigurarea protecției persoanelor, a

societății și a statului de eventuale tentative de dezinformare și/sau de informare manipulatoare din exterior și pentru neadmiterea provocărilor cu caracter mediatic îndreptate împotriva Republicii Moldova;

la acțiunea 4) privind armonizarea legislației naționale cu standardele și practicile CoE și UE în domeniul drepturilor omului, în vederea protecției demnității umane contra fenomenului de defăimare prin intermediul platformei on-line și domeniul audiovizualului, comunicăm despre inițiativa legislativă a Guvernului de modernizare a Codului civil, adoptată de Parlament prin Legea nr. 133 din 19 iulie 2018, prin care s-a propus introducerea unei noi secțiuni dedicată respectului datorat ființei umane și drepturilor ei inerente.

Potrivit art. 31^3 în redacția *Legii nr. 133 din 19 iulie 2018 privind modernizarea Codului civil și modificarea și completarea unor acte legislative* „[..] orice persoană fizică are dreptul la viață, la sănătate, la integritate fizică și psihică, la libera exprimare, la nume, la onorare, demnitate și reputație profesională, la propria imagine, la respectarea vieții intime, familiale și private, la protecția datelor cu caracter personal, la respectarea memoriei și corpului său după deces, precum și alte asemenea drepturi recunoscute de lege. Aceste drepturi sunt insesizabile și inalienabile.".

La fel, în art. 16 din *Codul audiovizualului* sunt reglementate drepturile persoanelor lezate la replică, rectificare și la remedii echivalente, iar în art. 41 al codului este instituită obligația Consiliului Coordonator al Audiovizualului de a asigura protecția demnității umane, respectarea drepturilor omului, inclusiv a principiului egalității între femei și bărbați, și protecția minorilor.

Normele citate poartă un caracter general aplicabil tuturor situațiilor, indiferent de metodele utilizate pentru defăimarea persoanelor. Astfel, doar precizarea *prin intermediul platformei on-line și domeniul audiovizualului* nu justifică intervențiile de ordin legislativ, iar o enumerare exhaustivă a metodelor utilizate ar pune în pericol aplicabilitatea normei în situațiile neprevăzute de lege în condițiile în care societatea și tehnologia este în continuă evoluție.

20. În scopul uniformizării terminologiei, se vor revizui instituțiile partenere de realizarea acțiunilor: *mass-media*, *organizații mass-media* și *societatea civilă, organizațiile societății civile*. Totodată, pentru claritatea și asigurarea realizării acțiunilor indicate, se va concretiza referința la *mediul privat.*

Secretar de stat **Nicolae EȘANU**

Ex. D. Lupașcu, m. 248[1]
Tel. 022-20-14-67/ e-mail: diana.lupascu@justice.gov.md

Sinteza
obiecțiilor și propunerilor la proiectul de lege pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia

Participantul la avizare(expertizare) /consultare publică	Conținutul obiecției/propunerii (recomandării)	Argumentele autorului proiectului
Consiliul Coordonator al Audiovizualului al Republicii Moldova *(Aviz nr.535 din 18 iulie 2018)*	Fără obiecții și propuneri.	**Se acceptă.**
Agenția Servicii Publice a Republicii Moldova *(Aviz nr.01/4546 din 30.07.2018)*	Fără obiecții și propuneri.	**Se acceptă.**
Agenția de Stat Pentru Proprietatea Intelectuală a RM *(Aviz nr.1761 din 12.09.2018)*	Fără obiecții și propuneri.	**Se acceptă.**
Comisia Electorală Centrală *(Aviz nr .CEC 8/2662 din 12.09.2018)*	Fără obiecții și propuneri.	**Se acceptă.**
Academia de Științe a Moldovei *(Aviz nr.493-01/5 din 09.08.2018)*	*1.* În cadrul notei informative la proiectul Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 și Planul de acțiuni pentru implementarea acesteia se menționează că „*Capitolul I – Introducere* descrie evoluția curentă a tehnologiilor informaționale ..., precum și evidențiază principalele vulnerabilități, riscuri și amenințări la adresa societății informaționale și a mediul național și general de securitate". De regulă, descrierea problemei în evoluție sau contextul care determină necesitatea elaborării unei strategii trebuie să se regăsească în cadrul compartimentului „Descrierea situației" (A se vedea: Ghid metodologic cu privire la procesul decizional, www.rapc.gov.md/file/Ghid%20procesul%20decizional_revi), iar în conținutul „Introducerii" se indică deciziile care au dus la elaborarea strategiei, de exemplu conexiunea cu Concepția securității informaționale, perioada	**1. Nu se acceptă.** Cadru legal care stabilește condițiile care urmează a fi respectate la elaborarea unei note informative este Legea nr. 100 din 22.12.2017 cu privire la actele normative. Ghidul metodologic cu privire la procesul decizional nu are caracter de act normativ.

	propusă de implementare, părțile implicate în elaborarea strategiei. În mare parte, aceasta va contribui la asigurarea unui conținut succint și explicit al introducerii (volum: 1 - 1,5 pag.).	
	2. În același timp, ținem să remarcăm că deși se menționează că sunt evidențiate „principalele vulnerabilități, riscuri și amenințări la adresa societății informaționale și a mediul național și general de securitate", totuși în proiectul Strategie nu se regăsește o clasificare a acestora din perspectiva securității informaționale sau au un caracter haotic.	**2. Nu se acceptă.** La Capitulul III *„Definirea problemelor"* riscurile și amenințări la adresa societății informaționale au fost divizate în cinci compartimente distincte 1)componenta cibernetică și investigarea criminalității informatice; 2)componenta de securitate a spațiului mediatic; 3)componenta contrainformativă și de securitate; 4)problemele de natură legală; 5)problemele de conștientizare a maselor.
	3. Reieșind din faptul că proiectul Strategiei respective se referă la una din dimensiunile securității – securitatea informațională –, este bine venit ca în cadrul compartimentului „Descrierea situației" contextul care determină necesitatea și importanța elaborării și adoptării unei astfel de strategii de structurat la nivel național, regional și internațional. Aceasta ar permite de accentuat situația privind asigurarea securității informaționale la nivel național, fundamentând necesitatea compartimentării acțiunilor prin prisma celor patru piloni menționați în introducerea Strategiei (punctul 15). În același timp, aceasta ar asigura evitarea generalizărilor sau constatărilor și focusarea pe argumente în baza unor analize sau cercetări. De exemplu, la pagina 8, punctul 31 se menționează că „Analiza evoluției fenomenului social-media și presei electronice reliefează reglementarea insuficientă a componentei de protecție a spațiului mediatic de la amenințări cu caracter hibrid și a componentei de securitate. ..." Aici apare întrebarea „Conform cărei analize?". Dacă este vorba de o analiză efectuată, atunci rezultatul problemelor identificate trebuie să se regăsească în cadrul compartimentului „Descrierea problemelor". În același timp, sensul propoziției/constatării trebuie revăzut, căci nu este clar despre ce „componentă de securitate" este vorba.	**3. Nu se acceptă.** Capitulul II *„Descrierea situației"* conține o descriere detaliată a parcursului Republicii Moldova în partea dezvoltării societății informaționale, actelor naționale și internaționale adoptate până în prezent care reglementează totalitatea raporturilor juridice apărute între subiecții, obiectul și interacțiunea spațiului informațional. Analiza nivelului de protecție a spațiului informațional a fost efectuată la nivelul grupului de lucru interdepartamental , statuîndu-se că spațiul informațional evoluează și modernizează într-o dinamică accelerată, din această perspectivă au fost descrise și accentuate direcțiile ce urmează a fi armonizate și dezvoltate.
	4. Referindu-ne la capitolul III „Definirea problemei", constatăm lipsa unui	**4. Nu se acceptă.** În cadrul

	fundament metodologic de identificare a problemelor, de exemplu efectuarea unei analize calitative şi cantitative cu referire strică la Republica Moldova. Cadrul național privind elaborarea de politici evidențiază că analiza problemei este importantă de a înțelege cauzele, efectele, amploarea, categoriile afectate şi cum ar putea evolua problema în timp.	elaborării Strategiei securității informaționale, Grupul de lucru interdepartamental, format din experți din diverse domenii, au expus o descriere reală şi practică a problemelor din Republica Moldova ce cuprind spațiul informațional. Or, definirea, trasarea, identificarea şi prezentarea problemelor nu se face prin prisma unui ghid/fundament metodologic ci prin prisma realității existente, analizei situației de fapt şi problemelor practice.
Ministerul Finanțelor *(Aviz nr.32/146 din 06.08.2018)*	**1.** Nerespectarea prevederilor art.30 din Legea nr.100 din 22 decembrie 2017 privind actele normative, conform cărora la proiectul de act prezentat spre examinare şi avizare, se întocmeşte o notă informativă care urmează să includă fundamentare economic-financiară, face dificilă expunerea privind impactul financiar asupra bugetului de stat. Prin urmare considerăm necesar, completarea notei informative.	**1. Se acceptă.** A fost completată cu un compartiment nou.
	2. Proiectul Hotărârii Guvernului se propune de completat cu un punct nou în redacția următoare: „Finanțarea acțiunilor prevăzute în Planul de acțiuni privind implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 se va efectua din contul şi în limita mijloacelor aprobate în bugetele instituțiilor responsabile de implementare"	**2. Se acceptă.**
	3. La proiectul Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023 menționăm că obiectivele Strategiei trebuie astfel formulate ca acestea să fie simple, măsurabile, accesibile, realiste şi încadrate în timp.	**3. Se acceptă parțial.** Deşi propunerea este prea generală şi nu a fost argumentată, unele obiective au fost revăzute şi reformulate.
	4. Proiectul urmează a fi adus în concordanță cu prevederile stipulate în pct.9 lit. e) Hotărârea Guvernului nr.33 din 11 ianuarie 2007 cu privire la regulile de elaborare şi cerințele unificate față de documentele de politici în special atragem atenția că Strategia trebuie să includă evaluarea impactului financiar.	**4. Se acceptă.** A fost completat conform redacției stabilite în cadrul discuțiilor din data de 21.09.2018 cu reprezentanții Ministerului Finanțelor. A fost unanim convenita următoarea redacție „ Costurile estimative ale acțiunilor vor fi ajustate pe perioada

		implementării Planului, ţinînd cont de volumele alocaţiilor disponibile în bugetul de stat.
	5. Pct.109 şi pct.110 urmează a fi excluse şi substituite cu un punct nou în următoarea redacţie „Finanţarea Strategiei se va realiza din bugetul de stat (resurse generale, venituri colectate şi resurse ale proiectelor finanţate din surse externe) şi din alte surse conform legislaţiei".	**5. Se acceptă.**
	6. Potrivit Planului, realizarea unor obiective/acţiuni urmează a fi asigurată din contul surselor financiare externe. Totodată, nu este clar dacă sunt sau nu deja încheiate angajamente financiare externe pentru implementarea obiectivelor/acţiunilor propuse. Astfel conform prevederilor pct.6, subpct 6) din anexa nr.1 la HG nr.696 din 30 august 2017 „Cu privire la organizarea şi funcţionarea Ministerului Finanţelor" ministerul este responsabil de coordonarea asistenţei financiare externe, respectiv orice decizie care poate avea impact financiar asupra bugetului public naţional, urmează a fi consultată preliminar cu Ministerul Finanţelor.	**6. Se acceptă.** În contextul solicitării asistenţei financiare de la partenerii externi, în prealabil va fi coordonat cu Ministerul Finanţelor.
Cancelaria de Stat *(Aviz nr.21-06-6442 din 06.08.2018)*	*1. La proiectul hotărîrii de Guvern:* Intrucît, conform prevederilor art.24 din Legea 100/2017 cu privire la actele normative, documentele de politici nu sînt acte normative, considerăm oportună aprobarea Strategiei sus-menţionate şi a Planului de acţiuni prin hotărîre de Parlament, dar nu prin lege.	**1. Se acceptă.**
	2. La proiectul de lege: La art.2 considerăm judicios de a exclude responsabilitatea Cancelariei de Stat de a prezenta rapoarte privind implementarea Strategiei şi Planului de acţiuni, precum şi de a transfera obligaţia respectivă Serviciului de Informaţii şi Securitate. Menţionăm că, în conformitate cu prevederile pct. 30 al Concepţiei securităţii informaţionale a Republicii Moldova, aprobată prin Legea nr.299/2017, Serviciul de Informaţii şi Securitate, în limita competenţelor, exercită atribuţiile autorităţii naţionale de coordonare a activităţii autorităţilor publice desfăşurate în domeniul securităţii informaţionale. Mai mult decît atît, în pct.28 al Concepţiei menţionate, care listează autorităţile statului cu atribuţii de asigurare a securităţii informaţionale, Cancelaria de Stat nu este menţionată.	**2. Nu se acceptă.** Serviciul de Informaţii şi Securitate al Republicii Moldova este organul de coordonare a activităţilor operaţionale ale autorităţilor publice în domeniul securităţii informaţionale, iar autoritatea responsabilă de elaborarea şi coordonarea politicii statului în domeniul respectiv este Guvernul Republicii Moldova. Cancelaria de Stat este autoritatea publică care asigură organizarea activităţii Guvernului în vederea elaborării şi implementării politicilor publice de către autorităţile

		guvernamentale. Iar, autoritatea responsabilă de elaborare şi prezentare a Strategiei, conform art. 3 al Legii nr. 299 din 21.12.2017, privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova, este *Guvernul care, în termen de 6 luni de la data intrării în vigoare a prezentei legi, va elabora şi va prezenta spre examinare Strategia securităţii informaţionale a Republicii Moldova şi Planul de acţiuni pentru implementarea acesteia.*
	3. La proiectul Strategiei: Se propune extinderea termenului de implementare a Strategiei în 2019-2024, pentru a evita situaţia în care, la momentul adoptării Strategiei, primul an de implementare să fi expirat deja.	**3. Se acceptă.**
	4. Capitolul II „Descrierea situaţiei" necesită a fi revizuit după cum urmează a) la pct.23 se va specifica tipul de „politici interne" ce urmează a fi adoptate de către operatorul de date cu caracter personal. Menţionăm că domeniul protecţiei datelor cu caracter personal este reglementat corespunzător de către legislaţia în vigoare şi că este în proces de implementare Strategia naţională în domeniul protecţiei datelor cu caracter personal pentru anii 2013-2018 şi Planul de acţiuni pentru implementarea acesteia.	**4. Nu se acceptă.** Operatorul de date cu caracter personal va activa după propriile politici interne de protecţie şi securitate. Totodată, nu pot fi impuse careva acte normative interne operatorului de date. Acesta îşi realizează activitatea după o politică confidenţială proprie, adoptată şi ajustată rigorilor individuale.
	5. La pct.26, pe lângă enumerarea documentelor de politici valabile până în anul 2020, tangenţiale dimensiunii securităţii informaţionale, urmează a fi inclusă o prezentare succintă a realizărilor de bază obţinute prin implementarea documentelor respective, identificate problemele care împiedică implementarea corespunzătoare a acestora, precum şi descrisă modalitatea prin care prezenta Strategie va dezvolta în continuare realizările obţinute, pentru a asigura atingerea obiectivelor stabilite. La fel,	**5. Nu se acceptă.** Realizările obținute prin implementarea documentelor de politici la care s-a făcut trimitere în Strategie, au fost incluse în Rapoartele anuale la documentele respective, publicate de către ministerele de resort.

	este necesară includerea informaţiei privind mecanismele ce vor fi utilizate pentru neadmiterea dublărilor de obiective şi acţiuni ale prezentului document de politici cu documentele aflate deja în proces de implementare. Sintagma „Strategia propune reglementarea şi abordarea unor segmente ale securităţii informaţionale neelucidate anterior" de la pct.28 al proiectului nu clarifică suficient felul în care autorul va evita potenţialele dublări de activităţi şi resurse pentru realizarea acestora.	Strategia securității informaționale propune acțiuni adaptate situației actuale. Potrivit Strategiei, sectorul securității informaționale cuprinde și integrează un sector tridimensional (cibernetic, mediatic și operațional) având scopul coroborării acțiunilor prezentate spre realizare. Conform analizei efectuate anterior elaborării Strategiei, în baza Raporturilor de evaluare a documentelor de politici, s-au reliefat principalele acțiuni căzute în desuetudine, fiind integrate în Strategie conform obiectului de reglementare, necesității promovării și expunerii conform situației actuale. Suplimentar, decizia de preluare a unor acțiuni din unele documentele de politici și adaptate Strategiei securității informaționale aparține Grupului de lucru de nivel interinstituțional, creat în baza scrisorii Cancelariei de Stat.
	6. La pct.31 urmează a fi incluse date adiţionale, care să confirme constatarea autorului privind „reglementarea insuficientă a componentei de protecţie a spaţiului mediatic".	**6. Nu se acceptă.** Capitolul II „Descrierea situației" este urmat de Capitolul III „Definirea Problemelor" care conține componenta de securitate a spațiului mediatic și descrierea problemelor de natură legală care statuează lipsa unui cadru juridic care să reglementeze raporturile dintre subiecții mass-media din Internet. Totodată, au fost reflectate noul tip de amenințări – hibride, care sunt în proces de studiere și evaluare. La

		moment, legislația (cu excepția Concepției securității informaționale) nu prevede noțiunea de amenințări hibride, un mecanism de prevenire sau combatere.
	7. La capitolul IV: Pentru evitarea dublării neargumentate a acţiunilor de realizare a obiectivelor specifice, acestea vor fi prevăzute doar în Planul de acţiuni;	**7. Nu se acceptă.** Conform Hotîrîrii Guvernului nr.33 din 11.01.2007 *„Cu privire la regulile de elaborare şi cerinţele unificate faţă de documentele de politici"*, Strategia trebuie să prevadă şi reglementeze atît obiectivele generale cît şi cele specifice pentru înțelegerea obiectului de reglementare.
	8. Obiectivele specifice ale fiecărui Pilon urmează a fi formulate după principiul SMART - pentru a fi specifice, măsurabile, accesibile, realiste şi determinate în timp. Mai mult decît atît, pentru fiecare obiectiv specific urmează a fi identificaţi indicatorii care vor permite evaluarea nivelului de atingere a obiectivului respectiv. Cu titlu de exemplu, menţionăm că gradul de realizare a obiectivului nr.2 al Pilonului I, „Monitorizarea permanentă şi evaluarea periodică a nivelului securităţii spaţiului cibernetic" în formularea actuală nu va putea fi evaluat	**8. Nu se acceptă.** Formularea obiectivelor specifice după principiul SMART nu este o condiție obligatoriu care urmează a fi respectată de un document de politici. Iar evaluarea nivelului de atingere a rezultatului scontat la fiecare obiectiv separat va fi efectuat reieșind din indicatorii de progres.
	9. Obiectivul nr.7 al Pilonului I urmează a fi reformulat pentru a exclude caracterul declarativ al acestuia;	**9. Nu se acceptă.** Nu este clar în ce constă caracterul declarativ al obiectivului. Totodată denumirea acestuia a fost propusă de autoritatea competentă la nivel național de realizarea lui.
	10. Propunem înlocuirea tabelelor cu acţiuni din fiecare Pilon cu un tabel cu indicatori de impact care ar permite evaluarea rezultatelor obţinute în cadrul fiecărui pilon;	**10.Nu se acceptă.** Tabelele cu acțiuni plasate după fiecare Pilon conțin și indicatori de rezultat/progres, ceea ce va permite o evaluare și monitorizare a rezultatelor obținute.
	11. Obiectivul nr.3 al Pilonului III repetă Obiectivul nr.3 al Pilonului I, de aceea propunem comasarea lor.	**11.Nu se acceptă.** Obiectivul 3 din Pilonul I prevede - Consolidarea

		capacităților de apărare cibernetică ca parte a Pilonului I „Asigurarea securității spațiului informațional-cibernetic și investigarea criminalității informatice iar Obiectivul III al Pilonului III prevede – Dezvoltarea competențelor operaționale de apărare cibernetică ca parte a Pilonului „Consolidarea capacităților operaționale. Astfel, comasarea acestora nu poate fi efectuată reieșind din faptul că rezultatul scontat la fiecare obiectiv diferă conceptual.
	12. La capitolul V este oportună estimarea costurilor implementării Strategiei. Menţionăm că estimarea necesarului de resurse pentru implementarea unui document de politici este o condiţie obligatorie pentru aprobarea acestuia, care, în acelaşi timp, va contribui la implementarea lui eficientă.	**7. Se acceptă.** A fost completat conform redacției stabilite în cadrul discuțiilor din data de 21.09.2018 cu reprezentanții Ministerului Finanțelor. A fost unanim convenita următoarea redacție „ Costurile estimative ale acţiunilor vor fi ajustate pe perioada implementării Planului, ţinînd cont de volumele alocaţiilor disponibile în bugetul de stat".
	13. La capitolul VI urmează a fi incluşi indicatorii de progres care lipsesc. Indicatorii respectivi vor permite monitorizarea eficientă, precum şi estimarea gradului de implementare a Strategiei.	**12.Nu se acceptă.** Indicatorii de rezultat/progres au fost indicați după fiecare Pilon în formă tabelară. Suplimentar, Planul de acțiuni al Strategiei prevede un compartiment separat cu indicatorii de progres
	14. In cadrul capitolului VII se impune includerea informaţiei privind procedura de evaluare a implementării Strategiei.	**13.Nu se acceptă.** Lipsa termenului de „Evaluare" în capitolul VII nu presupune lipsa procesului propriu zis. Or, conform art. 113 procesul de implementare a Strategiei va fi

		realizat prin monitorizarea acțiunilor, evaluarea rezultatelor și în caz de necesitate vor fi operate modificările necesare.
	15. La proiectul Planului de acțiuni: Pentru fiecare acțiune planificată vor fi indicate termenul de realizare și costul estimativ de implementare.	**14. Se acceptă parțial.** Termenul de realizare a acțiunilor a fost indicat. Cu referire la costul estimative, a fost completat conform redacției stabilite în cadrul discuțiilor din data de 21.09.2018 cu reprezentanții Ministerului Finanțelor. A fost unanim convenita următoarea redacție „ Costurile estimative ale acțiunilor vor fi ajustate pe perioada implementării Planului, ținînd cont de volumele alocațiilor disponibile în bugetul de stat.
	16. Totodată, propunem examinarea suplimentară a acțiunilor planificate în raport cu acțiunile incluse în Planul de acțiuni pentru implementarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, în vederea excluderii dublărilor sau neconcordanțelor dintre acestea. Spre exemplu, Acțiunea 1 a Obiectivului 1, în conformitate cu pct.3.1. al Programului, urma a fi realizată încă în anul 2016. Situație similară este și în cazul acțiunilor 4 și 6 ale acestui obiectiv, care urmau a fi realizate în anul 2017	**15.Nu se acceptă.** Strategia securității informaționale propune acțiuni adaptate situației actuale. Potrivit Strategiei, sectorul securității informaționale cuprinde și integrează un sector tridimensional (cibernetic, mediatic și operațional) având scopul coroborării acțiunilor prezentate spre realizare. Conform analizei efectuate anterior elaborării Strategiei, în baza Raporturilor de evaluare a documentelor de politici, s-au reliefat principalele acțiuni căzute în desuetudine, fiind integrate în Strategie conform obiectului de reglementare, necesității promovării și expunerii conform situației actuale. Suplimentar, decizia de preluare a unor acțiuni din unele documentele

		de politici şi adaptate Strategiei securităţii informaţionale aparţine Grupului de lucru la nivel interinstituţional, creat în baza scrisorii Cancelariei de Stat.
	17. La obiectivul nr. 1, acţiunea nr. 1 - *„crearea/desemnarea entităţii care va exercita rolul de Centru naţional de reacţie...",* la obiectivul nr. 10 acţiunea nr. 2 - *„crearea/ consolidarea laboratoarelor de securitate cibernetică...",* la obiectivul nr. 11 acţiunea nr. 5 - *„certificarea specialiştilor în domeniul securităţii cibernetice ...",* la obiectivul nr. 14 acţiunea nr. 1 — *„evaluarea spaţiului Internet...",* la obiectivul nr. 16 acţiunea nr. 1 - *„crearea la nivel naţional a entităţii...",* se propune excluderea din rubrica „instituţiile responsabile" a I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" şi includerea acesteia în rubrica „parteneri".	**16.Nu se acceptă.** Solicitarea privind desemnarea STISC ca instituţie responsabilă de realizarea acţiunii, a parvenit nemijlocit de la STISC. Totodată, reieşind din Statutul Instituţiei publice „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică", aprobat prin Hotărârea Guvernului nr. 414 din 08.05.2018, STISC este instituţia publică care are drept scop administrarea, menţinerea şi dezvoltarea infrastructurii de tehnologie a informaţiei, Sistemului de telecomunicaţii al autorităţilor administraţiei publice, ca parte a reţelei de comunicaţii speciale şi a sistemelor informaţionale de stat, gestionarea infrastructurii unice a cheii publice a Guvernului, precum şi implementarea politicii statului în domeniul securităţii cibernetice.
	18. La obiectivul nr. 2, acţiunea nr. 1 urmează a fi reformulată în corespundere cu acţiunile descrise la obiectivul nr. 2 „Monitorizarea permanentă şi evaluarea periodică a nivelului securităţii spaţiului cibernetic" al Pilonului I al Strategiei.	**17. Se acceptă.** A fost modificat
	19. Acţiunea 1 a obiectivul nr. 6, precum şi acţiunile 1,2 şi 3 ale obiectivului 7 din cadrul Pilonului urmează a fi revizuite, deoarece sînt formulate drept obiective.	**18.Nu se acceptă.** Acţiunea nr. 1 a obiectivului nr. 6 presupune eficientizarea procesului de combatere a criminalităţii informatice prin specializarea şi instruirea personalului calificat şi identificarea noilor metode şi tactici în instruirea personalului.

		Acţiunile nr. 1,2 şi 3 ale obiectivului nr. 7 presupun efectuarea unor măsuri speciale, or, legislaţia pertinentă stabileşte că noţiunea de „combatere" presupune în sine acţiuni şi măsuri (Ex. Legea nr. 50 din 22.03.2012 privind prevenirea şi combaterea criminalităţii organizate, Legea nr. 320 din 27.12.2012 cu privire la activitatea Poliţiei şi statutul poliţistului). Autorii acţiunilor (MAI şi PG) insistă asupra menţinerii redacţiei actuale, care este conformă totalmente cadrului legal.
	20. La obiectivul nr. 11 acţiunea nr. 6 - „*crearea platformelor web de sensibilizare şi informare privind pericolele în spaţiul cibernetic şi măsurile de protecţie ce pot fi luate de către persoanele fizice şi juridice*", se propune la rubrica „termen de realizare" substituirea sintagmei „2019-2020" cu sintagma „2019-2021", având în vedere că realizarea acţiunii ţine inclusiv de Cert-ul naţional, crearea căruia este stabilită pentru perioada 2018-2020.	**19.Se acceptă.**
	21. Acţiunea 3 a obiectivului 12, cu excepţia literei c), repetă acţiunile 2 şi 3 de la obiectivul 9 al Pilonului I şi, prin urmare, urmează a fi revizuită.	**20.Se acceptă parţial.** A fost revizuit.
	22. La obiectivul nr. 14 acţiunea nr. 1, se propune completarea rubricii „instituţiile responsabile" cu Ministerul Afacerilor Interne. Totodată, oportunitatea acţiunii 1 a obiectivului 16 al Pilonului III necesită a fi argumentată suplimentar, în textul Strategiei fiind prezentată informaţia privind potenţialul statut, precum şi sarcinile şi atribuţiile de bază ce urmează a fi atribuite entităţii care urmează a fi create. în acelaşi timp, propunem excluderea acţiunii 3 a aceluiaşi obiectiv, dat fiind faptul că un complex de măsuri de informare a publicului sînt deja menţionate la acţiunile 6 şi 7 ale Obiectivului 11 al Pilonului I.	**21.Se acceptă parţial.** La obiectivul nr. 14 acţiunea nr. 1, la rubrica „instituţii responsabile" a fost inclus Ministerul Afacerilor Interne. Cu referire la statutul, sarcinile şi atribuţiile de bază ce urmează a fi atribuite entităţii, acestea vor fi indicate în actul de constituire sau actul de reglementare a activităţii. Totodată, a fost inclus un punct separat la capitolul VI „Rezultatele scontate şi Indicatorii de progres" cu referire la Consiliul Coordonator pentru asigurarea securităţii

		informaționale. Cât ține de propunerea privind excluderea acțiunii 3 de la obiectivul 16, pe motiv că un complex de măsuri de informare a publicului sunt deja menționate la acțiunile 6 și 7 ale Obiectivului 11 al pilonului I, nu se acceptă din considerentul că acțiunea 3 obiectivul 16 presupune crearea unei platformei la nivel național specializată pe amenințările hibride, iar acțiunile 6 și 7 de la obiectivul 11 presupune crearea resursei informaționale pe segmentul cibernetic. Scopul acțiunilor este distinct.
	23. La acţiunea 2 a obiectivului 21 al Pilonului III se impune a fi revizuită lista responsabililor de implementare prin excluderea SIS în calitate de responsabil şi includerea tuturor instituţiilor ce urmează a remite rapoarte în adresa SIS despre starea de risc de la instituţiile statului cu competenţă în domeniul securităţii informaţionale.	**22.Se acceptă.**
	24. La obiectivul nr. 25 acţiunea nr. 1 şi acţiunea nr. 2 este oportună substituirea sintagmei „CTS" cu sintagma „STISC", avînd în vederea reorganizarea I.S. „Centrul de telecomunicaţii speciale".	**23.Se acceptă.** Textul a fost modificat
Ministerul Apărării (*Aviz nr.11/950 din 17.07.2018*)	Fără obiecţii şi propuneri.	**Se acceptă.**

Centrul Național pentru Protecția Datelor cu Caracter Personal *(Aviz nr.04-06/1690 din 31.07.2018)*	**1.** Includerea CNPDCP în calitate de autoritate partener la următoarele acțiuni din Planul de acțiuni pentru implementarea Strategiei. Obiectivul 1, acțiunea 2) *„Crearea unui sistem integrat de comunicare și evaluare a amenințărilor la adresa securității informaționale și de elaborare a măsurilor operative de răspuns”.* Obiectivul 2, acțiunea 3) *„Monitorizarea permanentă și evaluarea periodică a nivelului securității spațiului cibernetic”.* Obiectivul 3, acțiunile 2) și 3) *„Consolidarea capacităților de apărare cibernetică”.* Obiectivul 9, acțiunile 2) 3) și 4) „Dezvoltarea capacităților instituționale în combaterea criminalității informatice”. Obiectivul 11, acțiunile 2), 3) și 4) „Dezvoltarea capacităților de reziliență cibernetică și ridicarea nivelului de cultură în domeniul TIC” Obiectivul 22 acțiunile 3) și 4) „Dezvoltarea sistemului de pregătire a resurselor umane în domeniul securității informaționale”.	**1. Se acceptă.**
	2. Includerea în calitate de autorități partenere la acțiunea 5) obiectivul 4 „Protecția rețelelor de comunicații speciale ale Republicii Moldova și a informației cu accesibilitate limitată, pentru menținerea funcțiilor vitale ale statului” – MAI, SIS, PG, STISC.	**2. Se acceptă.**
Compania „Teleradio-Moldova” *(Aviz nr. 01-10/493 din 12.07.2018)*	Fără obiecții și propuneri.	**Se acceptă.**
Ministerul Afacerilor Interne al Republicii Moldova *(Aviz nr. 38/165 din 18.07.2018)*	Fără obiecții și propuneri.	**Se acceptă.**
Ministerul Sănătății, Muncii și Protecției Sociale al Republicii Moldova *(Aviz nr. DI/3/041-7124 din 20 iunie 2018)*	**1.** La capitolul VII. Proceduri de monitorizare și Evaluare al Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023, deși în titlul capitolului este menționat cuvântul „Evaluare” în text nu este specificat ce presupune și cum va avea loc acest proces. Prin urmare, se propune completarea acestui capitol în ceea ce privește procesul de evaluare a Strategiei.	**1. Nu se acceptă.** Lipsa termenului de „Evaluare” în capitolul VII nu presupune lipsa procesului propriu zis. Or, conform art. 114 procesul de implementare a Strategiei va fi realizat prin monitorizarea acțiunilor, evaluarea rezultatelor și în caz de necesitate vor fi operate modificările necesare.

	2. Cu privire la Planul de acțiuni unde este specificat ca partener Ministerul Sănătății, Muncii și Protecției Sociale, la abrevierea autorității a fost omisă ultima literă "S", respective se solicit completarea, conform Listei de abrevieri expuse la proiectul Strategiei.	**2. Se acceptă.**
	3. Pilonul I, subpunctul 4) perfecționarea cadrului legal ce reglementează salarizarea efectivului specializat în combaterea criminalității informatice și investigarea infracțiunilor informatice, ca responsabili sunt menționați Ministerul Finanțelor și Ministerul Afacerilor Interne, iar ca parteneri, la fel este menționat MF și MSMPS. Luînd în calcul că, după reforma administrației publice centrale, politica salarială în sectorul bugetar a fost preluată de Ministerul Finanțelor (HG nr.696 din 30.08.2017) această autoritate trebuie să fie responsabilă de acțiunea respectivă, iar la parteneri trebuie exclus MSMPS și de inclus MAI.	**3. Se acceptă.**
Procuratura Generală *(Aviz nr.28-2d/18-251 din 23.07.2018)*	**1.** La pct.111 din proiect, după cuvintele „Organizațiile internaționale" considerăm oportun de a complete cu sintagma „și regionale".	**1. Se acceptă.**
	2. La pct.112, subpct.3) din proiect, propunem substituirea sintagmei „datelor personale cu sintagma „datelor cu caracter personal" în vederea corelării terminologiei utilizate cu prevederile cadrului juridic existent (Legea nr.133 din 08.07.2011 privind protecția datelor cu caracter personal)	**2. Se acceptă.**
	3. Întru respectarea prevederilor art.54 alin. (1) lit. a) din Legea nr.100 din 22.12.2017 cu privire la actele normative, propunem revizuirea proiectului în integritate, din motiv că în textul acestuia sunt greșeli gramaticale (spre exemplu: la pct.92 subpct.1) lit. b) mass media la pct.104 subpct 1) inter-instituționale)	**3. Se acceptă.**
Ministerul Educației, Culturii și Cercetării *(Aviz nr.07-09/9389 din 27,07.2018)*	**1.** Pilonul I, obiectivul 10, acțiunea 1 coloana *Instituții responsabile* după sintagma „AȘM" se va suplimenta sintagmele „Agenția de Dezvoltare și Cercetare " și Serviciul de Informații și Securitate, iar în coloana termen de realizare sintagma 2019-2022 se va substitui cu sintagma 2020-2023.	**1. Se acceptă parțial.** Termenul a fost modificat. Cu referire la includerea SIS ca instituție responsabilă, nu poate fi acceptată pe motiv că acțiunea depășește atribuțiile funcționale stabilite de legea specială.
	2. Pilonul I, obiectivul 10, acțiunea 2 se va expune în următoarea redacție: „Crearea/consolidarea laboratoarelor de securitate cibernetică"	**2. Nu se acceptă.** Întru susținerea propunerii MECC nu a prezentat nici-un argument.
	3. Pilonul I, Obiectivul 11, acțiunea 5 este improprie Ministerului Educației, Culturii și Cercetării.	**3. Se acceptă.**
	4. Pilonul IV, obiectivul 22, acțiunea 1, coloana „Parteneri" se va	**4. Se acceptă parțial.** Totodată,

	complete cu sintagma „MECC" şi respective, din coloana „Instituţii responsabile" se va exclude sintagma „MECC" atît la acţiunea 1 cît şi la acţiunile 3 şi 4, ca fiind improprii.	MECC nu poate fi exclus din coloana instituţii responsabile de la acţiunea 3 a obiectivului 22. MECC potrivit art.140 din Codului Educaţiei, are atribuţie directă la elaborarea politicii de stat în domeniul pregătirii resurselor umane prin instituţiile de învăţământ subordonate Ministerului.
Agenţia de Guvernare Electronică *(Aviz nr.3007-50 din 20.07.2018)*	Acţiunile prevăzute la pct.81 din Strategia securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 *(Obiectivul nr.2 Monitorizarea permanentă şi evaluarea periodic a nivelului securităţii spaţiului cibernetic)* şi anume lit. b) pct.1 şi pct.2 urmează a fi exclude deoarece depăşesc competenţa Agenţiei de Guvernare Electronică, în domeniul auditului de securitate cibernetică. Aceiaşi situaţie se referă la Planul de acţiuni pentru implementarea Strategiei nominalizate şi anume, urmează a fi exclus subpct.1) şi lit.b) din pct.2 *Monitorizarea permanentă şi evaluarea periodic a nivelului securităţii spaţiului cibernetic,* deoarece depăşesc competenţa AGE în domeniul auditului de securitate cibernetică.	**Nu se acceptă.** Potrivit pct.10 subpct.4) din Statutului Instituţiei publice „Agenţia de Guvernare Electronică" conform Anexei nr. 1 la Hotărîrea Guvernului nr. 760 din 18.08.2010 , unul din domeniile de competenţă ale Agenţiei este auditului de securitate cibernetică. Totodată, conform pct. 11 din Statut Agenţia este responsabilă de efectuarea auditului de securitate cibernetică, a infrastructurilor de tehnologie a informaţiei şi a Sistemului de telecomunicaţii al autorităţilor administraţiei publice, precum şi a altor infrastructuri cibernetice de interes naţional, în vederea identificării disfuncţiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora
Banca Naţională a Moldovei *(Aviz nr.31-002/16/2951 din 27.07.2018)*	**1.** În calitate de instituţie responsabilă pentru acţiunea 8.3 „Identificarea mecanismelor comune de combatere a fraudelor card –present şi card not-present din Planul de acţiuni urmează a fi reţinute doar organele abilitate cu atribuţii de urmărire penală care deţin competenţe nemijlocite în cercetarea infracţiunilor". BNM ar putea fi indicată la coloana "Parteneri" a acţiunii 8.3 avînd în vedere că anumite cerinţe, ce ţin de identificarea de către prestatorii de servicii de plată a utilizării frauduloase a cardurilor emise şi/sau acceptate, ţinerea evidenţei, etc. sunt reglementate în actele	**1. Se acceptă.**

	normative ale acesteia. Totodată BNM este abilitată în supravegherea sistemelor de plăți în Republica Moldova și nu este abilitată cu competențe care să contribuie direct la identificarea mecanismelor de combatere a fraudelor.	
	2. Se recomandă uniformizarea noțiunilor cu care se operează în proiect (pct.87.1) din Strategie; pct.8.1)-3) din Planul de acțiuni – instituții bancare "băncile și instituțiile financiare") cu luarea în considerare a prevederilor art. 148 alin. (4) din Legea nr.202/2017.	**2. Se acceptă.**
Serviciul Tehnologia Informației și Securitate Cibernetică *(Aviz nr. 132 din 20.07.2018)*	**1.** La obiectivul nr.1, acțiunea nr.1- *crearea/desemnarea entității care va exercita rolul de Centru național de reacție la incidentele de securitate cibernetică și care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autoritățile publice competente și persoanele fizice și juridice*, se propune excluderea din rubrica „instituțiile responsabile" a I.P „Serviciul Tehnologia Informației și Securitatea Cibernetică" și includerea acesteia în rubrica „Parteneri" precum și completarea rubricii „instituții responsabile" cu Cancelaria de Stat.	**1. Se acceptă parțial.** A fost inclusă Cancelaria de Stat. Cu referire la solicitarea privind desemnarea STISC ca instituție responsabilă de realizarea acțiunii, acesta a parvenit nemijlocit de la STISC. Totodată, reieșind din Statutul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică", aprobat prin Hotărârea Guvernului nr. 414 din 08.05.2018, STISC este instituția publică care are drept scop administrarea, menținerea și dezvoltarea infrastructurii de tehnologie a informației, Sistemului de telecomunicații al autorităților administrației publice, ca parte a rețelei de comunicații speciale și a sistemelor informaționale de stat, gestionarea infrastructurii unice a cheii publice a Guvernului, precum și implementarea politicii statului în domeniul securității cibernetice.
	2. La Obiectivul nr.1, acțiunea nr.2 *desemnarea entității care va exercita rolul de Centru Guvernamental de reacție la incidentele de securitate cibernetică, și care va constitui punctul de raportare al incidentelor de securitate cibernetică al Guvernului, și stabilirea interacțiunii acestuia cu Centrul național de reacție la incidentele de securitate cibernetică* se propune completarea rubricii „instituții responsabile" cu Cancelaria de Stat.	**2. Se acceptă.**

	3. La obiectivul nr.2 acțiunea nr.1 urmează a fi modificată și expusă în corespundere cu acțiunile descrie la obiectivul nr.2 *Monitorizarea permanentă și evaluarea periodică a nivelului securității spațiului cibernetic* al Pilonului I al Strategiei.	**3. Nu se acceptă.** Nu este clară propunerea
	4. La Obiectivul nr. 10, acțiunea nr. 2 *„crearea /consolidarea laboratoarelor de securitate cibernetică din cadrul instituțiilor de învățământ superior și instituțiile de cercetare științifică"* se propune excluderea din rubrică „instituțiile responsabile" a I.P „Serviciul Tehnologia Informației și Securitatea Cibernetică" și includerea acesteia în rubrica „parteneri".	**4. Se acceptă.**
	5. La obiectivul nr.11, acțiunea nr.5 *„certificarea specialiștilor în domeniul securității cibernetice de către organizațiile/companiile specializate reieșind din standardele aplicate și cerințele minime obligatorii de securitate cibernetică aprobate"* se propune excluderea din rubrica „instituțiile responsabile" a I.P „Serviciul Tehnologia Informației și Securitate Cibernetică" și includerea acesteia în rubrica „parteneri".	**5. Se acceptă.**
	6. La obiectivul nr.11, acțiunea nr.6 *„crearea platformelor web de sensibilizare și informare privind pericolele în spațiul cibernetic și măsurile de protecție ce pot fi luate de către persoanele fizice și juridice"* se propune la rubrica „termen de realizare" substituirea sintagmei „2019-2020" cu sintagma „2019-2021", avînd în vedere faptul că realizarea acțiunii ține inclusiv de CERT-ul Național, crearea căruia este stabilită pentru perioada 2018-2020	**6. Se acceptă.**
	7. La obiectivul nr. 14, acțiunea nr.1 *„evaluarea spațiului Internet din perspectiva identificării actorilor implicați în producerea și diseminarea conținutului media on-line și alți intermediari și servicii auxiliare ce au impact pentru securitatea informațională"* se propune excluderea din rubrica „instituțiile responsabile" a I.P „Serviciul Tehnologia Informației și Securitate Cibernetică" și includerea acesteia în rubrica „parteneri", precum și completarea rubricii „instituții responsabile" cu Ministerul Afacerilor Interne	**7. Se acceptă parțial.** STISC nu poate fi exclus din rubrica „instituții responsabile" or potrivit Statutul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică", aprobat prin Hotărârea Guvernului nr. 414 din 08.05.2018, STISC este instituția publică responsabilă de menținerea securității cibernetice a infrastructurii tehnologiei informației și a Sistemului de telecomunicații al autorităților administrației publice conform

		cerinţelor minime obligatorii de securitate cibernetică şi de conlucrarea cu alte instituţii publice întru asigurarea securităţii spaţiului informaţional (cibernetic).
	8. La obiectivul nr.16 acţiunea nr.1 *„ crearea la nivel naţional a entităţii ce va avea competenţe de promovare şi coordonare a politicilor de securitate informaţională într-o societate democratică, în funcţie de dezvoltarea tehnologiei, raporturile juridice şi de altă natură din sectorul societăţii informaţionale la nivel naţional şi internaţional (Consiliul coordonator pentru asigurarea securităţii informaţionale)"* se propune excluderea din rubrica „instituţiile responsabile" a I.P „Serviciul Tehnologia Informaţiei şi Securitatea Cibernetică" şi includerea acesteia în rubrica „parteneri".	**8. Se acceptă.**
	9. La obiectivul nr.25, acţiunea nr.1 şi acţiunea nr.2 este oportună substituirea sintagmei „CTS" cu sintagma „STISC" având în vedere reorganizarea CTS.	**9. Se acceptă.**
Ministerul Economiei şi Infrastructurii *(Aviz nr.08/1-7748 din 23.07.2018)*	**1.** *Cu referinţă la proiectul Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023:* La pct. 4, sintagma „Uniunea Informaţională a Telecomunicaţiilor" de modificat cu sintagma „Uniunea Internaţională a Telecomunicaţiilor", iar sintagma „industriale în domeniul electronic" - cu sintagma „sectoriale în domeniul Tehnologiei Informaţiei".	**1.Se acceptă.**
	2. La pct. 7, de modificat cuvântul „interferenţei" cu cuvântul „interacţiunii"	**2.Se acceptă.**
	3. La pct. 10, de modificat cuvântul „remediere" cu cuvântul „implementare"	**3.Se acceptă.**
	4. La pct. 15, sintagma „spaţiului informaţional-cibernetic" se propune a fi modificată cu sintagma „spaţiului cibernetic", iar sintagma „spaţiului informaţional-mediatic" – cu cuvântul „informaţionale". Denumirea pilonului III se recomandă a fi completată la sfârşit cu cuvintele „în domeniul securităţii informaţionale"	**4.Nu se acceptă.** Denumirea piloanelor a fost stabilită în dependenţă de acţiunile şi măsurile propuse realizării, fiind coroborate după sens.
	5. La pct. 17, cuvântul „pertinente" se recomandă a fi exclus.	**5.Se acceptă.**
	6. În pct. 19 este oportun de utilizat cuvântul „îngrădirea" în locul cuvântului „împiedicarea";	**6.Se acceptă.**
	7. În pct. 21, sintagmele „organizarea protecţiei" şi „protecţia" nu reflectă scopul punctului de asigurare a securităţi informaţionale. Astfel, se	**7.Se acceptă.**

	recomandă revenirea la textul agreat în ultima ședință a grupului de lucru: „asigurarea securității" și „asigurarea securității informaționale"	
	8. Punctul 29 considerăm necesar a fi reformulat sau exclus, întrucât nu Legea 299/2017 constituie punctul de pornire în domeniul menționat în acest punct. Anterior acestei legi au mai fost aprobate o serie de acte normative ce reglementează acest domeniu (Legea 20/2009, HG 857/2013, HG 811/2015, etc.).	**8.Nu se acceptă.** Formularea pct. 29 nu este sub o formă categorică „Legea nr. 299/2017 poate fi considerată un punct de pornire ". Totodată, în pct.26 este făcută trimiterea la HG 857/2013, HG 811/2015, ca fiind principalele documente de politici existente la momentul elaborării prezentei Strategii.
	9. În pct. 35 din textul Strategiei după sintagma „atacurile informatice" de inclus sintagma „acțiunile hibride de destabilizare a ordinii publice a statului";	**9. Nu se acceptă.** Prevederile punctului respectiv se referă la fapte ce pot fi calificate ca infracțiuni, iar sintagma „acțiunile hibride de destabilizare a ordinii publice a statului" nu are bază juridică.
	10. Totodată, luând în considerație că tema amenințărilor hibride a fost mai puțin abordată în documentele de politici, Capitolul II al Strategiei propunem a fi completat cu mai multe informații ce descriu situația din domeniul amenințărilor hibride de destabilizare a ordinii publice și a statului.	**10. Nu se acceptă.** Tema amenințărilor hibride a fost descrisă la Capitolul III – Definirea Problemelor, fiind detaliate riscurile și amenințările pe diverse paliere.
	11. În pct. 36, sintagma „sutelor de miliarde" de expus în redacția „miliardelor", și dacă e posibil de indicat sursa acestei informații;	**11. Se acceptă.**
	12. În pct. 40, sintagma „unei entități" de expus în următoarea redacție „unei viziuni privind crearea unei entități";	**12. Nu se acceptă.** Conform sintagmei propuse de MEI se va denatura esența problemei, în contextul în care Strategia propune crearea unei entități și nu crearea/desemnarea unei viziuni.
	13. În pct. 43 subpunctul 7), sintagma „teritoriul necontrolat efectiv de autoritățile Republicii Moldova" de expus în următoarea redacție „teritoriul Republicii Moldova necontrolat efectiv de autoritățile constituționale"	**13. Se acceptă.**
	14. Punctul 45 poate fi exclus, întrucât problematica dată este expusă deja în pct. 42 subpct. 1).	**14. Se acceptă.**
	15. Punctul 48 din textul Strategiei este necesar de reformulat astfel încât	**15. Se acceptă.**

	să se identifice problematica situației existente. Însăși aprobarea Directivei UE nu constituie o problemă.	
	16. În pct. 51 sintagma „dezvoltării sale" de expus în redacția „dezvoltării sale statale";	**16. Se acceptă.**
	17. În pct. 52 sintagma „crearea unei stări de revoltă socială" de expus în redacția „crearea și exploatarea unei stări de nemulțumire socială"	**17. Se acceptă parțial.**
	18. Punctele 66 și 67 din textul Strategiei se recomandă a fi unificate într-un singur punct și expuse într-o formă depersonalizată, precum este prezentată situația din pct. 63. Totodată, Republica Moldova își are propriile pericole, precum acapararea de teritorii, separatism, subminarea statalității, ș.a., care considerăm că, la moment, încă nu sunt suficient reflectate în documentele de politici, și totuși, acestea vizează tangențial și spațiul informațional;	**18. Se acceptă parțial.** Punctele date vizează toate organizațiile teroriste islamiste, fiind doar evidențiată cea mai periculoasă la momentul actual. Totodată, comasarea punctelor o considerăm inoportună, deoarece pct. 66 evidențiază problemă, iar 67 unul din mecanismele de soluționare a acesteia. Concomitent alte pericole în adresa Republicii Moldova sunt evidențiate în textul Strategiei.
	19. Considerăm oportun completarea Capitolului III cu un punct nou cu referire la protecția datelor cu caracter personal: descrierea problemelor, lipsurilor/deficiențelor, necesitatea cadrului normativ aprobat sau a convenției ratificate.	**19. Nu se acceptă.** A fost suficient descris segmentul protecției datelor cu caracter personal (pct.18, 23, 24,32).
	20. La Cap. IV, denumirile pilonilor este necesar a fi reformulate conform propunerilor expuse în punctul 4 al prezentului aviz.	**20. Nu se acceptă.** Denumirea piloanelor a fost stabilită în dependență de acțiunile și măsurile propuse realizării, fiind coroborate după sens.
	21. Considerăm că, actuala redacție a pct. 81 alin. 4) și, respectiv, a pct. 2 acțiunea 4) din Planul de acțiuni contravine practicii internaționale. Aducem la cunoștință că, în astfel de țări precum Statele Unite ale Americii, Uniunea Europeană, Republica Populară Chineză, Federația Rusă accesul la codul sursă este solicitat pentru astfel de aplicații, precum antivirus și software care conțin elemente de criptare înaltă. În Statele Unite, companiile tehnologice le permit Guvernului să verifice codul sursă în situații limită ca parte a unor contracte din domeniul apărării sau altor activități foarte importante ale Guvernului. Astfel, în pct. 81 alin. 4) din	**21. Se acceptă.**

	Strategie şi, respectiv, a pct. 2 acţiunea 4) din Planul de acţiuni se recomandă de a include în finalul propoziţiei următoarea sintagmă: „pentru autorităţile publice”	
	22. În pct. 85, alin. 3), în finalul acţiunii de adăugat următoarea paranteză: „(atragerea companiilor private şi experţilor independenţi, dezvoltarea laboratoarelor, etc.)”	**22. Se acceptă parţial.**
	23. Acţiunile din pct. 86 de expus în următoarea redacţie: „1) promovarea unui Internet mai sigur pentru copii prin intermediul consilierii on-line şi încurajarea raportării prin proiecte informaţionale specializate; 2) organizarea campaniilor de informare şi instruire a părinţilor în scopul responsabilizării şi creşterii gradului de conştientizare a riscurilor la care se expun copiii pe Internet; 3) combaterea fenomenului de pornografie infantilă în Internet; 4) combaterea fenomenelor de grooming şi hărţuire sexuală a copiilor în Internet.”;	**23. Nu se acceptă.** De realizarea acestui obiectiv sunt responsabili IGP al MAI şi PG. Acţiunile respective au fost stabilite de către autorităţile competente în domeniu, potrivit atribuţiilor sale funcţionale şi în limita prevederilor legale.
	24. Se recomandă pe tot parcursul textului Strategiei şi a Planului de acţiuni, după caz, de substituit abrevierea „CERT” cu „CSIRT”, deoarece CERT (Computer Emergency Response Team) este o marcă comercială înregistrată şi pentru utilizarea acesteia va fi nevoie de o autorizare oficială, iar pentru utilizarea CSIRT (Computer Security Incident Response Team) nu sunt necesare autorizări;	**24. Nu se acceptă.** În cadrul Grupului de lucru, problema dată a fost abordată, fiind acceptată utilizarea noţiunii pe larg utilizată pe plan internaţional. Totodată, MEI nu a prezentat instituţia care certifică şi autorizează utilizarea noţiunii de „CERT”, precum şi autoritatea care a înregistrat după sine această sintagmă.
	25. Pct. 93 subpunctul 2) în finalul acţiunii de suplinit cu sintagma „în conformitate cu recomandările Comisiei Europene şi bunele practici europene”;	**25. Se acceptă.**
	26. În pct. 107 alin 4), sintagma „asigurarea investigării” de expus în următoarea redacţie: „asigurarea prevenirii şi investigării”, iar după alin. 16) de inclus un aliniat cu următorul conţinut: „17) protecţia datelor cu caracter personal precum şi a persoanelor, în special a copiilor, în mediul online”	**26. Se acceptă.**
	27. Pct. 112 în final de suplinit cu un aliniat cu următorul cuprins: „7) vor fi asigurate măsuri de prevenire şi combatere a criminalităţii informatice”	**27. Se acceptă.**

	. Punctele 115 şi 116 propunem a fi expuse în următoarea redacţie: „115. 115. Monitorizarea şi coordonarea procesului de realizare a Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023 şi Planului de acţiuni privind implementarea Strategiei se pune în sarcina Cancelariei de Stat. 116. Ministerele, instituţiile şi alte autorităţi administrative centrale, conform competenţelor atribuite: 1) vor asigura întreprinderea măsurilor necesare în vederea realizării integrale şi în termenele stabilite a acţiunilor incluse în Planul menţionat; 2) vor prezenta anual, până la data de 1 martie, Cancelariei de Stat, rezultatele acţiunilor prevăzute în Plan. 117. Cancelaria de Stat va generaliza informaţia recepţionată şi, până la data de 1 aprilie, va plasa pe pagina-web oficială proprie raportul privind rezultatele implementării Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023."	**28. Se acceptă.**
	29. *Cu referinţă la proiectul Planului de acţiuni pentru implementarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2018-2023, se recomandă următoarele:* La obiectivul 1 acţiunile 1) şi 2), în rubrica „Instituţiile responsabile" de inclus Cancelaria de Stat – ca fiind prima instituţie responsabilă, întrucât este fondatorul Instituţiei publice „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică";	**29. Se acceptă a fost inslus**
	30. La obiectivul 2 acţiunea 1), la instituţiile responsabile de inclus CSIRT-N, deoarece executarea acţiunii poate fi efectuată doar de CSIRT naţional;	**30. Se acceptă.** Doar că va fi inclusă sintagma agreată pe parcursul Strategiei – CERT N.
	31. La obiectivul 2 acţiunea 2), la instituţiile responsabile de substituit „MEI" cu „AGE", deoarece, în conformitate cu HG 760/2010, Agenţia de Guvernare Electronică este responsabilă pentru efectuarea auditului de securitate cibernetică în autorităţile publice şi monitorizarea implementării rezultatelor auditului. La acţiunea 4) din instituţiile partenere de exclus „MEI";	**31. Se acceptă.**
	32. La obiectivul 11 acţiunea 5), din instituţiile responsabile de exclus „MEI" şi de transferat la instituţiile partenere, iar la acţiunea 7) de exclus „MEI" din instituţiile partenere, deoarece Ministerul nu are astfel de atribuţii funcţionale;	**32. Se acceptă.**

	33. La obiectivul 12 acțiunea 3), trebuie specificat care resursă informațională este necesar a fi creată.	**33. Nu se acceptă.** Resursă informațională poate fi o platformă, site, etc. Considerăm oportun de a lăsă acest subiect deschis spre propuneri, inclusive din partea societății civile, mediului privat, ONG. Or, Pilonul II îi vizează nemijlocit.
	34. La obiectivul 18 acțiunea 2), din instituțiile partenere de exclus „MEI", deoarece Ministerul nu are astfel de atribuții funcționale;	**34. Se acceptă.**
	35. La obiectivul 19 acțiunea 3), instituțiile partenere de completat cu: „SIS, MAI, PG", deoarece considerăm că doar aceste instituții pot contribui la astfel de acțiuni;	**35. Nu se acceptă.** În cadrul Consiliului coordonator pentru asigurarea securității informaționale vor participa nemijlocit reprezentanți ai autorităților SIS, MAI, PG
	36. La obiectivul 22 acțiunea 1), în calitate de instituție responsabilă urmează a fi inclus SIS, iar instituții partenere – AAP, MECC, CCA, MEI, MA, MAI, PG, SIS, ONG. La acțiunea 4), instituții responsabile – INJ, MAI (Academia Ștefan cel Mare), PG, MA, iar instituții partenere – MECC, CCA, SIS, AȘM, ONG din domeniul media.	**36. Se acceptă parțial.** Au fost incluse autoritățile/instituțiile după competență.
	37. Totodată, considerăm oportun a completa Planul de acțiuni cu costurile estimative pe fiecare acțiune.	**37. Nu se acceptă.** Nu pot fi determinate costurile necesare, chiar și sub formă estimativă. Or, stabilirea mărimii acestora în cuantum fix va fi denaturată și eronată și nu vor corespunde necesităților de perspectivă. Suplimentar, conform celor convenite în cadrul Grupului de lucru la nivel interinstituțional, cu participarea inclusiv a MEI, a fost decis unanim ca mărimea costurilor se va decide odată cu implementarea, pentru a exclude careva erori bugetare.

Ministerul Afacerilor Externe și Integrării Europene *Aviz (DM/4/363.2/8278 din 19.07.2018)*	Propunerile și obiecțiile au fost înserate de către MAEIE direct în proiectele supuse avizării.	**Se acceptă.** Au fost operate modificările și completările conform Avizului prezentat de MAEIE.
Ministerul Justiției *(Aviz nr.04/9854 din 17.08.2018*	**1.** *La proiectul hotărârii Guvernului*: Sursa publicării actelor normative se va indica după formula „(Monitorul Oficial al Republicii Moldova, anul publicării, numărul Monitorului, numărul articolului)".	**1. Se acceptă.**
	2. *În* temeiul art. 41 din *Legea 136 din 7 iulie 2017 cu privire la Guvern*, precum și a pct. 6 din *Regulamentul privind organizarea și funcționarea Ministerului Justiției*, aprobat prin *Hotărârea Guvernului nr. 698 din 30 august 2017,* care stabilesc exercitarea funcției de reprezentant al Guvernului în Parlament de către Ministerul Justiției, în lista contrasemnatarilor se va include ministrul justiției.	**2. Se acceptă.**
	3. *La proiectul legii:*În scopul asigurări clarității prevederilor actului normativ, art. 1 se va expune conform următoarei redacții: „Art. 1. – Se aprobă: Strategia securității informaționale a Republicii Moldova pentru anii 2018-2023, conform anexei nr. 1; Planul de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2018-2023, conform anexei nr. 2."	**3. Se acceptă.**
	4. *La proiectul Strategiei (anexa nr. 1):*La pct. 16 se vor revedea cuvintele „Anexă la prezenta Strategie", întrucât conform art. 1 din proiectul legii, Planul de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova reprezintă anexa nr. 2 la aceasta.	**4. Se acceptă.**
	5. Pct. 17 este unul inutil, și prin urmare, se va exclude.	**5. Se acceptă.**
	6. Pct. 18 se va completa cu referința la *Legea nr. 122 din 2 iulie 2014 pentru ratificarea Acordului de Asociere între Republica Moldova, pe de o parte, și Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de altă parte.*	**6. Se acceptă.**
	7. La pct. 44 în virtutea caracterului obligatoriu al actelor normative, cuvintele „în vigoare" se vor exclude (obiecție valabilă și pentru restul referințelor la legislația în vigoare din proiect).	**7. Se acceptă.**

	8. La capitolul VII Proceduri de monitorizare şi evaluare se va ţine cont de prevederile pct. 38 din *Regulile de elaborare şi cerinţele unificate faţă de documentele de politici, aprobate prin Hotărârea Guvernului nr. 33 din 11 ianuarie 2007*, potrivit căruia, raportul de monitorizare trebuie să identifice cel puţin următoarele aspecte: remanierile instituţionale care au survenit în urma implementării; modificarea situaţiei grupurilor-ţintă vizate de document, atît pe parcursul implementării, cît şi la finalizarea acesteia; impactul în urma implementării (economic, juridic, social, ecologic etc.); costurile implementării; gradul de respectare de către responsabilii pentru implementare a termenelor, costurilor şi conţinutului acţiunilor din cadrul planului de implementare; motivele neexecutării sau executării parţiale.	**8. Se acceptă.**
	9. La pct. 116, cuvintele „pe pagina-web oficială" se vor substitui cu cuvintele „pe pagina oficială", în conformitate cu *Regulamentul cu privire la paginile oficiale ale autorităţilor administraţiei publice în reţeaua Internet*, aprobat prin *Hotărârea Guvernului nr. 188 din 3 aprilie 2012.*	**9. Se acceptă.**
	10. *La proiectul Planului de acțiuni (anexa nr. 2):*La obiectivul 1 nu este clar stabilită denumirea acțiunii 3), iar sistematizarea datelor statistice la capitolul securității cibernetice, analiza și evaluarea acestora se va expune ca o acțiune aparte sau o subacțiune.	**10.Se acceptă.** A fost stabilită ca subacțiune.
	11. La obiectivul 2 acțiunea 1) litera b) nu este stabilit indicatorul de progres, iar la obiectivul 2, acțiunea 2) necesită precizare indicatorul stabilit (obiecție valabilă și pentru obiectivele/acțiunile 5. 1), 5. 2), 5. 5), 8. 1), 12. 2), etc).	**11.Se acceptă**. Au fost modificați indicatorii
	12. La obiectivul 2 acțiunea 3) cu referire la *Consiliul coordonator pentru asigurarea securității informaționale*, atenționăm că nu poate fi desemnat în calitate de instituție responsabilă de realizarea unor acțiuni o entitate care nu este creată.	**12.Se acceptă**. Acțiunile stabilite inițial Consiliului au fost stabilite în sarcina SIS. Iar acțiunile stabilite inițial CERT-ului au fost stabilite în sarcina STISC.
	13. La obiectivul 3 acțiunile 2) și 3) se vor corela indicatorii de progres, întrucât ambele prevăd elaborarea unor măsuri de protecție.	**13.Se acceptă.**
	14. La obiectivul 4 acțiunea 1) indicatorul de progres nu corespunde acțiunii prevăzute, în acest sens se vor reanaliza obiectivele/acțiunile 4. 6), 9. 3), 10. 1),	**14.Se acceptă.**

	12. 3), 16. 1), 17. 3) şi 17. 6)	
	15. La obiectivul 4 acțiunea 2) se va revedea indicatorul în sensul că acesta trebuie să fie măsurabil (ex. numărul controalelor efectuate). Sub acest aspect se vor reexamina obiectivele/acțiunile 6. 1), 6. 2), 7. 1), 7. 2), 7. 3), precum și altele similare.	**15. Se acceptă.**
	16. La obiectivul 13 acțiunea 1) societatea civilă și organizații mass-media nu sunt subiecți de drept subordonați Guvernului și nu pot fi obligate să preia anumite sarcini. Din acest considerent, acestea vor fi menținute în plan, în calitate de parteneri, în colaborare cu care se va atinge rezultatul scontat (obiecție valabilă și pentru restul cazurilor similare din proiect).	**16. Nu se acceptă.** Acțiunea stabilită la obiectivul 13 vizează direct societatea civilă și organizațiile mass-media, aceștia urmează a fi interesați în realizarea acțiunilor pe motiv că se propun noi mecanisme de participare și conlucrare directă cu autoritățile publice, implicarea și promovarea unor politici de colaborare între autoritățile statului și actorii nominalizați.
	17. La obiectivul 14 acțiunea 2) menționăm că, potrivit pct. 6 din *Hotărârea Guvernului nr.698 din 30 august 2017 cu privire la organizarea și funcționarea Ministerului Justiției*, acesta este responsabil de elaborarea politicilor în domeniul justiției, drepturilor omului, profesiilor și serviciilor juridice, precum și politicile punitive ale statului. Acesta nu este responsabil de elaborarea politicilor în domeniul securității spațiului mediatic. Conform art. 40 alin. (1) lit. d^1) din *Codul audiovizualului nr. 260-XVI din 27 iulie 2006*, Consiliului Coordonator al Audiovizualului monitorizează și supraveghează respectarea de către radiodifuzorii și distribuitorii de servicii a prevederilor prezentului cod privind asigurarea securității. Totodată, având în vedere prevederile art. 1 alin. (1) din *Legea nr. 753-XIV din 23 decembrie 1999 privind Serviciul de Informații și Securitate al Republicii Moldova*, Serviciul de Informații și Securitate este organul de stat specializat în domeniul asigurării securității de stat, inclusiv a securității informaționale. Prin urmare, luând în considerare competențele funcționale, Ministerul Justiției nu poate fi instituția responsabilă de executarea acțiunii respective.	**17. Se acceptă**. A fost modificat
	18. În partea ce ține de atribuirea în competența Ministerului Justiției a unor acțiuni privind elaborarea politicilor ce țin de *asigurarea transparenței financiare în activitatea autorităților publice, asociațiilor obștești și societăților comerciale în contextul asigurării securității informaționale*, stabilite la acțiunea 15, se	**18. Se acceptă.** A fost modificat.

	reiterează poziția enunțată supra. Mai mult, având în vedere faptul că în prezent cadrul legislativ instituie principiul transparenței în gestionarea resurselor financiare publice, nu este clar ce măsuri legislative urmează a fi întreprinse în acest sens. Menționăm că, *Legea finanțelor publice și responsabilității bugetar-fiscale nr. 181 din 25 iulie 2014* stabileşte la art. 12 alin. (2) că, bugetele se elaborează, se aprobă şi se administrează în mod transparent, având la bază: a) procesul bugetar, bazat pe un calendar bugetar şi pe proceduri transparente; b) roluri şi responsabilităţi bine definite în procesul bugetar; c) informaţie bugetară cuprinzătoare, elaborată şi prezentată publicului într-o manieră clară şi accesibilă. De asemenea, art. 38 alin. (2) din *Legea nr. 837-XIII din 17 mai 1996 cu privire la asociațiile obștești* prevede că controlul asupra surselor de venit, cuantumului mijloacelor obţinute, plăţii impozitelor şi asupra altei activităţi financiare a asociaţiei obşteşti îl exercită organele de control financiar şi administrare fiscală. Adițional, în partea ce ține de obiectivul 15, acțiunile 1) și 2) comunicăm că acestea au un conținut ambiguu fiind lipsite de previzibilitate, prin urmare în eventualitatea adoptării acestora va fi dificil de identificat măsurile legislative care urmează a fi întreprinse. Mai mult, în partea ce ține de *elaborarea sub egida Consiliului creat sau existent* nu este clar dacă respectiva entitate la care se face referire există sau nu. În contextul celor enunțate, obiectivul 15 precum și acțiunile incluse urmează a fi revizuite și în același timp exclus Ministerul Justiției în calitate de executor principal.	
	19. La obiectivul 19: la acțiunea 1) în partea ce ține de prevenirea dezinformării și răspândirii știrilor false și/sau a informațiilor manipulatorii prin platformele media, atragem atenția că prin *Legea nr.257 din 22 decembrie 2017 cu privire la completarea Codului audiovizualului al Republicii Moldova nr. 260/2006*, a fost definită „securitate informațională" și instituite sancțiuni pentru prejudicierea securității informaționale, care implică măsuri pentru asigurarea protecției persoanelor, a societății și a statului de eventuale tentative de dezinformare și/sau de informare manipulatoare din exterior și pentru neadmiterea provocărilor cu caracter mediatic îndreptate împotriva Republicii Moldova;	**19. Nu se acceptă.** Procesul de armonizare a legislației este un proces continuu. Totodată, cadrul legal actual nu reglementează multe noțiuni și raporturi în sensul răspândirii știrilor false și/sau a informațiilor manipulatorii prin platformele media, nu oferă o soluție la stoparea fenomenului știrilor false sau a prevenirii răspândirii acestora.
	20. La obiectivul 19: la acțiunea 4) privind armonizarea legislației naționale cu standardele și practicile CoE și UE în domeniul drepturilor omului, în vederea protecției	**20. Se acceptă.** A fost exclus

	demnității umane contra fenomenului de defăimare prin intermediul platformei on-line și domeniul audiovizualului, comunicăm despre inițiativa legislativă a Guvernului de modernizare a Codului civil, adoptată de Parlament prin Legea nr. 133 din 19 iulie 2018, prin care s-a propus introducerea unei noi secțiuni dedicată respectului datorat ființei umane și drepturilor ei inerente. Potrivit art. 31^3 în redacția *Legii nr. 133 din 19 iulie 2018 privind modernizarea Codului civil și modificarea și completarea unor acte legislative* „[..] orice persoană fizică are dreptul la viaţă, la sănătate, la integritate fizică şi psihică, la libera exprimare, la nume, la onorare, demnitate şi reputaţie profesională, la propria imagine, la respectarea vieţii intime, familiale şi private, la protecţia datelor cu caracter personal, la respectarea memoriei şi corpului său după deces, precum şi alte asemenea drepturi recunoscute de lege. Aceste drepturi sunt insesizabile şi inalienabile.". La fel, în art. 16 din *Codul audiovizualului* sunt reglementate drepturile persoanelor lezate la replică, rectificare și la remedii echivalente, iar în art. 41 al codului este instituită obligația Consiliului Coordonator al Audiovizualului de a asigura protecția demnității umane, respectarea drepturilor omului, inclusiv a principiului egalității între femei și bărbați, și protecția minorilor. Normele citate poartă un caracter general aplicabil tuturor situațiilor, indiferent de metodele utilizate pentru defăimarea persoanelor. Astfel, doar precizarea *prin intermediul platformei on-line și domeniul audiovizualului* nu justifică intervențiile de ordin legislativ, iar o enumerare exhaustivă a metodelor utilizate ar pune în pericol aplicabilitatea normei în situațiile neprevăzute de lege în condițiile în care societatea și tehnologia este în continuă evoluție.	
	21. În scopul uniformizării terminologiei, se vor revizui instituțiile partenere de realizarea acțiunilor: *mass-media*, *organizații mass-media* și *societatea civilă, organizațiile societății civile*. Totodată, pentru claritatea și asigurarea realizării acțiunilor indicate, se va concretiza referința la *mediul privat*	**21. Se acceptă.**

Vasile BOTNARI
Director
Botnari