RAPORT

de monitorizare și evaluare a implementării Strategiei securităţii informaţionale a RM pentru anii 2019-2024

Perioada de raportare: 2019

SERVICIUL DE INFORMAȚII ȘI SECURITATE

Elaborat – martie 2020

CUPRINS:

LISTA DE ABREVIERI

- SSI – Strategia securităţii informaţionale a Republicii Moldova
- CSS – Consiliul Suprem de Securitate
- SIS – Serviciul de Informaţii şi Securitate
- MEI – Ministerul Economiei şi Infrastructurii
- MJ – Ministerul Justiţiei
- MF – Ministerul Finanţelor
- MECC – Ministerul Educaţiei, Culturii şi Cercetării
- MSMPS – Ministerul Sănătăţii, Muncii şi Protecţiei Sociale
- MAEIE – Ministerul Afacerilor Externe şi Integrării Europene
- MAI – Ministerul Afacerilor Interne
- MA – Ministerul Apărării
- PG – Procuratura Generală
- CNA – Centrul Naţional Anticorupţie
- ANRCETI – Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei
- CCA – Consiliul Coordonator al Audiovizualului
- AGE – Agenţia de Guvernare Electronică
- BNM – Banca Naţională a Moldovei
- CNPDCP – Centru Național pentru Protecția Datelor cu Caracter Personal
- STISC – IP „Serviciul Tehnologia Informației și Securitate Cibernetică”
- ASP – Agenţia Servicii Publice
- AGEPI – Agenţia pentru Protecţia Proprietăţii Intelectuale
- ANCD – Agenţia Naţională pentru Cercetare şi Dezvoltare
- TRM – IP Compania „Teleradio-Moldova”
- CTIF – IP „Centrul de Tehnologii Informaționale în Finanțe”/MF
- SV – Serviciul Vamal/MF
- IPRE – Institutul pentru Politici și Reforme Europene

REZUMAT EXECUTIV

Raportul de monitorizare şi evaluare a Strategiei securităţii informaţionale pentru anii 2019-2024 (în continuare SSI/Strategie) reprezintă o analiză a acţiunilor întreprinse, progresul înregistrat şi rezultatele obţinute pe parcursul anului 2019 la realizarea Planului de acţiuni al Strategiei, adoptată prin Hotărîrea Parlamentului nr.257 din 22.11.2018.

Serviciul de Informații și Securitate al Republicii Moldova, conform prevederilor art.art. 2 şi 3 al HP nr. 257 din 22.11.2018 şi a pct. 115 din Strategie, este desemnat ca autoritate coordonatoare şi responsabilă de monitorizarea şi coordonarea procesului de implementare a Planului de acţiuni.

Concepţia securităţii informaţionale a Republicii Moldova, aprobată prin Legea nr. 299/2017, reprezintă documentul de politici ce stă la baza reglementării procesului de implementare a Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024.

SSI 2019-2024 are scopul de a corela juridic şi de a integra sistemic domeniile prioritare cu responsabilităţi şi competenţe de asigurare a securităţii informaţionale la nivel naţional, fiind bazat pe rezilienţa cibernetică, pluralismul multimedia şi convergenţa instituţională în materie de securitate, destinate protejării suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

Planul de acţiuni însumează complexul de acţiuni elaborate de instituţiile de drept public şi privat, care sunt parte a societăţii informaţionale, precum şi acelor care direct sau indirect au competenţe şi atribuţii la domeniul informaţiei, comunicării şi tehnologiilor informaționale, pentru a realiza obiectivele Strategiei după cum urmează:

<u>Pilonul I</u> - Asigurarea securității spațiului informațional-cibernetic și investigarea criminalității informatice

1. *Crearea unui sistem integrat de comunicare şi evaluare a ameninţărilor la adresa securităţii informaţionale şi de elaborare a măsurilor operative de răspuns*
2. *Monitorizarea permanentă și asigurarea unui nivel înalt de securitate cibernetică*
3. *Consolidarea capacităților de apărare cibernetică Protecţia reţelelor de comunicaţii speciale ale Republicii Moldova şi a informaţiei cu accesibilitate limitată pentru menţinerea funcţiilor vitale ale statului*
4. *Asigurarea controlului asupra importului, certificării şi utilizării mijloacelor de protecţie a informaţiei*
5. *Combaterea criminalității informatice (investigarea infracțiunilor informatice)*
6. *Protecția copiilor față de orice formă de abuz în spațiul on-line*
7. *Combaterea fraudelor prin utilizarea mijloacelor de plată electronice*
8. *Dezvoltarea capacităţilor instituţionale în combaterea criminalității informatice*

9. *Efectuarea unor cercetări ştiinţifice aplicative în domeniul securităţii informaţionale*
10. *Dezvoltarea capacităţilor de rezilienţă cibernetică şi ridicarea nivelului de cultură în domeniul TIC*

<u>Pilonul II</u> - Asigurarea securității spațiului informațional-mediatic

1. *Dezvoltarea mecanismelor de comunicare strategică pentru realizarea intereselor naționale ale Republicii Moldova*
2. *Controlul civic și consolidarea cooperării societății civile cu autoritățile publice cu atribuții de asigurare a securității informaționale*
3. *Determinarea statutului juridic al publicațiilor periodice, al agențiilor de presă și al altor subiecți care activează în spațiul media din Internet*
4. *Asigurarea transparenței financiare în activitatea autorităților administrației publice, a asociațiilor obștești și a societăților comerciale în contextul asigurării securității informaționale*

<u>Pilonul III -</u> Consolidarea capacităților operaționale

1. *Dezvoltarea mecanismelor de prevenire, de depistare, de atenuare şi de răspuns la nivel naţional pentru asigurarea securităţii informaţionale*
2. *Dezvoltarea capacităților de reacție în cazul unor amenințări hibride de securitate*
3. *Dezvoltarea competențelor operaţionale de apărare cibernetică*
4. *Monitorizarea spațiului informațional și depistarea acțiunilor de dezinformare și/sau de informare manipulatorie din exteriorul și din interiorul țării*
5. *Sporirea capacităților de protecție a infrastructurilor critice naționale*
6. *Dezvoltarea capacităților de prevenire, de depistare și de contracarare a acțiunilor extremiste, teroriste și de altă natură ce periclitează securitatea informațională*

<u>Pilonul IV</u> - Eficientizarea proceselor de coordonare internă și de cooperare internațională în domeniul securității informaționale

1. *Dezvoltarea sistemului de pregătire a resurselor umane în domeniul securităţii informaţionale*
2. *Coordonarea activităţii autorităţilor administraţiei publice,a instituţiilor publice şi private în exercitarea atribuţiilor privind asigurarea securităţii informaţionale*
3. *Asigurarea cooperării internaţionale în domeniul securităţii informaţionale*
4. *Dezvoltarea cooperării naţionale şi internaţionale în domeniul apărării cibernetice*
5. *Consolidarea cooperării internaţionale în domeniul prevenirii şi combaterii criminalităţii informatice*

Pe parcursul anului 2019, care este primul an de implementare a HP nr. 257, Serviciul, de comun cu instituțiile responsabile, a realizat mai multe acțiuni organizatorice orientate la implementarea Planului și anume :

a) La nivelul instituțiilor au fost desemnate persoane coordonatoare responsabile pentru implementarea acțiunilor din Plan;
b) Au fost organizate şedinţe şi purtate discuţii în mod separat cu persoanele responsabile privitor la acțiunile de competență prevăzute în Planul Strategiei ;
c) În cazul unor instituții au fost elaborate planuri instituționale mult mai detaliate, în conformitate cu prevederile din Planul SSI;

În conformitate cu principiile de evaluare şi monitorizare a documentelor de politici, actuala Strategie este monitorizată prin prisma progresului şi a impactului produs, fiind utilizată metodologia de:

- Analiză a acţiunilor întreprinse de autorităţi prin prisma prevederilor Planului SSI şi a Planurilor instituționale elaborate în acest sens;
- Măsurare a progresului cantitativ şi calitativ al realizării SSI 2019-2024;
- Reflectare a indicatorilor de impact în primul an de implementare, conform aprecierilor insitituţiilor responsabile şi a indicatorilor prezentaţi în rapoarte;
- Identificare a riscurilor pentru implementarea bunelor practici şi a recomandărilor date.

Raportul cuprinde:

1. analiza acţiunilor şi a progreselor raportate de instituţiile implementatoare, conform rapoartelor remise în adresa Secretariatului Grupului de monitorizare creat în cadrul Serviciului de Informaţii şi Securitate;
2. aprecierea calitativă şi cantitativă a realizării acţiunilor în baza indicatorilor de progres şi a rezultatelor scontate, corelate cu obiectivul Strategiei;
3. descrierea riscurilor pentru realizarea acţiunilor scadente la finele perioadei de evaluare;
4. descrierea impactului realizării SSI conform indicatorilor de progres, a obiectivelor generale şi a scopului Strategiei, conform discuțiilor bilaterale şi multilaterale desfăşurate la nivelul instituţiilor responsabile şi partenere;
5. reflectarea evoluţiilor în grila indicatorilor de impact ai Strategiei, precum şi în conformitate cu aprecierile şi recomandările ce vor fi oferite de deputaţii din Comisia securitate naţională, apărare şi ordine publică, de organizaţiile neguvernamentale, experţii naţionali şi internaţionali din domeniul de securitate.

În procesul de analiză a rezultatelor şi indicatorilor de progres, pentru aprecierea rezultatelor acţiunilor întreprinse, sunt utilizate calificative după cum urmează: „Realizat", „Parţial Realizat", „În proces de realizare”, „Realizat înainte de termen” şi „Nerealizat".

DESCRIEREA ACȚIUNILOR PENTRU PERIOADA 2019

Planul prevede 3 acțiuni ce au ca termen de realizare anul 2019. Alte 26 acţiuni sunt definite cu caracter permanent, iar 10 acţiuni scadente din anul 2019, care se vor realiza pe o perioadă de mai mulţi ani.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
1/2	Desemnarea entităţii care va exercita rolul de Centru guvernamental de reacţie la incidente de securitate cibernetică şi care va constitui punctul de raportare a incidentelor de securitate cibernetică al Guvernului; stabilirea interacţiunii acestuia cu Centrul naţional de reacţie la incidente de securitate cibernetică	Trimestrul II, III, IV, anul 2019	Parțial realizat

Instituţia responsabilă: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică*

Corespunzător, sub egida STISC a fost elaborat proiectul Hotărîrii de Guvern pentru crearea CERT GOV, care a fost definit în versiune finală încă în luna septembrie. La 12 decembrie 2019 a fost discutat la ședința secretarilor generali. La moment proiectul HG urmează a fi introdus pe agenda ședințelor Guvernului, pentru a fi aprobat.

În cadrul Proiectului de HG, Serviciul Tehnologia Informaţiei şi Securitate Cibernetică se desemnează ca autoritate CERT GOV şi va constitui punctul unic de raportare a incidentelor de securitate cibernetică a Guvernului, pentru structurile de tip CERT departamentale, care funcţionează în cadrul instituţiilor sau autorităţilor publice guvernamentale şi va asigura implementarea măsurilor necesare pentru asigurarea securităţii cibernetice la nivel guvernamental.

Proiectul HG defineşte atribuţiile, principiile de organizare şi funcţionare a CERT GOV.

Proiectul a fost deja avizat, urmând procedura de aprobare a acestuia de către Guvern. (STISC)

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
16/1	Crearea, la nivel naţional, a entităţii cu 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): a) identificarea şi integrarea componentelor existente cu funcţii şi atribuţii în domeniul cibernetic şi mediatic, a autorităţilor administraţiei publice locale, precum şi a componentelor care vor fi create pe parcurs; b) determinarea liniei de activitate pentru fiecare componentă inclusă în cadrul Consiliului coordonator pentru asigurarea securităţii informaţionale, în funcţie de atribuţiile şi funcţiile deţinute din perspectiva asigurării securităţii informaţionale; c) elaborarea şi adoptarea cadrului normativ de interacţiune pentru	Trimestrul III, IV, anul 2019	Parțial realizat

	realizarea sarcinilor de depistare, prevenire şi contracarare a riscurilor şi ameninţărilor la adresa securităţii informaţionale	

Instituţia responsabilă: *Serviciul de Informaţii şi Securitate*

În calitate de autoritate responsabilă, sub egida SIS a fost creat Grupul de lucru ce a avut ca obiectiv central elaborarea Statutului Consiliului coordonator pentru asigurarea securității informaționale, constituit din reprezenanţi ai autorităților publice, societății civile, mass media și a companiilor private din domeniul TIC.

Grupul de lucru s-a întrunit în mai multe şedinţe conform Palierelor specializate și racordate la Strategia securității informaționale, în cadrul cărora a fost elaborat şi discutat proiectul Hotărârii de Guvern *„Cu privire la crearea Consiliului coordonator pentru asigurarea securității informaționale”*.

Ulterior, proiectul a fost examinat în mai multe runde prin prisma propunerilor/obiecțiilor conform atribuțiilor membrilor Grupului de lucru.

În cadrul şedinţei Grupului de lucru pentru examinarea proiectului ajustat al Statutului Consiliului Coordonator pentru Asigurarea Securităţii Informaţionale din 21 februarie 2020, organizate la sediul Centrului de Excelență TEKWILL, str. Studenţilor 9/11 din mun. Chișinău a fost aprobată versiunea finală a proiectului de HG.

La moment, Proiectul Hotărârii de Guvern urmează a fi aprobat de către Guvernul Republicii Moldova.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul III **Consolidarea capacităților operaționale**			
17/1	Crearea unei componente analitico-informaţionale, specializată pe ameninţările hibride de securitate în cadrul Serviciului de Informații și Securitate	Trimestrul II, III, IV, anul 2019	Realizat

Instituţia responsabilă: *Serviciul de Informaţii şi Securitate*

Conform prevederilor punctului de Plan, în cadrul Serviciului a fost creată o unitate analitico-informațională specializată în studierea ameninţărilor hibride de securitate.

Concomitent, în baza deciziei Prim-ministrului nr.60 a fost creat Grupul de lucru preocupat de crearea rețelei naționale pentru contracararea amenințărilor hibride la nivel național. Membrii Grupului de lucru sunt în proces de discuții privind adoptarea unei Concepții integrate privind amenințările hibride și a Protocoalelor de acțiune.

DESCRIEREA PROGRESELOR PENTRU ACȚIUNI SCADENTE DIN 2019 ȘI CU STATUT PERMANENT

Planul prevede alte 26 acţiuni definite cu caracter permanent, iar 10 acţiuni scadente din anul 2019, care se vor realiza pe o perioadă de mai mulţi ani.

Progresul realizării acţiunilor scadente din anul 2019 şi a celor cu termen permanent de implementare, este reflectat mai jos, pe fiecare palier și puncte din Plan ce corespund obiectivelor din partea descriptivă a Strategiei.

În acest capitol au fost incluse și rezultatele acțiunilor care au ca perioadă de realizare alta decît 2019, scadente din anul 2019 sau cu termen permanent, prezentate de instituțiile responsabile.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
1/1	Crearea/ desemnarea entităţii care va exercita rolul de Centru naţional de reacţie la incidente de securitate cibernetică şi care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autorităţile publice competente şi persoanele fizice şi juridice: a) elaborarea şi promovarea cadrului normativ relevant; b) crearea Centrului naţional de reacţie la incidente de securitate cibernetică	Perioada 2019-2020, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Cancelaria de Stat; Ministerul Finanţelor; Ministerul Economiei şi Infrastructurii.*

Crearea unui CERT naţional şi respectiv, elaborarea cadrului legal, care ar reglementa activitatea acestuia, este un proces complex, fapt pentru care este necesar să fie respectate prevederile Legii nr. 100 din 22.12.2017 cu privire la actele normative. Acest proces presupune iniţial efectuarea unei analize ample de impact la proiectul de lege cu privire la securitatea cibernetică, care este în proces de elaborare de către Ministerul Economiei şi Infrastructurii şi respectiv identificarea unui model optim de funcţionare a CERT naţional.

In acest context, STISC a demarat discuţii privind crearea CERT naţional pe parcursul anului 2019. În anul 2020, acţiunile STISC au ca obiectiv central crearea unui grup de lucru reprezentat de instituţiile responsabile conform "Strategiei de securitate informaţională pentru 2019 - 2024" şi a Planului de acţiuni pentru implementarea acesteia, care urmează să identifice paşii necesari a fi întreprinşi şi partajarea responsabilităţilor în procesul creării/desemnării entităţii care va exercita rolul de Centru naţional de reacţie la incidente de securitate cibernetică.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
1/5	Elaborarea cadrului normativ pentru asigurarea unui nivel înalt de securitate a reţelelor şi a sistemelor informatice la nivel naţional în baza bunelor practici ale UE	Perioada 2021-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția resonsabilă: *Ministerul Economiei şi Infrastructurii.*

MEI a iniţiat procedura de elaborare a proiectului de lege de transpunere în legislaţia naţională a Directivei UE 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune. Prin Ordinul MEI nr. 54 din 04.03.2019 a fost creat grupul de lucru pentru elaborarea proiectului de lege privind securitatea reţelelor şi sistemelor informaţionale. Concomitent, Corporaţia MITRE din SUA a elaborat un raport de pre-evaluare a capacităţii cibernetice naţionale, ce va fi utilizat la elaborarea legii prenotate

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
2/1	Identificarea şi eliminarea surselor de ameninţare la adresa securităţii persoanei, a societăţii şi a statului în spaţiul cibernetic: a) efectuarea auditului de securitate cibernetică a infrastructurilor de tehnologie a informaţiei de interes naţional şi a Sistemului de telecomunicaţii al autorităţilor administraţiei publice, precum şi a altor infrastructuri cibernetice de interes naţional, în vederea identificării disfuncţiilor şi vulnerabilităţilor; furnizarea soluţiilor/recomandărilor de remediere a acestora; b) implementarea rezultatelor auditului de securitate cibernetică	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Agenţia de Guvernare Electronică; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică*

În conformitate cu pct.10 subpct. 4) și pct.11 subpct. 11) și 13) din Statutul AGE, aprobat prin HG nr.760/2010, *cu modificările introduse prin HG nr.414/2018 „Cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat”*, în sfera de competență a Agenției a intrat domeniul auditului de securitate cibernetică, instituția fiind abilitată cu următoarele funcții: „11) efectuarea auditului de securitate cibernetică a infrastructurilor de tehnologie a informației și a Sistemului de telecomunicații al autorităților administrației publice, precum și a altor infrastructuri cibernetice de interes național, în vederea identificării disfuncțiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora; 12) efectuarea și evaluarea conformității auditului de securitate cibernetică efectuate în autoritățile publice cu cerințele minime obligatorii de securitate cibernetică, aprobate de Guvern, și informarea autorităților interesate conform domeniilor de competență; 13) monitorizarea implementării rezultatelor auditului de securitate cibernetică efectuate în autoritățile publice în conformitate cu cerințele minime obligatorii de securitate cibernetică, aprobate de Guvern;”.

Astfel, întru realizarea competențelor respective, pentru anul 2019, AGE a efectuat audite la următoarele APC:

1. Cancelaria de Stat;
2. Ministerul Apărării;
3. Ministerul Afacerilor Interne;
4. Ministerul Afacerilor Externe și Integrării Europene;
5. Ministerul Economiei și Infrastructurii;
6. Ministerul Finanțelor;

7. Ministerul Justiției;
8. Ministerul Agriculturii, Dezvoltării Regionale și Mediului;
9. Ministrul Educației, Culturii și Cercetării;
10. Ministrul Sănătății, Muncii și Protecției Sociale;
11. Agenția Servicii Publice;
12. Serviciul Tehnologia Informației și Securitate Cibernetică;
13. Centrul de Tehnologii Informaționale în Finanțe.

În cadrul efectuării auditului de securitate cibernetică la entitățile sus-menționate și implementării recomandărilor auditului, pentru atingerea obiectivului de asigurare a unui nivel înalt de securitate cibernetică:

• S-a remis către autoritățile auditate Raportul de Audit;

• S-a solicitat elaborarea și informarea AGE, în termen de 30 zile, privind planul de înlăturare a neajunsurilor depistate. La moment doar 4 instituții (Agenția Servicii Publice, Ministerul Economiei și Infrastructurii, Ministerul Educației, Culturii și Cercetării, Ministerul Sănătății, Muncii și Protecției Sociale) au informat AGE privind statutul elaborării planului de înlăturare a neajunsurilor depistate.

• Este în proces de elaborare raportul consolidat privind rezultatele auditului, care va fi remis autorităților abilitate. Raportul va fi finalizat și remis până în 27 martie 2020.

ASP - Pe parcursul lunilor noiembrie-decembrie ale anului 2019 Agenția de Guvernare Electronică *(AGE)* a efectuat în cadrul Instituţiei Publice „Agenția Servicii Publice” *(ASP)* auditul privind implementarea Hotărârii Guvernului nr.201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică. Raportul de audit privind implementarea Hotărârii Guvernului nr.201/2017 a fost prezentat de AEG către conducerea ASP prin demersul nr.3004-26 din 31.12.2019. Planul de tratare este în faza de coordonare pe interior și aprobare de către conducerea ASP.
Evaluările realizate relevă zone unde sunt necesare îmbunătățiri și persistă riscuri ce necesită a fi tratate corespunzător.

PG - În anul 2019, Secția tehnologii informaționale și combaterea crimelor cibernetice din cadrul Direcției urmărire penală și criminalistică a Procuraturii Generale nu a efectuat un audit intern al infrastructurilor de tehnologie la nivel instituțional, în vederea identificării disfuncțiilor și vulnerabilităților, iar în ceea ce privește efectuarea unui audit extern, Direcția finanțe și contabilitate a Procuraturii Generale urmează să identifice auditorul extern, în colaborare cu Secția tehnologii informaționale și combaterea crimelor cibernetice, în baza demarării procedurilor de achiziții publice.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
2/2	Asigurarea aplicării Cerinţelor minime de securitate cibernetică de nivelul II în cadrul prestării serviciilor electronice publice; determinarea direcţiilor de activitate	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

	prioritare pentru prevenirea şi suprimarea ameninţărilor respective	

Instituția responsabilă: *Agenţia de Guvernare Electronică*

În cadrul implementării acestei acțiuni s-au efectuat două sub-acțiuni practice:

2.1.) A fost efectuat auditul de securitate cibernetică privind implementarea Cerințelor minime obligatorii de securitate cibernetică.

2.2.) S-au efectuat 3 seminare de instruire destinate persoanelor responsabile din partea prestatorilor de servicii privind implementarea Cerințelor minime obligatorii de securitate cibernetică. La seminare au participat în jur de 18 persoane.

ASP – Au fost identificate următoarele domenii pentru îmbunătățiri:

- organizarea sistemului intern de securitate cibernetică/informațională;
- cerințele minime obligatorii de securitate cibernetică de nivelul II;
- achiziția/actualizarea sistemelor informaționale;
- externalizarea administrării/ mentenanței sistemelor informaționale;
- răspunsul la incidente, continuitatea proceselor și recuperarea.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
2/3	Elaborarea mecanismelor şi a metodelor de prevenire şi contracarare a pericolelor în spaţiul cibernetic, generate de serviciile informaţionale prestate de către persoanele fizice şi juridice	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Serviciul de Informații și Securitate*

În perioada anului 2019, SIS a elaborat ***Proiectul de lege pentru modificarea art. 64 din Legea 241/2007 privind comunicațiile electronice,*** în contextul diminuării numărului de utilizatori ai cartelelor de telefonie mobilă preplătite *(PrePay)*. Prin *(scr. nr. 7/2-1898 din 18.07.2019)*, Serviciul a remis proiectul de lege pentru promovare în adresa Ministerului Economiei și Infrastructurii *(MEI)*.

MEI prin *(scr. nr. 09-4860 din 31.07.2019)*, nu a susținut promovarea proiectului actului legislativ, invocând faptul că în cadrul UE nu există prevederi legislative cu reflecție unitară, asupra diminuării numărului de utilizatori de cartele de telefonie mobilă preplătite *(PrePay)*.

Potrivit informațiilor deținute de SIS, în majoritatea statelor UE, cartelele de telefonie mobilă preplătite *(PrePay),* pot fi procurate doar prin înregistrarea prealabilă a datelor utilizatorilor. Recent, astfel de norme au fost incluse în legislația Austriei și României, iar la nivel mondial, există în legislația a peste 150 de țări.

În contextul celor menționate, SIS identifică soluții pentru promovarea proiectului respectiv.

În perioada de referință, Serviciul a delegat un ofițer în Grupul interinstituțional moderat de către MEI, în vederea elaborării ***Proiectului actului normativ*** pentru transpunerea **Directivei NIS (UE) 2016/1148** *privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană, adoptată la 06 iulie 2016.*

Directiva NIS (UE) 2016/1148 – este primul act legislativ al UE, care abordează provocările în materie de securitate cibernetică în ceea ce privește reziliența și cooperarea pe segmentul dat în UE.

În anul 2019, experții SIS au participat la ședințe comune consemnate cu factorii de decizie și specialiștii Companiei *"Teleradio – Moldova"* și *Consiliului Audiovizualului*, în vederea stabilirii mecanismelor de sesizare reciprocă în scopul prevenirii şi de contracarare a pericolelor în spaţiul cibernetic, determinării planurilor interne ale autorităților menționate în scopul realizării obiectivelor trasate conform Strategiei securității informaționale și Planului de acțiuni pentru implementarea acesteia.

În contextul inițierii procesului de creare a Consiliului Coordonator de Asigurare a Securității Informaționale *(CCASI)*, specialiștii SIS au participat la ședințe ordinare de lucru cu reprezentanții societății civile și a instituțiilor mass-media.

În perioada de referință, experții Serviciului au studiat aspectele teoretice și practice de creare a unui CERT instituțional cu atribuții de reacţie rapidă la incidente de securitate cibernetică.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
2/4	Identificarea unui mecanism legal de interacţiune între autorităţile publice competente şi persoanele fizice şi juridice, indiferent de tipul de proprietate, în vederea acordării de către acestea a accesului la codul-sursă al aplicaţiilor elaborate, comercializate şi distribuite pentru autorităţile publice	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne*

Specialiștii SIS au studiat practicile statelor UE, în scopul asigurării unui nivel înalt de securitate cibernetică, inclusiv modalitatea de interacțiune între autoritățile publice competente, persoanele fizice și juridice în vederea acordării de către aceștia a accesului la informațiile de interes.

În scopul preluării bunelor practici de la partenerii externi în Planul de cooperare externă pentru anul 2020 au fost trasate obiective de cooperare pe această dimensiune cu statele UE.

Experții SIS au revizuit ***Cerințele minime obligatorii de securitate cibernetică***, aprobate prin **Hotărârea Guvernului nr. 201/2017**, care prevăd unele mecanisme de transmitere a codului sursă către autoritatea care efectuează achizițiile sistemelor informaționale.

ASP – Pe parcursul anului 2019, în vederea asigurării securității informației la utilizarea resurselor informaționale a avut loc instruirea planificată a personalului Agenției, inclusiv la angajare. Totodată, s-au efectuat două audituri externe, inclusiv și în privința securității informaționale. În baza rapoartelor de audit urmează să fie elaborat un plan de lucrări de înlăturare a vulnerabilităților depistate și a minimiza pericolele în spațiul cibernetic pentru a îmbunătăți protecția resurselor informaționale și a asigura complexitatea serviciilor electronice publice prestate de Agenție.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
2/5	Coordonarea cu Centrul Naţional pentru Protecţia Datelor cu Caracter Personal a măsurilor de protecţie a datelor cu caracter personal, care să asigure aplicarea principiului protecţiei datelor începînd de la conceperea acestora şi protecţia implicită a datelor atunci cînd se elaborează, se proiectează, se selectează şi se utilizează aplicaţii, servicii şi produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează astfel de date în corespundere cu legislaţia privind protecţia datelor cu caracter personal	Perioada 2019-2020, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: Autoritățile administrației publice

În anul 2019 CNPDCP a avizat 17 proiecte de acte normative prezentate spre examinare de către autoritățile administrației publice.

În activitatea sa, Serviciul de Informaţii şi Securitate protejează datele cu caracter personal în conformitate cu Politica de asigurare a securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale ale SIS.

ASP – Pentru aplicarea măsurilor de protecție a datelor cu caracter personal și asigurarea securității informaționale a serviciilor electronice, care se bazează pe prelucrarea datelor cu caracter personal în corespundere cu legislația în vigoare, se consultă și se coordonează Centrul Național pentru Protecția Datelor cu Caracter Personal. La moment sunt înregistrate 12 sisteme informaționale ce prelucrează date cu caracter personal, iar 2 sisteme sunt în proces de coordonare.

MSanatMPS – Pe parcursul anului 2019 au fost organizate 2 ședințe comune cu CNPDCP în scopul ajustării documentației și sistemelor informaționale cu legislația privind protecția datelor cu caracter personal.

MECC – Prin scrisoarea nr. 08/3-09/l395 din 19.03.19, Ministerul Educaţiei, Culturii şi Cercetării a trimis spre consultare Centrului Național pentru Protecția Datelor cu Caracter Personal proiectul Politicii de securitate a datelor cu caracter personal în cadrul Ministerului Educaţiei, Culturii şi Cercetării.

La data de 08.08.19 ministerul a înregistrat Sistemul de evidenţă contabilă şi Sistemul de evidenţă a resurselor umane în Registrul de evidenţă al operatorilor de date cu caracter personal. Totodată, prin scrisoarea nr. 08/3-09/4377 din 17.08.19,

ministerul a expediat toate documentele necesare pentru aprobarea notificării în registrul menţionat. Au fost aprobate: 1) Ordinul nr. 383/2019 cu privire la aprobarea Politicii de securitate a datelor cu caracter personal în cadrul Ministerului Educaţiei, Culturii şi Cercetării.

MF – Conform prevederilor Legii nr.133/2011 privind protecţia datelor cu caracter personal, Ministerul Finanțelor, în coordonare cu Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (CNPDCP): - a elaborat și aprobat Politica de securitate privind protecția datelor cu caracter personal la prelucrarea datelor acestora în sistemele informaționale gestionate de minister (*Ordinul MF nr.82 din 27.05.2019*); - s-a înregistrat în calitate de operator de date cu caracter personal la CNPDCP.

Totodată, au fost aprobate următoarele acte normative:

- Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a resurselor umane (*Ordinul MF nr.83 din 27.05.2019);*

- Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă (*Ordinul MF nr.84 din 27.05.2019*). Ambele sisteme au fost notificate la CNPDCP.

SFS a MF – Pe parcursul anului 2019 au fost realizate următoarele acțiuni:

1. La data de 11.11.2019, în adresa CNPDCP a fost remisă pentru examinare notificarea privind înregistrarea Sistemului informațional al SFS nr. 1573469322419 în format electronic la adresa www.registru.datepersonale.md;
2. În perioada 11.10.2019 - 25.11.2019 au fost aprobate un șir de ordine cu privire la modul de utilizare a sistemelor informaționale ale SFS, după cum urmează:

- Ordinul SFS nr. 438 din 11.10.2019 Cu privire la aprobarea *Regulamentului privind autentificarea şi administrarea înregistrărilor de utilizator al resurselor informaţionale ale SFS*;
- Ordinul SFS nr. 487 din 04.11.2019 Cu privire la aprobarea *Instrucțiunii privind modul de utilizare și acces al echipamentelor multifuncționale în cadrul Sistemului unificat de imprimare protejată „DocPrint”;*
- Ordinul SFS nr. 535 din 25.11.2019 Cu privire la modificarea *„Regulamentului privind organizarea, administrarea și funcționarea Sistemului informațional al SFS” aprobat prin Ordinul SFS nr. 458 din 24.10.2019;*
- Ordinul SFS nr. 536 din 25.11.2019 Cu privire la modificarea *„Regulamentului privind prelucrarea și protecția informațiilor ce conțin date cu caracter personal în cadrul SFS”, aprobat prin Ordinul SFS nr. 715 din 28.12.2018.*

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
3/2	Elaborarea măsurilor de apărare cibernetică pentru protecţia infrastructurii critice naţionale, precum şi a altor sectoare prioritare pentru stat	Perioada 2021-2023, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Serviciul de Informaţii şi Securitate, Ministerul Apărării*

În conformitate cu solicitările parvenite, Serviciul a acordat suport Ministerului Apărării în scopul creării CERT - ului militar cu atribuții de reacție rapidă la incidente cibernetice.

Simultan, specialiștii Serviciului au consultat I.P. STISC în procesul de elaborare a proiectului Hotărârii de Guvern *privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental*.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
3/3	Elaborarea şi implementarea măsurilor de protecţie a sistemelor informaţionale ce prelucrează informaţii atribuite la secret de stat şi a componentei TIC din sistemele de apărare naţională	Anul 2022, cu verificarea anuală indicatorilor de progres în cazul realizării înainte de termen	În proces de realizare

Instituția responsabilă: *Serviciul de Informaţii şi Securitate*

În perioada de referință experții SIS au perfectat și remis **11 avize** pentru entitățile de protecție a sistemelor informaționale ce prelucrează informații atribuite la secret de stat și a componentei TIC din sistemele de apărare națională.

SIS a înaintat propuneri de modificare a Hotărârii Guvernului nr. 885 din 22.08.2005 *pentru aprobarea Concepției privind Registrul de stat al resurselor de mobilizare*.

Simultan, experții SIS au examinat o versiune de Cerinţe de Securitate Specifice elaborate de IGP al MAI, fiind remise recomandările necesare pentru protecția secretului de stat, în scopul autorizării sistemului informaţional în conformitate cu prevederile Hotărârii Guvernului nr. 1176/2010.

Concomitent, ofițerii SIS au participat la ședința Ministerului Finanțelor privind acțiunile necesare de a fi întreprinse pentru certificarea sistemelor informaționale ce prelucrează informații atribuite la secret de stat.

În conformitate cu cerințele stabilite în Hotărârea Guvernului nr. 1176 din 22 decembrie 2010, Serviciul a acordat asistența necesară pentru consolidarea capacităților de apărare cibernetică.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
4/1	Dezvoltarea mecanismelor de protecţie a sistemelor speciale de comunicaţii electronice prin aplicarea mijloacelor de protecţie criptografică şi tehnică a informaţiilor	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate*

SIS a elaborat Proiectul tehnic pentru modernizarea Sistemului de comunicații guvernamentale. După aprobarea acestuia urmează a fi stabilit numărul soluțiilor de protecție ce urmează a fi instalate.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
4/2	Efectuarea controalelor asupra sistemelor speciale de comunicaţii electronice şi raportarea către autoritatea responsabilă cu privire la măsurile tehnice şi tehnico-organizatorice întreprinse pentru asigurarea securităţii cibernetice	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate*

În anul 2019, au fost executate **20 proceduri** de audit pentru sisteme informaționale aflate în gestiunea subunității de profil a SIS.

În perioada de referință nu au parvenit rapoarte de audit de la alte autorități ce gestionează sisteme speciale de comunicații.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
4/3	Actualizarea cadrului normativ în domeniul sistemelor speciale de comunicaţii electronice	Perioada 2020-2023, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate*

În vederea excluderii prevederilor care pot duce la apariția riscurilor de securitate pentru sistemul de comunicații guvernamentale, experții SIS au revizuit ***Regulamentul cu privire la telecomunicațiile speciale, aprobat prin Hotărârea Guvernului nr. 735/2002*** și a fost propusă includerea în ***Regulament*** a normei care va asigura obținerea gratuită a liniilor de telecomunicații de la **”Moldtelecom”**.

A fost elaborat proiectul Hotărârii de Guvern și remis spre promovare în adresa MEI *(scr. nr. 7/3-1989 din 30.07.2019)*.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
4/6	Promovarea cadrului normativ privind instituirea subdiviziunilor responsabile de protecţia datelor cu caracter personal în cadrul persoanelor juridice de drept public şi de drept privat	Anul 2020, cu verificarea trimestrială a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Centrul Naţional pentru Protecţia Datelor cu Caracter Personal*

Centrul Naţional pentru Protecţia Datelor cu Caracter Personal a elaborat şi promovat în anul 2019 proiectul de lege privind protecţia datelor cu caracter

personal, care a fost votat în prima lectură la 30.11.2018 de către Parlamentul RM. Proiectul menţionat conţine reglementări cu privire la măsurile de asigurare a protecţiei datelor cu caracter personal în cadrul persoanelor juridice de drept public şi de drept privat. În perioada de raportare CNPDCP a fost informat despre crearea şi desemnarea subdiviziunilor responsabile de protecţia datelor cu caracter personal în cadrul Procuraturii Generale şi Serviciului Fiscal de Stat.

Nr *(din Plan)*	Acţiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
5/1	Certificarea mijloacelor de protecţie tehnică şi criptografică a informaţiei	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituţia responsabilă: *Serviciul de Informaţii şi Securitate*

În cadrul Grupului de lucru departamental au fost examinate două solicitări ale agenţilor economici privind importul mijloacelor tehnice speciale, destinate pentru obţinerea ascunsă a informaţiei.

Nr *(din Plan)*	Acţiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
5/3	Alinierea cadrului normativ în domeniul protecţiei criptografice a informaţiei la cadrul normativ european	Anul 2021, cu verificarea anuală indicatorilor de progres în cazul realizării înainte de termen	În proces de realizare

Instituţia responsabilă: *Serviciul de Informaţii şi Securitate*

A fost examinat cadrul normativ European care reglementează cerinţele pentru serviciile de certificare a cheilor publice *(Regulamentul UE 910/2014, Decizia UE 2015/1505, Decizia UE 2015/1506, Decizia UE 2016/650).*

A fost elaborat *Proiectul ordinului de modificare a Normelor tehnice în domeniul semnăturii electronice avansate calificate, pentru reglementarea standardului CaDES (Decizia UE 2015/1506).* Respectiv acesta a fost remis spre examinare autorităţilor competente *(scr. Nr. 7/2-3058 din 26.11.2019).*

Complimentar, a fost elaborat proiectul Legii pentru transpunerea Regulamentului UE 910/2014 *(scr. nr. 7/2-3058 din 26.11.2019)*, ce a fost expediat Cancelariei de Stat *(scr. nr. 7/2-1554 din 18.06.2019 şi repetat prin scr. nr. 7/2-2494 din 03.10.2019).*

La moment conform solicitării Cancelariei de Stat se elaborează Analiza impactului sectorial.

Nr *(din Plan)*	Acţiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
5/5	Exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice	Permanent, cu verificarea anuală a indicatorilor de	În proces de

		progres	realizare

Instituția responsabilă: *Serviciul de Informații și Securitate*

A fost recepționată și examinată cererea de acreditare a prestatorului din cadrul I.P. „STISC” și documentele anexate la aceasta *(scr. 7/2-2615 din 18.10.2019)*. În rezultat fiind refuzată acreditarea prestatorului *(scr. nr. 7/2-3365 din 30.12.2019)*.

În anul 2019, au fost desfășurate **2 controale** a prestatorilor de servicii de certificare din cadrul I.P. „STISC” şi I.P. „CTIF”.

În procesul de monitorizare permanentă a activității prestatorilor de servicii de certificare, au fost stabilite derogări de la prevederile cadrului normativ de reglementare, fiind înaintate prescripţiile de rigoare.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
6/1	Eficientizarea capacităților (mecanismului) de combatere a criminalității informatice	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală*

În cadrul MAI au fost instruiți 18 angajați.

Pe parcursul anului 2019, procurorii au avut mai multe întruniri în ceea ce ține de combaterea crimelor informatice și anume:

- „Metodici și tactici de identificare, investigare și judecare a infracțiunilor săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale”, organizat de către INJ (mun. Chișinău, 4 martie 2019);
- „Particularitățile urmăririi penale și judecării cauzelor privind infracțiunile în domeniul informaticii și telecomunicațiilor”, organizat de către INJ (mun. Chișinău, 5 martie 2019);
- „Securitatea informațională și implementarea cerințelor față de asigurarea securității datelor cu caracter personal”, organizat de către INJ (mun. Chișinău, 6 martie 2019);
- „Specificul activității speciale de investigații la cercetarea infracțiunilor din domeniul informaticii”, organizat de către INJ (mun. Chișinău, 9 aprilie 2019);
- Lucrările Comitetului Convenției privind criminalitatea informatică al Consiliului Europei (T-CY) și la cea de a 4-a reuniune plenară de elaborare a Protocolului II la Convenția de la Budapesta;
- „Conferința CyberEast: Acțiuni pro-reziliență cibernetică în regiunea Parteneriatului Estic (Bruxelles, Regatul Belgiei, 19 septembrie 2019 – 20 septembrie 2019);
- Evenimentul de lansare a platformei EU4Digital (mun. Chișinău, 24 septembrie 2019);

- „Conferința internațională privind investigațiile online: Dark web și abuzurile asupra copiilor prin internet”, organizată de Biroul de programare informatică al Consiliului Europei (C-PROC) , în cooperare cu EUROJUST (or. Haga, Regatul Țărilor de Jos, 29 septembrie 2019 – 02 octombrie 2019);
- Participarea la Exercițiul de securitate cibernetică, organizat de Agenția de Guvernare Electronică în comun cu reprezentanți din Estonia și de la compania CybExer (mun. Chișinău, 16 octombrie 2019 și 29 octombrie 2019);
- Conferința *Octopus* dedicată cooperării împotriva criminalității informatice (Cybercrime@Octopus) (Strasbourg, Franța, 20 – 22 noiembrie 2019).

De asemenea, în cadrul Procuraturii mun. Chișinău activează 5 procurori specializați în domeniu, din cadrul Biroului Antitrafic și Combaterea Crimelor Cibernetice.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
6/2	Acordarea ajutorului metodico-practic subdiviziunilor teritoriale privind investigarea infracţiunilor informatice	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală*

În contextul executării acţiunii date au fost instruiţi 146 angajați.

Dispoziția șefului IGP nr. 613 din 29.11.2019, având la bază Ordinul șefului interimar al Inspectoratului General al Poliției nr. 429/2019 „Cu privire la crearea rețelei de persoane din cadrul subdiviziunilor teritoriale ale Inspectoratului General al Poliției, responsabile în domeniul prevenirii și combaterii infracțiunilor informatice și celor conexe (inclusiv de exploatare sexuală și abuz asupra copiilor prin Internet)”;

În perioada 02 – 05 decembrie 2019, în incinta Inspectoratului Național de Investigații, ofițerii Centrului pentru combaterea crimelor informatice au desfășurat cursul de instruire în domeniul prevenirii și combaterii infracțiunilor informatice și celor conexe (inclusiv de exploatare sexuală și abuz asupra copiilor prin Internet).

Conform Ordinului MAI nr. 214 din 22 iunie 2018 „Cu privire la organizarea cursurilor de perfecţionare/specializare/recalificare în anul de studii 2018 - 2019”, au fost organizate şi desfăşurate 3 cursuri cu genericul „Combaterea crimei organizate”, „Activitatea de urmărire penală” şi „Tehnologii informaţionale”.

PG – Ghidul privind metodica de investigare a infracțiunilor informatice și în domeniul telecomunicațiilor este în proces de elaborare și urmează a fi definitivat.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
6/3	Implementarea de noi mecanisme la nivelul instituţiilor implicate în combaterea criminalităţii informatice (atragerea companiilor private şi a experţilor independenţi, dezvoltarea laboratoarelor)	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală*

Pe parcursul anului 2019, Secția Justiție Penală și Aplicarea Legii a Ambasadei SUA în Republica Moldova a donat echipament destinat extragerii și analizării informațiilor stocate în memoria telefoanelor mobile precum, 16 dispozitive de stocare a informațiilor necesare asigurării funcționalității serverelor, stațiilor de lucru și stocare a imaginilor criminalistice, o sursă de alimentare neîntreruptibilă și un calculator.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
6/4	Perfecţionarea cadrului legal ce reglementează salarizarea efectivului specializat în combaterea criminalităţii informatice şi investigarea infracţiunilor informatice	2020	În proces de realizare

Instituția responsabilă: *Ministerul Finanţelor; Ministerul Afacerilor Interne*

La 28 iunie 2019 în adresa Ministerului Finanțelor au fost expediate propuneri de modificare a Legii nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar (*scrisoarea MAI nr. 38/1544*).

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
7/1	Combaterea fenomenului de pornografie infantilă pe Internet	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală*

Pe parcursul perioadei ianuarie-decembrie 2019, ofițerii Secției protecția copiilor a CCCI au participat la 18 activități de dezvoltare a capacităților profesionale, dintre care 11 la nivel național și 7 activități internaționale.

Cazuri investigate

Au fost investigate 43 de cazuri după cum urmează:

art. 173 Codul penal (*Hărțuirea sexuală*) - 1

art. 175 Codul penal (*Acțiuni perverse*) – 3

art. 177 Codul penal (*Încălcarea inviolabilității vieții personale*) - 1

art. 178 Codul penal(*Violarea dreptului la secretul corespondenței*) – 1.

art. 206 Codul penal (*Traficul de copii*) – 1.

art. 208[1] Codul penal (*Pornografia infantilă*) – 24

art. 303 Codul penal (*Amestecul în înfăptuirea justiției și în urmărirea penală*) – 1.

Cazuri referite - 11

PG – Pentru art. 208[1] din Codul penal al Republicii Moldova a fost înregistrat un număr de 39 de cazuri.

Cauze transmise în judecată – 19.

Sentințe de condamnare în număr de 16.

MECC – În RM Ziua siguranţei pe internet este marcată anual, începând cu anul 2012. Această zi este marcată sub formă de decadă, cu durata de 1 săptămână, fiind organizate diverse activităţi la nivelul instituţiilor de învăţământ cu implicarea elevilor, părinţilor, cadrelor didactice, cu privire la promovarea utilizării într-un mod mai sigur şi responsabil a tehnologiei on-line şi a telefoanelor mobile de către elevi, precum şi conştientizarea şi educarea acestora privind riscurile navigării pe internet.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
7/2	Combaterea fenomenelor de ademenire (grooming) şi hărţuire sexuală a copiilor prin intermediul Internetului	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală*

Cazuri investigate grooming – 4 și cazuri referite – 4.

PG - Pentru art. 175[1] din Codul penal al Republicii Moldova, în anul 2019, au fost înregistrate 2 cazuri.

A fost transmisă în judecată o cauză penală și nici o sentință nu a fost pronunțată.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
7/3	Promovarea unui Internet mai sigur pentru copii prin intermediul consilierilor on-line și încurajarea raportărilor prin proiecte informaționale specializate	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală*

1) A fost elaborat în comun cu MECC și semnat Ordinul comun nr. 132/86 din 19.02.2019 al MAI și MECC cu privire la realizarea măsurilor de prevenire a

riscurilor în mediul online a tinerilor. Ulterior, la data de 28.03.2019, în incinta MECC a fost desfășurată o ședință de lucru pentru planificarea realizării Ordinului comun 132/86;

2) A fost elaborată, în comun cu DGUP și DGSP a IGP, DPPCC, Academia ”Ștefan cel Mare” și DPPÎ a MAI, Instrucțiunea metodică cu privire la specificul investigării infracțiunilor cu caracter sexual săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale, aprobată prin Ordinul MAI nr.112 din 01.03.2019;

3) La data de 26.11.2019 a fost semnat și înregistrat cu nr. 458 Ordinul IGP cu privire la aprobarea Procedurii operaționale standard referitor la investigarea infracțiunilor de pornografie infantilă.

4) Campanii desfășurate – 2 și 13 lecții de informare în liceele din RM în cadrul campaniilor „Ziua siguranței pe Internet” (februarie 2019) și „Luna securității cibernetice (octombrie 2019**)**

PG – La data de 18.11.2019 în contextul marcării Zilei europene pentru protecția copiilor împotriva exploatării și a abuzurilor sexuale, împreună cu reprezentanții Centrului Internațional „La Strada” în incinta Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale a fost desfășurată o conferință de presă privind preocupările instituțiilor de stat implicit a celor de drept și a ONG-urilor la contracararea exploatării sexuale a copiilor, în special cele cu utilizarea tehnologiilor on-line, care pun în pericol grav sănătatea și dezvoltarea psihosocială a copilului.

MECC – În parteneriat cu CI „La Strada”, în anul 2019 au avut loc un șir de activităţi cu privire la asigurarea securităţii copiilor în internet, principalele fiind:

1) Concurs pentru cadrele didactice din comunitatea „Intersecţie. Zona sigură online” cu genericul „Împreună pentru un internet mai bun!”;

2) Două ateliere de formare „Siguranţa online a copilului prin procesul educaţional”, organizate separat pentru cadrele didactice din învăţământul primar şi gimnazial (16-18.08.2019 şi 23-25.09.2019);

3) Un atelier de lucru pentru profesori „Aspecte practice în lucrul cu copiii la tema siguranţei online” (01.11.2019);

4) Două conferinţe naţionale pentru cadre didactice (30.11.2019 şi 07.12.2019) – „Siguranţa copiilor online”, desfăşurate în cadrul programului „Intersecţie. Zona sigură online” cu aderarea cadrelor didactice noi la comunitatea „Zona sigură online”, menită să unească cadrele didactice, să le implice în dialog şi schimb de opinii, bune practici, etc.;

5) Marcarea Zilei europene a siguranţei copiilor în internet în februarie 2019, prin desfăşurarea diverselor acţiuni de informare pentru părinţi, elevi şi profesori în cadrul cărora au fost informaţi despre riscurile online, comportamentele riscante, cât şi despre modalităţile de protecţie pe internet;

6) Au fost elaborate peste 20 de modele de proiecte de lecţii care pot fi utilizate de cadrele didactice în cadrul lecţiilor sau diverselor activităţi extraşcolare, proiectele fiind plasate pe site-ul siguronline.md;

7) Desfăşurarea în luna octombrie 2019 a Lunarului Securităţii Cibernetice, fiind organizate activităţi pentru elevi, cadre didactice şi părinţi cu informarea cu privire la protecţia datelor cu caracter personal, securitatea informaţiilor, etc.;

8) Cu suportul UTM, pe parcursul lunii septembrie 2019, au fost organizate training-uri pentru cadre didactice cu referire la securitatea cibernetică.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
8/1	Schimbul de informaţii între Centrul pentru combaterea crimelor informatice din cadrul MAI şi departamentele de securitate ale instituţiilor financiare	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală*

BNM - Pe parcursul anului 2019, Banca Naţională a Moldovei şi Inspectoratul General al Poliţiei au iniţiat discuţii privind modificarea *Acordului privind schimbul de informaţii periodic între Banca Naţională a Moldovei şi Inspectoratul General al Poliţiei,* în vederea racordării prevederilor Acordului la cerinţele actuale.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
8/2	Promovarea unor măsuri de securitate sporită în privinţa bancomatelor (ATM-urilor) la nivel de hardware şi software	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală*

MAI – La 12.03.2019 - ședință cu reprezentanții Băncii Naționale a Moldovei în vederea abordării subiectului plăților electronice, întru elucidarea problemelor apărute în cadrul documentării grupărilor criminale. În cadrul ședinței menționate au fost puse în discuție problematicile aferente mijloacelor de plată electronice, în cadrul căreia s-a decis ca fiecare parte să prezinte informații relevante care vor servi drept temei pentru inițierea modificărilor de regulamente, platforme, metode de filtrare a unor tipologii etc.;

La 30.07.2019 angajații secției mijloace de plată electronice a CCCI de comun cu reprezentanții Băncii Naționale a Republicii Moldova, s-au întrunit într-o ședință pentru a discuta modificările contractuale a contractului încheiat privind schimbul reciproc de informații cu IGP.

BNM – Conform planului, BNM a solicitat băncilor licenţiate elaborarea unui plan de acţiuni privind migrarea ATM-urilor la sisteme de operare sigure ce au suport de la producător.

În baza recomandărilor BNM şi a planului de măsuri, băncile licenţiate au migrat o parte din ATM-uri ce rulau pe sistemul de operare Windows XP pe sisteme de operare sigure. Astfel, numărul bancomatelor ce rulează pe sistemul de operare Windows XP în anul 2019 s-a diminuat cu 150 de bancomate. Ponderea bancomatelor ce rulează pe sistemul de operare Windows XP în totalul

bancomatelor deţinute de către bănci (1137 bancomate la finele anului 2019) este de 46% (525 bancomate), diminuându-se în anul 2019 faţă de anul precedent cu 13 p.p.

De asemenea, băncile licenţiate asigură în continuu migrarea ATM-urilor ce rulează pe sistemul de operare Windows XP la sisteme de operare sigure. Până la asigurarea migrării totale a ATM-urilor ce rulează pe sistemul de operare Windows XP la sisteme de operare sigure, băncile au aplicat măsuri compensatorii pentru minimizarea riscurilor şi prevenirea atacurilor, instalând soluţii dedicate în acest sens (de ex.: MacAfee - Integrity Control, Diebold Nixdorf GMBH -Intrusion Protection).

Banca Naţională a Moldovei va monitoriza în continuu îndeplinirea de către băncile licenţiate a planului de acţiuni şi a procesului de migrare a bancomatelor, sisteme de operare sigure ce au suport de la producător.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
8/3	Identificarea mecanismelor comune de combatere a fraudelor în tranzacţiile cu card şi fără card (card present şi card non-present)	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală*

MAI – La capitolul infracțiunilor comise cu utilizarea mijloacelor de plată electronice se atestă o creștere considerabilă la fraudele cu utilizarea numărului cardului (card not present), de la 247 în anul 2016 la 1645 cazuri în 2019. Acest lucru se datorează faptului că, tot mai multe persoane utilizează cardurile bancare pe diferite platforme online, în scopul achitării serviciilor, cumpărării diferitor produse, abonare la diferite platforme cu informații, care nemijlocit sunt des sparte, cu ulterioara vânzare a informațiilor despre cardurile folosite pe platforma Darknet.

De asemenea, fraudele cu cardurile contrafăcute sunt în creștere nesemnificativă față de perioada anului 2018, dar în continuare scădere, datorită politicilor de securitate tot mai riguroase ale instituțiilor financiare.

Totodată, în perioada de raport, s-a atestat o creștere a fraudelor cu carduri pierdute/furate, în perioada anilor 2016-2019 mărindu-se numărul lor de la 121 în 2016 la 253 în 2019.

Analiza datelor privind numărul și valoarea fraudelor înregistrate și raportate BNM, relevă faptul că tranzacțiile cu carduri de plată emise în RM la bancomate au loc în siguranță. În perioada anilor 2018 - 2019 cazuri de copiere și instalare a utilajului specializat la bancomate nu au fost înregistrate și raportate de către instituțiile bancare din țară.

BNM – La data de 30.10.2019 pe pagina oficială a Băncii Naţionale a Moldovei a fost publicat comunicatul „Recomandări pentru sporirea siguranţei in utilizarea cardului de plată”.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
9/1	Dezvoltarea unor subdiviziuni specializate în cadrul Inspectoratului General al Poliţiei al Ministerului Afacerilor Interne, al Procuraturii Generale şi al Serviciului de Informaţii şi Securitate în scopul depistării şi contracarării tentativelor infracţionale în domeniu	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală; Serviciul de Informatii şi Securitate*

MAI - În luna noiembrie 2019, având la bază ordinul IGP nr.729 din 07.11.2019,, Cu privire la crearea rețelei de persoane din cadrul subdiviziunilor teritoriale ale IGP, Inspectoratelor de Poliție din țară a fost transmisă solicitarea de desemnare a 1 sau 2 persoane din cadrul subdiviziunilor teritoriale, responsabile de domeniul prevenirii și combaterii infracțiunilor informatice și a celor conexe (inclusiv de exploatare sexuală și abuz asupra copiilor prin internet).

De asemenea, CCCI de comun cu DRU a IGP a elaborat și Procedura Standard de Operare, anexă la ordinul șefului IGP indicat mai sus.

În aceeași ordine de idei, în conformitate cu Dispoziția șefului IGP nr. 613 din 29.11.2019 în perioada 02 - 05 decembrie 2019, în incinta Inspectoratului Național de Investigații, ofițerii Centrului pentru combaterea crimelor informatice au desfășurat cursul de instruire în domeniul prevenirii și combaterii infracțiunilor informatice și celor conexe (inclusiv de exploatare sexuală și abuz asupra copiilor prin Internet).

Astfel, au fost instruiți 81 de ofițeri de investigații (6 femei și 75 bărbați), după cum urmează, în perioada:

02.12.2019 – 03.12.2019, au fost instruiți 38 de ofițeri de investigații;

04.12.2019 – 05.12.2019, au fost instruiți 43 de ofițeri de investigații.

PG - După cum am menționat anterior, pe parcursul anului 2019, personalul Secției și procurorii din procuraturile specializate și teritoriale au avut mai multe seminare de instruire în ceea ce ține de combaterea crimelor informatice și anume:

- „Metodici și tactici de identificare, investigare și judecare a infracțiunilor săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale”, organizat de către INJ (mun. Chișinău, 4 martie 2019);
- „Particularitățile urmăririi penale și judecării cauzelor privind infracțiunile în domeniul informaticii și telecomunicațiilor”, organizat de către INJ (mun. Chișinău, 5 martie 2019);
- „Securitatea informațională și implementarea cerințelor față de asigurarea securității datelor cu caracter personal”, organizat de către INJ (mun. Chișinău, 6 martie 2019);
- „Specificul activității speciale de investigații la cercetarea infracțiunilor din domeniul informaticii”, organizat de către INJ (mun. Chișinău, 9 aprilie 2019);

- Lucrările Comitetului Convenției privind criminalitatea informatică al Consiliului Europei (T-CY) și la cea de a 4-a reuniune plenară de elaborare a Protocolului II la Convenția de la Budapesta;
- „Conferința CyberEast: Acțiuni pro-reziliență cibernetică în regiunea Parteneriatului Estic (Bruxelles, Regatul Belgiei, 19 septembrie 2019 – 20 septembrie 2019);
- Evenimentul de lansare a platformei EU4Digital (mun. Chișinău, 24 septembrie 2019);
- „Conferința internațională privind investigațiile online: Dark web și abuzurile asupra copiilor prin internet", organizată de Biroul de programare informatică al Consiliului Europei (C-PROC) , în cooperare cu EUROJUST (or. Haga, Regatul Țărilor de Jos, 29 septembrie 2019 – 02 octombrie 2019);
- Participarea la Exercițiul de securitate cibernetică, organizat de Agenția de Guvernare Electronică în comun cu reprezentanți din Estonia și de la compania CybExer (mun. Chișinău, 16 octombrie 2019 și 29 octombrie 2019);

Conferința *Octopus* dedicată cooperării împotriva criminalității informatice (Cybercrime@Octopus) (Strasbourg, Franța, 20 – 22 noiembrie 2019).

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
9/3	Ajustarea activităţii desfăşurate în domeniul criminalităţii informatice în banca centrală de date a Sistemului informaţional automatizat „Registrul informaţiilor criminalistice şi criminologice"	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Serviciul Tehnologia Informaţiei şi Securitate Cibernetică*

MAI - La moment în cadrul Sistemului informațional automatizat "*Registru informației criminalistice și criminologice*" sunt supuse evidenței centralizate toate tipurile de infracțiuni, prevăzute de Codul Penal, inclusiv infracțiunile în domeniul criminalității informatice.

Astfel noi necesități de ajustare a Băncii centrale de date a SIA RICC nu au fost necesare.

CNA – Subdiviziunea specializată în analitică a examinat şi a înaintat propuneri la proiectul de lege pentru modificarea Legii nr. 216/2003 cu privire la Sistemul informaţional integrat automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvârşit infracţiuni (demersul MAI din 03.09.2019).

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
10/1	Planificarea şi dezvoltarea activităţii de cercetare ştiinţifică în domeniul tehnologiei informaţionale şi comunicaţionale	Perioada 2019-2021, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituţii responsabile: *Ministerul Educaţiei, Culturii şi Cercetării; Academia de Ştiinţe a Moldovei; Agenţia Naţională pentru Cercetare şi Dezvoltare*

Prin intermediul Programului naţional în domeniile cercetării şi inovării pentru anii 2020-2023 şi a Planului de realizare a acestuia, aprobat prin Hotărârea Guvernului nr. 381/2019, Ministerul Educaţiei, Culturii şi Cercetării a stabilit prioritatea strategică „Competitivitate economică şi tehnologii inovative" cu direcţia strategică de cercetare „Tehnologia informaţiei şi dezvoltare digitală" pentru următorii patru ani.

Nr *(din Plan)*	Acţiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
11/1	Desfăşurarea unor acţiuni de sensibilizare şi informare a societăţii privind ameninţările, vulnerabilităţile şi riscurile la adresa securităţii cibernetice	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituţii responsabile: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică*

Acţiunile de sensibilizare şi informare a societăţii privind ameninţările, vulnerabilităţile şi riscurile la adresa securităţii cibernetice desfăşurate de I.P. Serviciul Tehnologia Informaţiei şi Securitate Cibernetică, au avut drept scop dezvoltarea şi consolidarea unui ecosistem cibernetic sigur şi modern.

Prin intermediul acţiunilor de conştientizare a riscurilor din spaţiul cibernetic, a fost adus în prim plan rolul factorului uman în promovarea şi adoptarea unei culturi cibernetice corecte.

Dezvoltarea educaţiei precum şi dezvoltarea parteneriatelor şi mecanismelor de cooperare au constituit principalele pârghii de rezilienţă cibernetică. La 10 mai 2019, Serviciul Tehnologia Informaţiei şi Securitate Cibernetică în colaborare cu Universitatea Tehnică a Republicii Moldova şi comunitatea InfoSec Moldova au organizat şi desfăşurat, un eveniment ce are în vizor subiecte şi soluţii de securizare a mediului informaţional şi de prevenire şi combatere a agresiunilor din spaţiul virtual, InfoSec Meetup.

La 13 septembrie 2019 a avut loc prima ediţie a conferinţei Security Espresso Moldova unde s-au reunit ingineri, dezvoltatori, profesionişti în domeniul securităţii cibernetice şi toţi cei care şi-au propus să-şi îmbunătăţească resursele şi calităţile profesionale în securitatea informaţiei. Evenimentul a fost organizat de Comunitatea Security Espresso in parteneriat cu Universitatea Tehnică din Republica Moldova şi Serviciul Tehnologia Informaţiei şi Securitate Cibernetică. În perioada 29 Octombrie - 02 Noiembrie 2019, Serviciul Tehnologia Informaţiei şi Securitate Cibernetică a organizat cea de-a 7-a ediţie Moldova Cyber Week, care a cuprins Forumul regional de securitate cibernetică, ateliere de lucru, instruiri în cadrul mediului de învăţământ liceal şi universitar.

Evenimentul a fost organizat de către Serviciul Tehnologia Informaţiei şi Securitate Cibernetică sub patronajul Guvernului Republicii Moldova, cu suportul Ministerului Afacerilor Externe şi Integrării Europene şi Universităţi Tehnice a

Republicii Moldova. În cadrul evenimentului au participat peste. 40 de experţi şi 300 de participanţi din ţări precum, SUA, Elveţia, Ucraina, Georgia, România, Marea Britanie, Estonia etc.

Prin intermediul comunicării mediatice şi canalelor media, au fost răspândite informaţii şi programe de conştientizare a factorului uman cu privire la vulnerabilităţile, ameninţările şi riscurile prezente în spaţiul virtual. Asigurarea unui spaţiu cibernetic sigur este responsabilitatea atât a statului, cât şi a autorităţilor competente, a sectorului privat şi a societăţii civile. În acest context, schimbul de informaţii şi colaborarea cu instituţii din alte state a constituit un alt obiectiv important în cooperarea strategică şi schimbul de informaţii relevante privind incidentele cibernetice.

Monitorizarea şi menţinerea unui dialog activ cu organizaţiile internaţionale, crearea grupurilor de lucru şi consultare publică, precum şi implicarea societăţii civile şi parteneriatul public-privat au devenit direcţii cheie pe care ne-am axat.

Nr *(din Plan)*	**Acţiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
11/3	Desfăşurarea unor exerciţii şi antrenamente comune de consolidare a capacităţilor de reacţie la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituţii responsabile: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică*

Asigurarea unui spaţiu cibernetic sigur este responsabilitatea atât a statului, cât şi a autorităţilor competente, a sectorului privat şi a societăţii civile. In acest context, schimbul de informaţii şi colaborarea cu instituţii din alte state a constituit un alt obiectiv important în cooperarea strategică şi schimbul de informaţii relevante privind incidentele cibernetice. Monitorizarea şi menţinerea unui dialog activ cu organizaţiile internaţionale, crearea grupurilor de lucru şi consultare publică, precum şi implicarea societăţii civile şi parteneriatul public-privat au devenit direcţii cheie pe care ne-am axat.

Nr *(din Plan)*	**Acţiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
11/4	Organizarea şi desfăşurarea atelierelor de lucru în domeniul securităţii cibernetice pentru personalul din sectorul public şi privat deţinători de elemente de infrastructură critică	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituţii responsabile: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică*

În contextul *Lunii europene a securităţii cibernetice*, STISC s-a alăturat campaniei organizate de ENISA prin organizarea şi desfăşurarea atelierelor de lucru şi cursurilor de formare în domeniul securităţii cibernetice. Instruirile desfăşurate au fost prioritar axate pe prezentarea politicii de securitate adaptate

cerinţelor şi particularităţilor instituţionale, dar şi instrumentele necesare pentru dezvoltarea capacităţilor de rezilienţă cibernetică şi sporirea nivelului de cultură în domeniul TIC.

Scopul lor a fost de a informa şi antrena utilizatorii cu privire la cerinţele minime obligatorii de securitate cibernetică prin educaţie, conştientizare şi schimb de bune practici, în vederea minimizării numărului de erori neintenţionate şi a vulnerabilităţilor IT.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
11/5	Certificarea specialiştilor în domeniul securităţii cibernetice de către organizaţii /companii specializate pornind de la standardele aplicate şi cerinţele minime obligatorii de securitate cibernetică	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituții responsabile: *Agenția Guvernare Electronică*

În cadrul implementării acestei acțiuni s-au realizat următoarele sub-acțiuni practice:

5.1.) S-au efectuat 3 seminare de instruire dedicate persoanelor responsabile din partea prestatorilor de servicii privind implementarea Cerințelor minime obligatorii de securitate cibernetică. La seminare au participat în jur de 18 persoane.

5.2.) În perioada 18-22 martie 2019, AGE, în colaborare cu Academia de e-Guvernare a Estoniei, a organizat cursul de instruire „Implementarea și gestiunea sistemului de management al securității informației în baza standardului ISO 27001”. La curs au participat 16 reprezentanți ai serviciilor TI din cadrul diferitor autorități/instituții publice.

5.3.) În perioada 7-10 octombrie 2019, AGE, în colaborare cu Academia de e-Guvernare a Estoniei, a organizat cursul de instruire „Auditarea sistemului de management al securității informației în baza standardului ISO 27001”. La curs au participat 18 reprezentanți ai serviciilor TI din cadrul diferitor autorități/instituții publice.

5.4.) S-a inițiat procesul de achiziție a serviciilor de dezvoltare și implementare a unor module de instruire de la distanţă privind asigurarea securității cibernetice, cu emiterea certificatelor la finalizarea cu succes a lor, pentru următoarele categorii:

✓ Utilizatori

✓ Manager

✓ Administratori TI

✓ Dezvoltatori TI.

La moment are loc analiza ofertei tehnice și financiare a companiei calificate.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
11/7	Introducerea şi promovarea unor conţinuturi curriculare privind securitatea informaţională în programele naţionale de studii	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituţii responsabile: *Ministerul Educaţiei, Culturii şi Cercetării*

În anul 2019 au fost desfăşurate următoarele activităţi în cadrul USM:

7.1.) Au fost elaborate planuri de studii de nivel de licenţă şi master în domeniul Securităţii informaţiei;

7.2.) Au fost acreditate Programele de studii cu traseul Securităţii informaţiei;

7.3.) Au fost elaborate conţinuturi pentru unele discipline ale traseului Securităţii informaţiei la nivel de licenţă şi master.

În altă ordine de idei, în 2019 a avut loc modernizarea curriculumului la disciplina Informatică pentru clasele VII-XII care la fel promovează securitatea online şi informaţională.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
11/8	Organizarea, inclusiv împreună cu partenerii străini, a cursurilor de instruire tematică în domeniul securităţii cibernetice pentru angajaţii instituţiilor publice	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Agenția Guvernarea Electronică*

În cadrul implementării acestei acțiuni s-au realizat următoarele sub-acțiuni practice:

8.1.) S-au efectuat 3 seminare de instruire dedicate persoanelor responsabile din partea prestatorilor de servicii privind implementarea Cerințelor minime obligatorii de securitate cibernetică. La seminare au participat în jur de 18 persoane.

8.2.) În perioada 18-22 martie 2019, AGE, în colaborare cu Academia de e-Guvernare a Estoniei, a organizat cursul de instruire „Implementarea și gestiunea sistemului de management al securității informației în baza standardului ISO 27001”. La curs au participat 16 reprezentanți ai serviciilor TI din cadrul diferitor autorități/instituții publice.

8.3.) În perioada 7-10 octombrie 2019, AGE, în colaborare cu Academia de e-Guvernare a Estoniei, a organizat cursul de instruire „Auditarea sistemului de management al securității informației în baza standardului ISO 27001”. La curs au participat 18 reprezentanți ai serviciilor TI din cadrul diferitor autorități/instituții publice.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
12/1	Evaluarea sectoarelor vulnerabile la componenta mediatică din cadrul sistemului de securitate informaţională	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituții responsabile: *Autorităţile administraţiei publice*

CA – Sectorul vulnerabil în domeniul audiovizualului din Republica Moldova rămâne a fi spațiul on-line. La etapa actuală nu există o bază de reglementare exhaustivă și mecanisme viabile de a supraveghea acest domeniu, iar absența unor reglementări primare impuse acestui sector lipsește de drept autoritatea statului de a interveni în caz de necesitate.

Astfel, se impune necesitatea dezvoltării cadrului normativ de reglementare a sectorului dat, inclusiv sub aspectul componentei de securitate informațională.

Concomitent, au fost reliefate și încălcări ale reglementărilor privind retransmiterea canalelor TV și publicarea informațiilor pe pagini web.

SIS – Centrul Antiterorist al SIS a inițiat procesul de identificare a sectoarelor vulnerabile a mass mediei, din perspectiva acţiunilor desfăşurate în spaţiul informaţinal de exponenţii organizaţiilor teroriste sau promotorii proceselor conexe fenomenului terorist.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
12/2	Dezvoltarea unor politici de comunicare strategică pe plan intern şi racordarea la platformele de comunicare strategică externe ale structurilor sistemului de securitate, apărare şi ordine publică pentru asigurarea securităţii informaţionale şi promovarea intereselor naţionale ale Republicii Moldova	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituții responsabile: *Consiliul Audiovizualului*

Fiind unica autoritate autonomă care reglementează domeniul audiovizualului și reieșind din competențele funcționale stabilite prin legea cadru, administrarea securității informaționale în domeniul audiovizualului nu comportă comunicare externă cu alte structuri ale sistemului de securitate.

Totodată, Consiliul Audiovizualului asigură dezvoltarea politicilor de comunicare internă pe domeniul securității informaționale atât în raport cu subiecții de reglementare participanți la raporturile audiovizuale, cât și cu platforma civilă, organizațiile mass-media și ONG-urile de profil.

În acest sens, pentru a asigura o comunicare mai eficientă între autoritatea de reglementare și furnizorii de servicii media audiovizuale, Consiliul Audiovizualului a organizat, la Chișinău, Comrat și Bălți, cu suportul Consiliului Europei, seminare cu genericul „Reflectarea campaniei electorale la alegerile parlamentare și referendumul republican din 24 februarie 2019 de către furnizorii de servicii media audiovizuale”, pentru jurnaliştii şi editorii de la posturile de radio

și televiziune. În cadrul seminarelor date a fost abordat și subiectul întitulat „Asigurarea securității informaționale în cadrul serviciilor de programe de către furnizorii de servicii media”, unde Consiliului Audiovizualului a venit cu anumite recomandări care trebuie să fie respectate pentru a asigura securitatea informațională în cadrul serviciilor de programe de către furnizorii de servicii media.

TV Moldova 1 pentru anul 2019 şi-a propus şi a realizat următoarele priorităţi:

- Informarea şi instruirea producătorilor, editorilor şi reporterilor privind necesitatea verificării informaţiilor din mai multe surse şi documentarea judicioasă, astfel încât să fie prevenite ştirile false şi informaţia manipulatorie;
- Asigurarea condiţiilor pentru informarea echidistantă a telespectatorilor prin instituirea unor reguli stricte în cazul emisiunilor de dezbateri: invitarea în studio a tuturor părţilor, oferirea condiţiilor pentru dreptul la replică, etc.;
- Difuzarea comunicatelor SIS în jurnalul de sinteză informaţională al zilei „Mesager”;
- Difuzarea constantă a informaţiilor privind măsurile de combatere a terorismului de orice gen la nivel naţional şi internaţional;
- Realizarea unor reportaje şi interviuri, unor discuţii în platou care se referă la educarea populaţiei, cu detalii privind protecţia datelor cu caracter personal, etc.

Anul 2019 a fost unul cu multe evenimente de rezonanţă, cât şi cu două campanii electorale – alegerile parlamentare din 24 februarie şi cele locale din 20 octombrie, care au necesitat un efort sporit şi promptitudine din partea angajaţilor TV Moldova. Astfel, în perioadele menţionate, au fost realizate 45 de ore de dezbateri electorale, cu genericul „Mă informez şi votez”. La TV Moldova 1 au fost organizate dezbateri electorale pentru candidaţii electorali, a fost pusă pe post emisiunea „Tribuna electorală” de promovare a conceptelor electorale ale partidelor, în ediţia „Mesager” şi ştirile de limbă rusă de la ora 22.00 au fost plasate rubricile „Alegeri parlamentare şi referendum 2019” şi „Electorala 2019”.

Potrivit monitorizărilor independente ale Centrului pentru Jurnalism Independent şi Coaliţia pentru Alegeri Libere şi Corecte, postul public Moldova 1 a reflectat echidistant şi imparţial ambele campanii electorale, a oferit acces egal concurenţilor electorali în ştiri, fără a favoriza sau defavoriza evident vreunul din candidaţi.

În rapoartele de monitorizare a activităţii posturilor de televiziune antrenate în campania electorală, elaborate şi prezentate săptămânal de Consiliul Audiovizualului, TV Moldova 1 a fost calificată ca un post care a respectat toate rigorile legale de elucidare a ambelor campanii electorale. În perioada 01.01.-31.12.2019, Moldova 1 nu se regăseşte în nici o monitorizare care a avut drept scop identificarea informaţiilor false difuzate de mass-media.

Radio Moldova – Campaniile electorale din anul 2019 au fost reflectate la Radio Moldova în cadrul dezbaterilor electorale – alegeri parlamentare, referendum consultativ şi alegeri locale. Moderatorii, în cadrul dezbaterilor, au asigurat participanţilor posibilitatea să-şi expună punctul de vedere asupra temelor

dezbătute. Pe parcursul dezbaterilor, participanţilor li s-au asigurat condiţii egale pentru libera exprimare a opiniilor.

Cu referinţă la actele normative interne, în anul 2019 au fost actualizate Regulamentul privind prelucrarea datelor cu caracter personal în cadrul sistemelor informaţionale gestionate de instituţie, Regulamentul cu referire la supravegherea prin mijloace video cu anexa planului de amplasare a camerelor video şi Regulamentul de acces pe teritoriu şi în sediile Companiei.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
14/1	Dezvoltarea unor politici de comunicare strategică pe plan intern şi racordarea la platformele de comunicare strategică externe ale structurilor sistemului de securitate, apărare şi ordine publică pentru asigurarea securităţii informaţionale şi promovarea intereselor naţionale ale Republicii Moldova	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituții responsabile: *Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; autorităţile administraţiei publice*

Conform Codului serviciilor media audiovizualului, subiecții de reglementare cu utilizarea rețelelor electronice în format on-line sunt calificați:

- furnizorii de servicii media audiovizuale liniari și neliniari;
- distribuitorii de servicii media audiovizuale;
- furnizorii de servicii de platforme de partajare a materialelor video aflați în jurisdicția Republicii Moldova;
- serviciile web care intră în concurență cu serviciile media audiovizuale a cărui conținut audiovizual prezentat pe pagină constituie scopul principal al acestora.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităţilor operaţionale**			
15/2	Ajustarea cadrului legal în vederea eficientizării colectării de date pentru identificarea provenienţei mijloacelor financiare şi a proprietăţii ale subiecţilor implicaţi în activităţi de dezinformare, manipulare şi propagandă ce subminează securitatea informaţională	Perioada 2019-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Serviciul de Informaţii şi Securitate; Ministerul Justiţiei; Centrul Naţional Anticorupţie; Consiliul Audiovizualului*

CA – La etapa actuală nu există o concepție dezvoltată de cadru legal pe domeniul audiovizualului cu privire la definirea acțiunilor și fenomenelor de dezinformare, manipulare și propagandă ce subminează securitatea informațională.

În acest sens urmează a fi amendat cadrul normativ în vigoare prin constituirea unui grup de lucru format din reprezentanții structurilor sistemului de securitate.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
16/2	Elaborarea, promovarea şi coordonarea politicilor de securitate informaţională în conformitate cu Concepţia, cu prezenta Strategie şi cu alte documente de politici de nivel naţional şi internaţional ce se referă la societatea informaţională	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Serviciul de Informații și Securitate*

MECC – În cadrul Ministerului Educaţiei, Culturii şi Cercetării au fost aprobate următoarele acte normative: 1) Ordinul nr.798/2019 cu privire la aprobarea Regulamentului privind utilizarea serviciilor internet şi de poştă electronică de serviciu în cadrul MECC; 2) Ordinul nr. 203/2019 cu privire la aprobarea Politicii interne privind securitatea cibernetică a MECC; 3) Ordinul nr. 383/2019 cu privire la aprobarea Politicii de securitate a datelor cu caracter personal în cadrul MECC; 4) Ordinul nr. 846/2019 cu privire la aprobarea Regulamentului privind prelucrarea informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă contabilă în cadrul MECC.

Radio Moldova – Despre războiul informaţional, care a căpătat amploare în ultimul timp, se discută, preponderent, la emisiunile „Moldova şi Lumea”, „Loc de dialog”, unde sunt invitaţi săptămânal reprezentanţi ai diferitor partide, experţi şi analişti politici. Difuzarea mesajelor psihologice destructive, a ştirilor false care pot genera panică, tensiuni sau conflicte în societate, a materialelor cu caracter extremist este exclusă şi interzisă conform Codului deontologic şi actelor normative interne ale IP Compania „Teleradio-Moldova”.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
16/3	Informarea publicului privind modalităţile de prevenire şi contracarare a riscurilor şi ameninţărilor la adresa componentelor sistemice ale securităţii informaţionale, inclusiv privind fenomenele nou-apărute la nivel naţional	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Serviciul de Informații și Securitate*

MECC – Angajaţii Ministerului Educaţiei, Culturii şi Cercetării au fost informaţi cu privire la măsurile generale de asigurare a securităţii informaţionale: resursele informatice, informatizarea şi conştientizarea ameninţărilor cibernetice şi recomandări împotriva atacatorilor cibernetici. Totodată, angajaţii au avut parte de sesiuni consultative şi practice la aplicarea: politicilor şi a actelor normative în domeniul securităţii cibernetice; regulilor privind utilizarea staţiilor de lucru, dispozitivelor mobile, echipamentelor portabile de tip laptop/tabletă/smartphone; prevenirea accesului neautorizat în sistemul informaţional şi utilizarea neautorizată a calculatoarelor; cerinţele privind parolele de acces; accesul la distanţă; cerinţele minime de securitate privind prelucrarea datelor cu caracter personal; utilizarea poştei electronice.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
18/1	Crearea în cadrul Forţelor Armate a entităţii responsabile de apărarea cibernetică la nivel naţional	Perioada 2019-2020, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Apărării*

În scopul realizării obiectivului, a fost iniţiat procesul de achiziție a echipamentului necesar – în progres. Crearea entității este planificată pentru august 2020.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
18/2	Consolidarea capacităţilor de instruire şi formare cibernetică prin participarea la exerciţii interstatale şi internaţionale de apărare cibernetică	Perioada 2019-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Apărării; Serviciul de Informații și Securitate*

1. Participarea a unui contingent militar format din 10 persoane la exercițiul internațional „Cetatea 2019”;
2. Participarea a 2 militari ca observatori la Exercițiul ”Cybershield 19”, SUA.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
18/3	Identificarea, prevenirea şi contracararea factorilor de risc cu potenţial informativ-subversiv în adresa apărării cibernetice a Republicii Moldova prin implementarea unui management integrat al spaţiului virtual şi dezvoltarea unui sistem de avertizare timpurie cu privire la elementele de risc la adresa obiectivelor de infrastructură	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate*

În luna iulie 2019, Serviciul de Informații și Securitate a inițiat măsuri de investigație tangențiale unor atacuri cyber.

În perioada noiembrie – decembrie 2019 au fost identificate tentative de atacuri *cibernetice* asupra sistemelor informaționale ale Armatei Naționale (AN), contracarate de către subdiviziunea de profil.

În perioada anului 2019, în adresa beneficiarilor au fost remise sinteze privind factorii de risc asupra sistemelor informaționale:

1. Comisiei Electorale Centrale cu privire la vulnerabilitățile din cadrul sistemului informațional, care ar putea compromite scrutinul electoral din 24 februarie 2019. A urmat un răspuns din partea CEC cu privire la măsurile ce vor fi luate în scopul diminuării riscurilor.

2. Informarea IGP privind identificarea programelor malițioase în sistemul informatic al Secției supraveghere contravențională a Brigăzii de Patrulare a INP al IGP, prin intermediul cărora există riscul de culegere și transmitere neautorizată a datelor sensibile.

3. Informarea Consilierului în domeniul apărării și securității naționale, Secretar al Consiliului Suprem de Securitate al RM, cu privire la *„Sistemul internaţional al securităţii informaţionale, ca garant al stabilităţii strategice şi parteneriatul echitabil în mediul internaţional global”*.

4. Informarea Serviciului Tehnologia Informaţiei şi Securitate Cibernetică (STISC) privind factorii care implică STISC şi generează vulnerabilităţi în asigurarea protecţiei cibernetice.

5. Informarea Directorului SFS privind activitatea unui Centru neînregistrat de instruire în domeniul TIC, sub marca *„Skillup-Moldova”*.

6. Informarea Vice-prim ministrului, Ministrului Afacerilor Interne al RM privind Practicile abuzive în cadrul INP al IGP al MAI.

În perioada menționată au fost elaborate **<u>studii analitice</u>**, după cum urmează:

- privind existenţa vulnerabilităţilor care pot compromite integritatea unor informaţii, implicit cu caracter sensibil, în contextul exploatării Sistemului automatizat de Gestionare și Eliberare a Actelor Permisive *(SIA GEAP)*;

- studiu *„Aspecte privind situația de securitate cibernetică în instituțiile guvernamentale din Republica Moldova”*. La subiect, au fost remise informații Președintelui și Prim-ministrului RM.

<u>Au fost întocmite note informative:</u>

- privind *„Aspecte generale privind securitatea informaţională internaţională”*, referitor la ameninţările moderne, atacuri cibernetice asupra sistemului informaţional internaţional;

- *„Referitor la incidentele cibernetice asupra infrastructurii informaţionale guvernamentale”***.**

<u>Au fost remise interpelări în adresa autorităților publice centrale:</u>

- *„Privind incidentele cibernetice”* - interpelare MAEIE și Ministerul Finanțelor.

Concomitent, în perioada de referinţă, 3 ofiţeri ai SIS, au participat la întrevederea cu protagoniștii Companiei ***„Verint Systems Inc”*** *(unul dintre liderii mondiali în dezvoltarea soluțiilor de Inteligență Cibernetică și lider în soluții de Inteligență Acționabilă)*, în cadrul căreia ultimii au prezentat **soluţiile software** pe domeniul OSINT.

În contextul inițiativei de dezvoltare a relaţiilor de cooperare cu partenerii externi, experții SIS, au elaborat propuneri pentru a fi abordate şi dezvoltate în cadrul unor întrevederi, şi anume pentru impulsionarea cooperării pe palier de analiză şi OSINT.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
19/1	Revizuirea cadrului legal existent în sensul definirii şi uniformizării noţiunilor cu privire la dezinformare, ştirile false şi/sau informarea manipulatorie, precum şi în vederea prevenirii răspîndirii acestora prin platformele media. Determinarea sectoarelor din cadrul securităţii naţionale a căror afectare (prin dezinformare) ar crea riscuri majore pentru funcţionalitatea statului	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituţia responsabilă: *Ministerul Justiţiei; Consiliul Audiovizualului*

Baza normativă cu privire la asigurarea securității informaționale în domeniul audiovizualului a fost asigurată odată cu completarea Codului audiovizualului al Republicii Moldova nr. 260-XVI din 27.07.2006 cu o normă care prevede că: *În vederea protejării spaţiului audiovizual naţional şi asigurării securităţii informaţionale, se permite furnizorilor de servicii media şi distribuitorilor de servicii media transmisiunea programelor de televiziune şi de radio cu conţinut informativ, informativ-analitic, militar şi politic care sunt produse în statele membre ale Uniunii Europene, în SUA şi Canada, precum şi în statele care au ratificat Convenţia europeană cu privire la televiziunea transfrontalieră.*

Reglementarea respectivă a fost menținută și în Codul serviciilor media audiovizuale nr.174 din 08.11.2018, art.17 alin.(4).

În vederea realizării normei respective, Consiliul Audiovizualului, prin Decizia nr. 2/5 din 15 ianuarie 2018, a obligat toți radiodifuzorii și distribuitorii de servicii aflați sub jurisdicția Republicii Moldova să-și racordeze serviciile de programe audiovizuale și ofertele serviciilor de programe retransmise în concordanță cu noile norme audiovizuale în termen de 30 de zile din data publicării în Monitorul Oficial al Republicii Moldova.

Scopul deciziei date este de a asigura protecția consumatorului de informație de eventuale tentative de dezinformare sau de informare manipulatoare din exterior și excluderea provocărilor cu caracter mediatic îndreptate împotriva Republicii Moldova prin neadmiterea spre transmisie/retransmisie a programelor de televiziune și radio cu conținut informativ, informativ-analitic, militar și politic care nu sunt produse în statele membre ale Uniunii Europene, SUA, Canada, precum și în statele care nu au ratificat Convenția Europeană cu privire la televiziunea transfrontalieră.

Totodată, radiodifuzori și distribuitori de servicii media au fost informați despre consecințele nerespectării legislației audiovizuale care implică aplicarea de către Consiliul Coordonator al Audiovizualului, în condițiile legii, a unor sancțiuni, în funcție de gravitatea şi frecvența încălcărilor comise, în conformitate cu art. 38 alin. (61) din Codul Audiovizualului al Republicii Moldova nr. 260-XVI din 27.07.2006.

În temeiul cadrului legal, pe parcursul anilor 2018-2019, Consiliul Audiovizualului a efectuat monitorizări atât a furnizorilor de servicii media, cât și a distribuitorilor de servicii media.

În cazul depistării derapajelor de la prevederile legale, Consiliul Audiovizualului a aplicat sancțiuni, care constituie de la 40 000 la 70 000 lei.

Cu privire la acțiunile de dezinformare, manipulare și propagandă din interiorul țării nu există un cadru legal de reglementare. Pentru acoperirea acestui sector, urmează a fi elaborate propuneri de amendare a cadrului legislativ.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
20/1	Elaborarea și aprobarea cadrului legal privind identificarea și desemnarea infrastructurilor critice naționale, inclusiv a celor ce țin de sistemele informaționale de importanță vitală	Perioada 2019-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate*

Experții SIS au participat la elaborarea Proiectului de lege privind Infrastructura critică națională *(în baza Directivei 2008/114/CE a Consiliului UE din 02.12.2008 privind identificarea și desemnarea infrastructurilor critice europene)*. Ulterior, proiectul a fost remis în adresa Cancelariei de Stat pentru crearea Grupului de lucru interinstituțional și definitivarea proiectului menționat. La data de 07.02.2019 a fost emis Ordinul Secretarului General de Stat nr. 36 *„Cu privire la instituirea grupului de lucru pentru definitivarea proiectului de lege privind infrastructura critică națională*”, pentru definitivarea proiectului în cauză. Concomitent, Serviciul a delegat un reprezentant în Grupul de lucru creat.

Centrul Antiterorist al SIS a elaborat ***Programul național privind protecția antiteroristă a infrastructurii critice pentru anii 2020-2024***, precum și ***Planul de implementare a Programului*** menționat.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
20/2	Evaluarea și raportarea privind starea și nivelul de securitate ale obiectivelor de infrastructură critică din perspectiva securității informaționale	Perioada 2021-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Serviciul de Informații și Securitate*

Centrul Antiterorist al SIS, pe parcursul anului 2019, a realizat **12 teste** *privind Protecția antiteroristă*, conform atribuțiilor deținute.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
21/1	Sincronizarea şi repartizarea raţională a forţelor instituţiilor naţionale spre depistarea preventivă a acţiunilor derulate din exteriorul şi/sau interiorul ţării, concepute ca diversiuni	Perioada 2020-2022, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Serviciul de Informaţii şi Securitate*

În anul 2019 experții SIS în domeniul juridic, au examinat și selectat cadrul normativ, care urmează a fi supus modificărilor în scopul armonizării legislației.

În acest sens, au fost purtate discuții cu reprezentanții organelor de drept, în scopul elaborării unor propuneri de completare a cadrului normativ pentru dezvoltarea capacităților instituționale.

Nota și studiul pe spețe ce țin de domeniul prevenirii, depistării și contracarării acțiunilor extremist-teroriste și de altă natură, ce periclitează securitatea informațională au fost elaborate.

SIS a realizat un studiu privind situația existentă în domeniul prevenirii, depistării și contracarării acțiunilor extremist-teroriste și de altă natură, ce periclitează securitatea informațională, cu evaluarea cadrului legal în acest domeniu.

Analiza efectuată a relevat o serie de deficiențe și a conturat domeniile în care cadrul legal existent necesită a fi completat prin prisma prevederilor Concepției securității informaționale.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
22/1	Evaluarea nivelului actual de pregătire a resurselor umane în domeniul securităţii informaţionale, pe fiecare compartiment în parte: mass-media, tehnologia informaţională, apărare, ordine publică şi contrainformaţii	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Autorităţile administraţiei publice; Consiliul Audiovizualului; Ministerul Economiei şi Infrastructurii; Ministerul Apărării; Ministerul Afacerilor Interne; Procuratura Generală; Serviciul de Informaţii şi Securitate; organizaţiile neguvernamentale*

SIS – În contextul testării capacităților de reacție a colaboratorilor SIS la atacuri cibernetice au fost simulate **2 atacuri.** Ulterior, datele privind rezultatele simulărilor au fost prezentate conducerii Serviciului.

Concomitent, s-a efectuat instruirea tuturor colaboratorilor, inclusiv a celor din cadrul direcțiilor teritoriale, privind modalitatea de reacție la incidente de securitate cibernetică și necesitatea de respectare a cerințelor de securitate și bunelor practici în ceea ce ține de igiena cibernetică.

ANCD – la nivel instituţional au fost evaluaţi 19 angajaţi şi realizată 1 instruire.

CA – În vederea consolidării capacităților funcționale, Autoritatea de reglementare în domeniul audiovizualului pentru asigurarea securității informaționale examinează posibilitatea de instituire în cadrul Consiliului Audiovizualului a unei direcții specializate în monitorizarea conținutului audiovizual în spațiul on-line, care va fi dotată din punct de vedere logistic (soft, tehnică și personal calificat).

La moment, nivelul capacităților Consiliului Audiovizualului de monitorizare și asigurare a securității informaționale acoperă doar realizarea prevederilor art.17 din Codul serviciilor media audiovizuale.

Pentru realizarea acțiunii date, este necesară modificarea cadrului legislativ ce ține de extinderea concepției securității informaționale în domeniul audiovizualului, cât și modificarea statutului prin care a fost aprobată organigrama Consiliului Audiovizualului prin hotărârea Parlamentului Nr. 433 din 28.12.2006.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
22/2	Identificarea categoriilor de beneficiari care urmează să fie incluşi cu prioritate în programele noi de instruire a resurselor umane în domeniul vizat	Anul 2021, cu verificarea trimestrială a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Autorităţile administraţiei publice*

SIS a elaborat un modul de instruire privind securitatea cibernetică și informațională. În planul propus spre aprobare directorului SIS, au fost identificați formatorii, timpul și locul desfășurării cursului de instruire în corespundere cu Strategia securității informaționale și Planului de acțiuni al SIS RM pentru implementarea acesteia.

În acest sens a fost desfășurat un curs de instruire pentru colaboratorii SIS din data de 20.11.2019, petrecut la INIS cu tematica **„Securitate informațională”.**

Totodată, în perioada de referință, ofițerii SIS au participat la o serie de evenimente de instruire în domeniul securităţii informaționale:

- la data de 4-5 martie 2019 un ofițer de informație a participat la ședințele de lucru a misiunii de experți TAIEX privind asigurarea securității și integrității rețelelor și serviciilor de comunicații electronice în cadrul ANRCETI;
- la data de 25 martie 2019, 6 ofițeri de informație au participat la instruirea *„Malware Analysis”,* oferită de specialiștii companiei *Kaspersky laboratory*;
- în perioadele 25-29 martie și 27-31 mai 2019, 2 ofițeri de informație au participat la cursul pregătit de *Naval Postgraduate School, Monterey (SUA)*, cu genericul *„Gestionarea incidentelor de securitatea cibernetică”,* desfășurat în cadrul Ministerului Apărării;
- în perioada 10-11 iunie 2019, un ofițer de informație a participat la *Wokrshop-ul CSDP Cyber Security (Politica comună de apărare și securitate pe securitate cibernetică)* pentru țările din cadrul Parteneriatului Estic, eveniment ce a avut loc la Tbilisi;
- în perioada 12-13 iunie 2019, 3 ofițeri de informație, au participat la *Workshop-ul EU4Digital: Trust & Security Network*;
- în perioada 15-28 iulie 2019, un ofițer al SIS, a participat la cursurile de instruire *„Cybersecurity Summer BootCamp”,* organizate de *Ministerul Economiei* al Spaniei, Institutul național de securitate cibernetică al Spaniei. Cursurile au avut loc în orașul Leon, Spania și au avut ca tematică crearea/dezvoltarea unui CERT;

- în perioada 29-30 octombrie 2019, un ofițer al SIS a participat la conferința pe domeniul securității cibernetice *European Cybersecurity Forum – CyberSec*, desfășurată în orașul Katowice, Polonia;

- în data de 29 octombrie 2019, 2 ofițeri ai SIS au participat de comun cu alte autorități naționale responsabile de domeniul securității cibernetice, la exercițiul de răspuns la incidente de securitate cibernetică, organizat de Agenția de Guvernare Electronică;

- în perioada 19-20 noiembrie 2019, 3 ofițeri ai SIS au participat la *Forumul regional de reziliență cibernetică Moldova Cyber Week*, organizat de STISC.

- în perioada 28-29 noiembrie 2019, un ofițer al SIS a participat la instruirea subregională cu privire la rolul tehnologiilor informației și comunicației în contextul securității regionale și internaționale, eveniment ce a avut loc în Skopje, Macedonia de Nord, eveniment organizat de OSCE.

- în perioada trimestrului IV a. 2019, ofițerii SIS au participat la cursurile online oferite de SANS cu tematica *„Windows Forensic Analysis”*.

ANCD – la nivel instituţional au fost identificaţi şi instruiţi 13 angajaţi.

MSanatMPS – pe parcursul 2019 reprezentanții MSMPS au participat la 2 training-uri privind prelucrarea informației.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
24/2	Stabilirea cooperării dintre Republica Moldova şi statele partenere, în special cele din cadrul Uniunii Europene, privind schimbul de informaţii, experienţe şi analize în scopul prevenirii, depistării şi contracarării ameninţărilor hibride de securitate în spaţiul informaţional	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Autorităţile administraţiei publice*

MECC - Universitatea de Stat din Moldova şi Universitatea Tehnică din Moldova sunt parteneri de implementare a proiectului Capacity Building/ Cooperarea Instituţională „Programe de licenţă şi de masterat profesional pentru dezvoltare, administrare, management, protecţia sistemelor şi reţelele de computere în companii”. În cadrul proiectului a fost organizat ciclul de cursuri în Securitatea informaţiei, predate de cinci profesori de la Universitatea West Attica, Grecia: Charalambos Patrikakis, Dimitrios Kogias, Panos Yannakopoulos, Konstantinos Mavrommatis şi Georgios Tselikis.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
25/3	Semnarea unor acorduri de colaborare (asistenţă mutuală) în domeniul apărării cibernetice	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Realizare înainte de termen

Instituția responsabilă: *Ministerul Apărării; Serviciul de Informaţii şi Securitate*

În baza Acordului de Cooperare încheiat de SIS cu Banca Națională a Moldovei din 31 ianuarie 2019, Serviciul dezvoltă platforma de dialog cu Departamentul de profil al BNM, lansat în noiembrie 2019.

Centrul Antiterorist al SIS a inițiat procedura de aderare la Acordul privind schimbul de informații în cadrul CSI în domeniul luptei cu terorismul și alte forme de manifestare violentă a extremismului precum și finanțarea acestora.

A fost expediată o solicitare la Interpol pentru conectare la sistemul informațional „Sirius".

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
26/1	Consolidarea mecanismelor de cooperare internaţională între autorităţile statului cu atribuţii în combaterea criminalităţii informatice şi organismul internaţional specializat EMAS (Europol Malware Analysis Solution) al EUROPOL	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală*

În luna martie a anului 2019, urmare solicitării parvenite din partea Proiectului de Analiză Cyborg, în vederea fortificării cooperării cu OEP Europol, a fost desemnat un angajat al CCCI al IGP responsabil de produsul EMAS.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
26/2	Utilizarea la nivel național a instrumentelor și metodelor de identificare a victemelor, inclusiv prin utilizarea Sistemului informațional automatizat „Protecția copiilor" și a bazei de date privind exploatarea sexuală a copiilor (ICSE) a OIPC INTERPOL	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală*

A fost obținut acces la platforma gestionată de către OEP EUROPOL "***LFE-Large File Explorer***", destinată pentru experți "***Europol platform for experts***".

În scopul acumulării probelor pe cazurile de pornografie infantilă, aflate în gestiunea centrului în adresa colegilor din cadrul Europol AP-TWINS, a fost expediată o solicitare pentru a se expune asupra imaginilor încărcate de către angajații SPC în baza internațională de date ICSE.

În urma solicitării suportului cu privire la categorizarea fișierelor încărcate în baza de date ICSE, de la membrii FP TWINS din cadrul Europol, la data de 10.04.2019 a fost primit răspuns, prin intermediul platformei LFE, gestionată de către Europol.

În cadrul proiectului internațional „I-CARE”, a fost realizată actualizarea soft-ului ce stă la baza Sistemului Informațional „Protecția copiilor”, în vederea interconectării cu baza de date ICSE a OIPC Interpol. De asemenea, au fost contactați reprezentanții Secretariatului General al OIPC Interpol în vederea întreprinderii acțiunilor necesare pentru conexiune cu server.

În cadrul a 22 c/p, au fost prelucrate cu utilizarea Sistemului Informațional ”Protecția Copiilor” și bazei de date ICSE a OIPC Interpol fișierele identificate pe dispozitivele ridicate în urma percheziției la domiciliul suspectului.

PG – La data de 14.03.2019, de către Consiliul Superior al Procurorilor a fost aprobată participarea a 2 procurori din cadrul Procuraturii Generale (inclusiv un procuror din cadrul Secției combatere a traficului de ființe umane din cadrul Direcției urmărire penală și criminalistică a Procuraturii Generale) în cadrul grupului de lucru constituit pentru elaborarea lucrării științifice cu titlul – „*Compendiu de norme juridice internaționale și naționale corespunzătoare în domeniul exploatării sexuale și abuzului sexual al copiilor cu utilizarea tehnologiilor informaționale și de comunicare (ESACTIC)*”, dezvoltată în cadrul proiectului „*Ensuring Self Sexual Assault Victims To Adequate And Social Protection*”, implementat de Centrul Internațional „La Strada” în cooperare cu Biroul INL al Ambasadei SUA în Republica Moldova.

În cadrul proiectului vor fi dezvoltate instrumente și metode de identificare a victimelor, inclusiv prin utilizarea Sistemului informațional automatizat.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
26/3	Cooperarea în cadrul punctelor naţionale de contact 24/7 în baza Convenţiei Consiliului Europei privind criminalitatea informatică (Budapesta, 2001) şi G7 24/7	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală*

MAI – În cadrul punctelor naționale de contact 24/7 în baza Convenției Consiliului Europei privind criminalitatea informatică au fost: trimise solicitări – 4 (1-Ucraina, 1- România, 1- Cipru, 1- Olanda)

- parvenite răspunsuri – 3 (1 – Ucraina, 1- Cipru, 1- Olanda)
- parvenite solicitări – 10 (2- Ucraina, 1 – Marea Britanie, 1- Belorusia, 1- Cehia; 4- SUA, 1- Germania, Rusia -2)
- trimise răspunsuri – 12 (2-Ucraina, 1- Belarus, 2 – Rusia, 1 – Marea Britanie, 1- Cehia; 4- SUA, 1- Germania)

PG – În anul 2019, Secția tehnologii informaționale și combaterea crimelor cibernetice a examinat 18 comisii rogatorii parvenite de la autoritățile competente din: Austria, Federația Rusă, Irlanda, Coreea, Belarus, Kazahstan, Germania, Turcia și Cehia.

Totodată Secția tehnologii informaționale a examinat și solicitarea Republicii Franceze privind conservarea datelor informatice prin intermediul punctului de contact 24/7.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
26/4	Dezvoltarea parteneriatelor existente cu NCMEC (Centrul Naţional al SUA privind Copiii Dispăruţi şi Exploataţi) şi aderarea la alte iniţiative similare	În funcţie de necesitate, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală*

Ministerul Afacerilor Interne a expediat 3 solicitări conform competenţei către NCMEC.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
26/5	Dezvoltarea unor parteneriate în scopul identificării, blocării, sechestrării şi confiscării produselor şi a instrumentelor provenite din infracţiunile transfrontaliere	2021	Realizare înainte de termen

Instituția responsabilă: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală; Serviciul de Informaţii şi Securitate*

Au fost recepţionate 7 solicitări internaţinoale parvenite prin intermediul CCPI.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
26/6	Participarea la evenimente internaţionale în domeniul prevenirii şi combaterii criminalităţii informatice în scopul formării personalului de specialitate	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Afacerilor Externe şi Integrării Europene; Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală; Serviciul de Informaţii şi Securitate*

Reprezentanţii autorităţilor responsabile de contracararea criminalităţii informatice au participat la 24 instruiri la nivel internațional, fiind instruiţi 25 angajați în acest domeniu.

În perioada anului 2019, experții SIS au participat în cadrul a șapte reuniuni, întrevederi și evenimente internaționale cu preluarea bunelor practici pe dimensiunea combaterii criminalității informatice.

PG – Pe parcursul anului 2019, personalul Secției și procurorii din procuraturile specializate și teritoriale au avut mai multe seminare de instruire în ceea ce ține de combaterea crimelor informatice și anume:

- Lucrările Comitetului Convenției privind criminalitatea informatică al Consiliului Europei (T-CY) și la cea de a 4-a reuniune plenară de elaborare a Protocolului II la Convenția de la Budapesta;
- „Conferința CyberEast: Acțiuni pro-reziliență cibernetică în regiunea Parteneriatului Estic (Bruxelles, Regatul Belgiei, 19 septembrie 2019 – 20 septembrie 2019);
- „Conferința internațională privind investigațiile online: Dark web și abuzurile asupra copiilor prin internet", organizată de Biroul de programare informatică al Consiliului Europei (C-PROC), în cooperare cu EUROJUST (or. Haga, Regatul Țărilor de Jos, 29 septembrie 2019 – 02 octombrie 2019);

Conferința *Octopus* dedicată cooperării împotriva criminalității informatice (Cybercrime@Octopus) (Strasbourg, Franța, 20 – 22 noiembrie 2019).

REFLECTAREA INDICATORILOR DE PROGRES CONFORM PRIORITĂŢILOR

În condiţiile unei evaluări intermediare, eficacitatea acţiunilor realizate de instituţiile responsabile şi partenere este relativ prematur de apreciat prin prisma priorităţilor prevăzute de SSI.

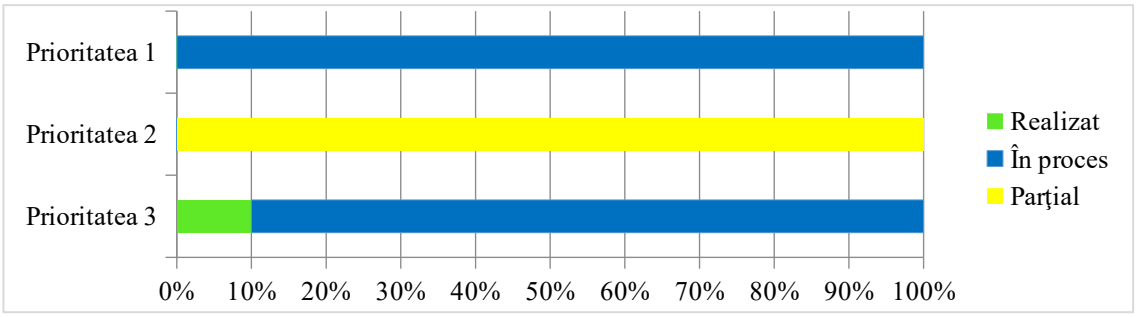
Totuși, trebuie de menţionat că trei acţiuni stabilite de Plan pentru a fi realizate în anul 2019 sunt esenţiale procesului de implementare de mai departe a Strategiei.

Printre acestea se numără priorităţile 3 şi 2 din Pilonul I, priorităţile 1 şi 2 din Pilonul III.

Ponderea procentuală a realizării priorităţilor pe parcursul anului 2019 sunt prezentate în graficile 1, 2 şi 3, elaborate prin prisma indicilor de rezultat.

Pilonul I. **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**	
Priorităţile pilonului	Indicatori de rezultat
1. Crearea Centrului naţional de reacţie la incidente de securitate cibernetică (CERT naţional)	1. Centrul naţional creat, care elaborează documente de politici şi asigură interacţiunea dintre toate componentele de asigurare a securităţii cibernetice
2. Desemnarea entităţii care va exercita rolul de Centru guvernamental de reacţie la incidente de securitate cibernetică al Guvernului (CERT Gov)	2. Centrul guvernamental asigură funcţionarea şi protecţia reţelelor speciale la nivel de Guvern şi autorităţi publice
3. Consolidarea cooperării dintre CERT-ul naţional, CERT Gov şi CERT-urile private	3. Acorduri de colaborare şi sustenabilitate în scopul prevenirii şi soluţionării incidentelor de securitate cibernetică

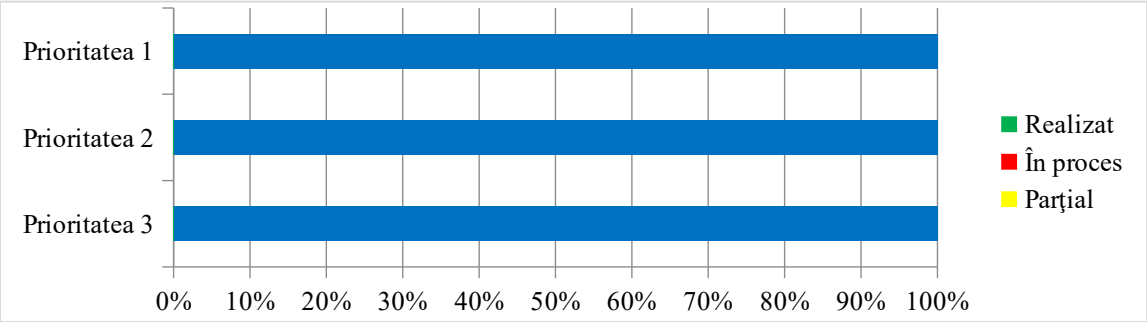
Grafic 1. Ponderea procentuală de realizare a priorităţilor Pilonului I



Pilonul II. **Asigurarea securităţii spaţiului informaţional-mediatic**	
Priorităţile pilonului	Indicatori de rezultat
1. Dezvoltarea instrumentelor de control civic în scopul asigurării securităţii informaţionale	1. Mecanism de interacţiune şi implicare a experţilor în scopul asigurării securităţii spaţiului informaţional
2. Elaborarea cadrului juridic pentru	2. Lege de modificare a cadrului juridic

determinarea statutului juridic al publicaţiilor periodice, al agenţiilor de presă şi al altor entităţi care activează în spaţiul media din Internet	existent
3. Crearea resursei/ platformei informaţionale de comunicare strategică	3. Resursă/ platformă informaţională de comunicare strategică creată

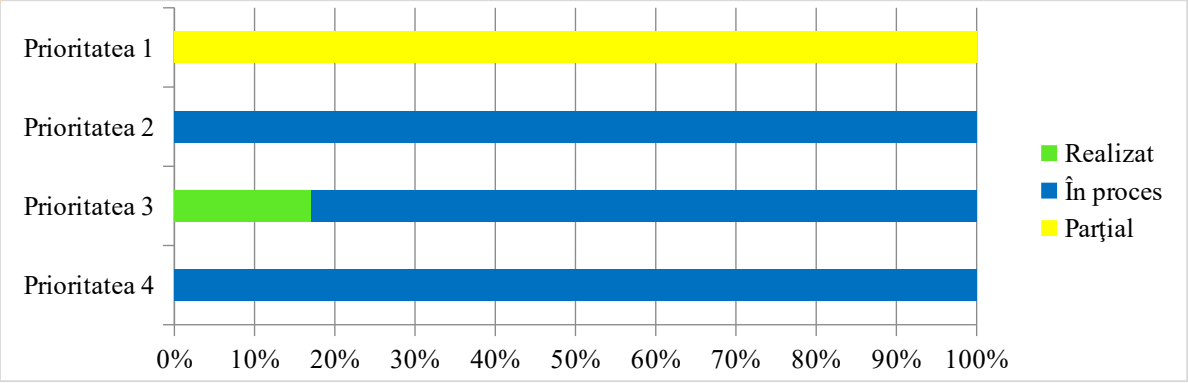
Grafic 2. Ponderea procentuală de realizare a priorităţilor Pilonului II



Pilonul III. Consolidarea capacităţilor operaţionale

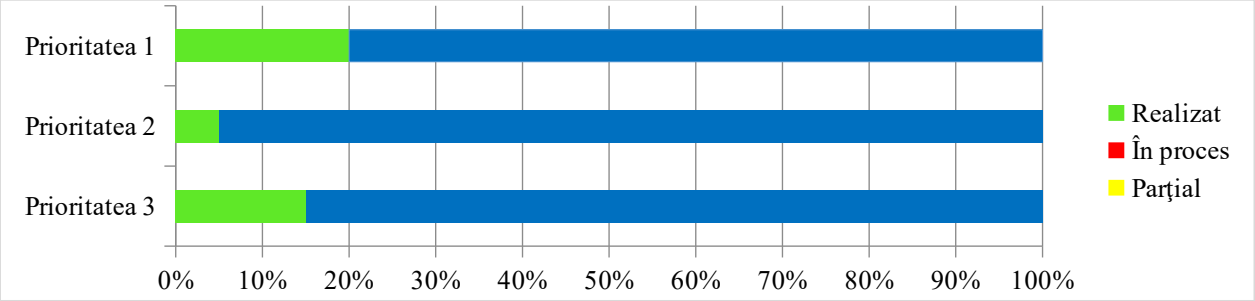
Pilonul III. **Consolidarea capacităţilor operaţionale**	
Priorităţile pilonului	Indicatori de rezultat
1. Crearea, la nivel naţional, a Consiliului coordonator pentru asigurarea securităţii informaţionale, în cadrul căruia vor fi identificate proceduri de comunicare strategică	1. Cadrul normativ privind crearea Consiliului coordonator pentru asigurarea securităţii informaţionale, elaborat şi aprobat
2. Crearea în cadrul Forţelor Armate a entităţii responsabile de apărarea cibernetică la nivel naţional	2. Cadrul normativ privind crearea în cadrul Forţelor Armate a entităţii responsabile de apărarea cibernetică la nivel naţional, elaborat şi aprobat
3. Crearea unei platforme specializate pe ameninţările hibride la adresa securităţii	3. Platformă creată şi funcţională
4. Elaborarea şi promovarea cadrului legal de reglementare a infrastructurii critice naţionale	4. Cadrul legal de reglementare a infrastructurii critice naţionale elaborat şi aprobat

Grafic 3. Ponderea procentuală de realizare a priorităţilor Pilonului III



Pilonul IV. **Eficientizarea proceselor de coordonare internă şi de cooperare internaţinoală în domeniul securităţii informaţionale**	
Priorităţile pilonului	Indicatori de rezultat
1. Dezvoltarea şi implementarea programelor de instruire adresate angajaţilor cu atribuţii de investigare şi urmărire penală în spaţiul informaţional	1. Specialişti instruiţi în baza practicilor UE
2. Dezvoltarea cooperării naţionale şi internaţionale în domeniul apărării cibernetice	2. Cadrul legal de cooperare negociat şi încheiat
3. Stabilirea mecanismelor de cooperare internaţională între autorităţile statului cu atribuţii în combaterea criminalităţii informatice şi organismele internaţionale pe segmentul asigurării securităţii informaţionale	3. Runde de consultări; acorduri bilaterale/ multilaterale semnate şi încheiate

Grafic 4. Ponderea procentuală de realizare a priorităţilor Pilonului IV



DESCRIEREA RISCURILOR DE IMPLEMENTARE

Implementarea Strategiei necesită cooptarea tuturor componentelor societății informaționale, care prin acțiuni comune, coordonate și agreate reciproc să ducă la realizarea obiectivelor Strategiei. Totodată, obiectivele și complexul de acțiuni definite pentru realizarea lor, au caracter transectorial și implică instituții din domeniul civil, mass media, companii TIC, trecând ulterior în spectrul autorităţilor publice și ajungând la dimensiuni mai sensibile ca cel de securitate, apărare, de drept și ordine publică.

Reieșind din caracterul transectorial al acțiunilor prevăzute de Planul SSI 2019-2024, au fost identificate mai multe riscuri a procesului de implementare, unele dintre care necesită o atenție specială și identificate soluții pentru eliminarea acestora.

Pentru a fi supuse atenției și soluționării, riscurile indentificate au fost divizate în trei categorii după cum urmează:

Categoria I: ***Riscuri la nivelul managementului asociat procesului de implementare a Planului de acțiuni al SSI 2019-2024:***

R:1.1. Managementul strategic din cadrul unor instituții responsabile sau partenere conform Planului de acțiuni, manifestă o atitudine superficială în adoptarea documentelor de politici interne, la nivel instituțional sau sectorial, care derivă din Staregia SSI 2019-2024;

R:1.2. Interacțiunea redusă dintre echipa de experți în materie de securitate informațională din cadrul instituțiilor de drept public și privat vizate în Planul SSI 2019-2024 și managementul decizional, care în asemenea circumstanțe poate lua decizii orientate la excluderea anumitor acțiuni și obiective din Strategie, reprofilându-le sub alte documente de politici sau institui noi procese solitare, diminuând caracterul unitar și continuu în implementarea Planului de acțiuni.

Categoria II: ***Riscuri operaționale la implementarea Planului de acțiuni al SSI 2019-2024:***

R:2.1. Fluxul de cadre sau insuficiența specialiștilor în domeniul tehnologiilor informaționale și ale comunicării în subdiviziunile responsabile de asigurarea securității informaționale în cadrul autorităților publice, în special la funcționarea și dezvoltarea Centrelor de reacție la incidentele de securitate cibenretică (CERT departamental);

R:2.2. Dotarea insuficientă a CERT-urilor departemantale cu sisteme operaționale și tehnica specializată pentru asigurarea securității cibernetice conform rigorilor și cerințelor de securitate informațională;

R:2.3. Elaborarea la nivel departamental a unor politici și protocoale operaționale focusate pe circumstanțe de moment și cu accent redus pe evoluții de

viitor în dezvoltarea tehnologiilor informaționale și comunicării, care pot genera vulnerabilități, riscuri și amenințări de securitate informațională;

Categoria III: ***Riscuri de natură complementară proceselor de implementare a Planului de acțiuni al SSI 2019-2024:***

R:3.1. Apariția unor noi generații de amenințări la adresa securităţii informaționale, catalizate de dezvoltarea accelerată a tehnologiilor informaționale și comunicării, care nu sunt vizate de Strategie și Planul de acțiuni pentru implementarea SSI 2019-2024;

R: 3.2. Caracterul electoral al anului 2020, care va influența procesele din domeniul civic, media și autorităţilor publice, în aprobarea unor documente de politici la nivel național derivate din Planul de acțiuni al SSI 2019-2024.

NOTĂ: Grupul de monitorizare din cadrul SIS va discuta cu reprezentanții autorităților responsabile de implementarea Planului de acțiuni al SSI 2019-2024 riscurile menționate supra și vor determina soluții pentru fiecare risc, în funcție de atribuțiile și competențele departamentale.

CONCLUZII ŞI RECOMANDĂRI

Procesul de monitorizare realizat pe parcursul anului 2019 şi expus în contextul prezentului Raport pentru primul an de implementare, denotă relevanța SSI, iar prioritățile de securitate informaţională stabilite în Strategie continuă să fie conforme tendinţelor de dezvoltare a societăţii informaţionale la nivel naţional şi internaţional.

Analiza şi evaluarea indicatorilor raportaţi de instituţiile responsabile prin prisma competenţei şi a spectrului de acţiuni din Plan, realizate de fiecare instituţie în parte sau prin interacţiune cu alte autorităţi, corelaţi cu obiectivele şi scopul Strategiei, reflectă de fapt un **progres relativ scăzut** în atingerea minimului de securitate informaţională.

Problemele de securitate şi criminalitate cibernetică, apărare cibernetică şi evoluţia noilor forme de ameninţări la adresa securităţii informaţionale, precum războiul informaţional, ameninţările hibride, dezinformarea, manipularea, propagandă etc., asupra cărora se adresează SSI **nu au fost diminuate**.

Se atestă o înţelegere a problemelor de securitate informaţională din partea reprezentanţilor insitituţiilor de drept public şi privat, cu identificarea coerentă a vulnerabilităților şi a riscurilor pe anumite domenii, **ceea ce validează unii indicatori de progres,** dar care nu s-au dezvoltat în **forme integrate şi transectoriale** de abrodare.

Majoritatea instituţiilor responsabile şi partenere raportează acţiuni implementate, care au o perioadă de realizare alta decît 2019, scadente din 2019 sau cu termen permanent, ceea ce generează o necesitate **de reevaluare şi revalidare a acestor acţiuni la o etapă ulterioară** şi denotă **lipsa de consecutivitate în măsurile ce se impun conform** prevederilor Planului de acțiuni al SSI la etapa de moment.

Unele realizări, raportate de autorităţi, se pliază pe cadrul de competență instituțională și activitatea acestora în mod ordinar. Din această perspectivă, devine important să distingem cerineţe Planului de acțiuni al Strategiei, unde se face trimitere la obiective și acțiuni concrete orientate pe probleme de securitate și activitatea autorităţilor pe atribuţii şi competenţe.

În rapoartele prezentate pe activități nu se observă o interacțiune între instituțiile responsabile și cele partenere, fapt ce denotă lipsa de coeziune interinstituțională, deși problemele de securitate informațională au o geneză transectorială și pentru soluționarea lor sunt necesare remedii complexe, cu aplicabilitate directă în toate domeniile centrale și de către toate instituțiile de drept public și privat, componente ale societății informaționale.

Evaluarea de față oferă un cadru de reconstrucție ce poate fi folosit ca bază de fundamentare şi o perspectivă asupra modului în care se poate propune reconfigurarea sistemului de raportare şi monitorizare.

Devine imperativ ca rezultatele acţiunilor scadente în anul 2019 şi a celor cu termen permanent de implementare prezentate de instituțiile responsabile și cele

partenere, urmează a fi examinate în cadrul şedinţelor Grupului de lucru din cadrul SIS și reprezentanții desemnați de fiece instituție inclusă în Plan.

Persoanele responsabile din cadrul instituțiilor de drept public și privat în cel mai responsabil mod urmează să racordeze acțiunile întreprinse la nivel instituțional cu obiectivele Strategiei și prevederile Planului de acțiuni.

Totodată, devine recomandabil ca membrii Grupului de monitorizare din cadrul SIS, pentru eficientizarea gradului de implementare al Strategiei și Planului de acțiuni al SSI 2019-2024 să evalueze la nivelul instituțiilor de drept public și privat modul de implementare a priorității 3. din Pilonul I *(Consolidarea cooperării dintre CERT-ul naţional, CERT Gov şi CERT-urile private)*.

Un rol important întru realizarea Strategiei și a implementării acțiunilor din Plan îl joacă ministerele incluse ca responsabile sau ca partenere, în special la promovarea actelor normative elaborate.

Mai cu seamă, importanța acestor ministere, precum MAI, MF, MEI, MJ sau MA devine relevantă în cazul proiectelor de acte normative elaborate de autoritățile care nu au drept de inițiativă legislativă, dar sunt responsabile de anumite acțiuni din Planul de implementare al SSI 2019-2024.

De menționat, că în cazul când Cancelaria de Stat va desemna un minister pentru promovarea actelor normative ce vor fi elaborate de instituțiile de drept public și privat pentru a fi promovate spre adoptare la nivel de Guvern sau Parlament, ministerul respectiv va devini coresponsabil la implementarea unei sau altei acțiuni și va raporta corespunzător acțiunile care au fost întreprinse de la etapa desemnării de către Cancelaria de Stat.