R A P O R T

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

Perioada de raportare: 2020

SERVICIUL DE INFORMAȚII ȘI SECURITATE

Elaborat – martie 2021

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

REZUMAT EXECUTIV

Raportul de monitorizare a procesului de implementare a Strategiei securităţii informaţionale pentru anii 2019-2024 *(în continuare SSI/Strategie)* constitue o evaluare complexă a acţiunilor executate şi rezultatele înregistrate pe parcursul anului 2020 la realizarea Planului de acţiuni al Strategiei, adoptat prin Hotărîrea Parlamentului nr. 257 din 22.11.2018.

Serviciul de Informaţii şi 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 drept autoritate coordonatoare şi responsabilă de monitorizarea şi coordonarea procesului de implementare a Planului de acţiuni.

Strategia securității informaționale a Republicii Moldova pentru anii 2019 – 2024 are scopul de a integra juridic și sistemic domeniile prioritare cu responsabilităţi şi competenţe în asigurarea securităţii informaţionale la nivel naţional, pilonii de bază fiind reziliența cibernetică, pluralismul multimedia şi convergenţa instituţională în materie de securitate, destinate protejării suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

Planul de acţiuni pentru implementarea Strategia securității informaționale *(în continuare Plan)* include un complex de acţiuni, ce are scopul realizării obiectivelor 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 capacităților instituționale în combaterea criminalității informatice;
9. Efectuarea unor cercetări ştiinţifice aplicative în domeniul securităţii informaţionale;
10. Dezvoltarea capacităţilor de reziliență cibernetică și 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 publicaţiilor periodice, al agenţiilor de presă și al altor subiecți care activează în spațiul media din Internet;
4. Asigurarea transparenței financiare în activitatea autorităților administraţiei publice, a asociațiilor obștești şi 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 și combaterii criminalității informatice

Pe parcursul anului 2020, care este al doilea an de realizare a HP nr. 257, Serviciul de Informații și Securitate, de comun cu instituțiile responsabile, au realizat mai multe acțiuni organizatorice orientate la implementarea Planului, în special:

a) Au avut loc discuții între reprezentanții Secretariatului Grupului de monitorizare și persoanele responsabile desemnate de instituțiile vizate pentru implementarea acțiunilor din Plan privitor la acțiunile de competență prevăzute în Planul de acțiuni;

b) În cazul unor instituții au fost elaborate/revizuite planurile instituționale detaliate, în conformitate cu prevederile Planului 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;
- ❖ Reflectarea indicatorilor de impact în al doilea an de implementare, conform aprecierilor insitituţiilor responsabile şi a indicatorilor prezentaţi în rapoarte;
- ❖ Identificarea 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 a Parlamentului RM, de organizaţiile neguvernamentale, experţii naţionali şi internaţionali din domeniul de securitate.

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

DESCRIEREA PROGRESELOR ACȚIUNILOR REALIZATE ÎN PERIOADA ANULUI 2020

Capitolul include progresul realizării acțiunilor scadente din anul 2020 şi a celor cu termen permanent de implementare, pe fiecare palier și puncte din Plan ce corespund obiectivelor din partea descriptivă a Strategiei și informațiilor 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 entității 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 autoritățile 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 2019-2021, cu verificarea anuală a indicatorilor de progres	Parțial realizat

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

La data de 20 februarie 2020, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” (STISC) a organizat şedinţa grupului de lucru, format din reprezentanţii instituţiilor responsabile, în cadrul căreia au fost examinate prevederile obiectivului 1, acţiunea 1 din Plan. În context, participanţii s-au expus cu privire la mecanismul de desemnare a entităţii care va exercita rolul de Centru naţional de reacţie la incidente de securitate cibernetică şi instituţiile responsabile în realizarea acestui obiectiv, cât și la stabilirea interacţiunii Centrului guvernamental de reacţie la incidente de securitate cibernetică cu Centrul naţional de reacţie la incidente de securitate cibernetică.

Astfel, crearea unui CERT naţional şi respectiv, elaborarea cadrului legal ce ar reglementa activitatea acestuia, este un proces complex, care necesită respectarea prevederilor Legii nr. 100 din 22.12.2017 cu privire la actele normative. Procesul 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-ului naţional.

În cadrul şedinţei, reprezentanţii instituţiilor responsabile s-au pronunțat inclusiv pentru atragerea expertizei externe în efectuarea analizei de impact la proiectul de lege menționat, opţiunile, costurile, model optim de funcţionare a CERT-lui naţional, delimitarea atribuţiilor, raportarea incidentelor, desemnare şi interacţiune cu furnizorii de servicii digitale şi operatorii de infrastructură critică, sub aspectul asigurării securităţii cibernetice a sistemelor informaţionale utilizate.

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	Anul 2019	Realizat

Instituţia responsabilă: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică, Cancelaria de Stat.*

În corespundere cu prevederile Hotărârii de Guvern nr. 482 din 08.07.2020 *(Monitorul Oficial Nr. 180-187 din 17.07.2020)* privind aprobarea unor măsuri necesare privind asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr. 414/2018, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" este desemnat în calitate de Centru guvernamental de reacţie la incidente de securitate cibernetică (CERT Gov).

Corespunzător, STISC, în calitate de Centru guvernamental de reacţie la incidente de securitate cibernetică, va constitui punctul unic de contact şi de raportare a incidentelor de securitate cibernetică, pentru structurile de tip CERT departamentale a Guvernului. De asemenea, prezenta hotărâre delimitează competenţele şi responsabilităţile entităţilor publice în domeniul securităţii cibernetice, inclusiv mecanismele necesare implementării acestora, în scopul menţinerii unui spaţiu cibernetic deschis, sigur şi securizat la nivel guvernamental.

În acest context, misiunea CERT Gov, presupune oferirea consultanţei şi elaborarea recomandărilor de soluţionare şi prevenire a incidentelor de securitate cibernetică, precum şi remiterea avertizărilor operative către entităţile publice supuse riscurilor şi organele competente.

Respectiv, sub egida STISC a fost elaborat proiectul Hotărârii de Guvern pentru crearea CERT GOV, care a fost definitivat în versiune finală în luna decembrie 2019, fiind discutat și la ședința secretarilor generali. Actualmente, proiectul HG urmează a fi introdus pe agenda ședințelor Guvernului pentru a fi aprobat.

Potrivit proiectului în cauză de HG, STISC 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. La fel, proiectul HG defineşte atribuţiile, principiile de organizare şi funcţionare a CERT GOV, fiind deja avizat și urmând procedura de aprobare a acestuia de către Guvern.

Nr ***(din Plan)***	**Acţiunea**	**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	În proces de realizare

Instituţia resonsabilă: *Ministerul Economiei şi Infrastructurii.*

În temeiul art. 23 din Legea nr. 100/2017 cu privire la actele normative, a fost inițiată procedura de elaborare a analizei preliminare de impact la proiectul de lege de transpunere în legislația națională a Directivei UE 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva NIS).

Concomitent, în procesul de dialog cu partenerii de dezvoltare, a fost solicitată asistența tehnică pentru elaborarea proiectului de lege privind securitatea rețelelor și sistemelor informaționale, având ca scop conformarea acesteia la standardele internaționale.

De menționat că în anul 2020, Comisia Europeană a lansat proiectul *Cybersecurity East*, un obiectiv al căruia este asistarea țărilor Parteneriatului Estic în transpunerea Directivei NIS. Din cauza situației pandemice, implementarea operațională a proiectului a fost transferată pentru anul 2021.

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 Agenției de Guvernare Electronică (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 AGE a intrat domeniul auditului de securitate cibernetică. Astfel, întru realizarea competenței respective, AGE a finalizat în anul 2020 auditele 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. Ministerul 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 menționate supra 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. Astfel, mai multe instituții au informat

AGE privind statutul elaborării planului de înlăturare a neajunsurilor depistate (ASP, MEI, MECC, MSMPS, etc.) Raportul consolidat privind rezultatele auditului a fost remis autorităților abilitate în luna aprilie 2020.

Agenția Servicii Publice – pentru implementarea rezultatelor auditului de securitate cibernetică, s-a aprobat Ordinul ASP nr. 300 din 01.07.2020 cu privire la asigurarea Planului de măsuri pentru implementarea recomandărilor în urma auditului de securitate cibernetică. Prin ordinul menționat s-au aprobat:

- Planul de măsuri pentru realizarea recomandărilor auditului de securitate cibernetică al Agenției Servicii Publice privind implementarea HG nr. 201 din 28.03.2017, efectuat de Agenția de Guvernare Electronică;
- Lista persoanelor din subdiviziunile ASP, responsabile în limitele competențelor, pentru executarea măsurilor prevăzute în plan.

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 prioritare pentru prevenirea şi suprimarea ameninţărilor respective	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Agenţia de Guvernare Electronică*.

În scopul implementării acțiunii a fost efectuat auditul de securitate cibernetică privind implementarea Cerințelor minime obligatorii de securitate cibernetică.

Adițional, pe Platforma guvernamentală de instruire la distanță (e-Learning) au fost dezvoltate 4 module de instruire electronică Moodle pentru diferite roluri în instituțiile publice (manageri, utilizatori, administratori IT, dezvoltatori) pentru a:

- consolida cunoștințele și abilitățile de bază în domeniul informațiilor și principiilor de securitate cibernetică, cât și cele mai bune practici în rândul autorităților publice centrale;
- crea o cultură a securității între autoritățile publice centrale și continuarea sporirii capacităților în domeniul securității cibernetice.

Cele 4 module dedicate securității cibernetice sunt:

1. Instruire generală privind securitatea cibernetică;
2. Instruire în domeniul securității cibernetice pentru manageri;
3. Instruire privind securitatea cibernetică pentru administratorii de sistem;
4. Instruire în domeniul securității cibernetice pentru dezvoltatori.

Modulele de instruiri enunțate au fost pilotate cu ASP și alte autorități, iar la etapa curentă structura și conținutul lor se ajustează conform propunerilor participanților la instruiri.

Agenția Servicii Publice – Planul de măsuri pentru realizarea recomandărilor auditului de securitate cibernetică al ASP privind implementarea HG nr. 201 din 28.03.2017, efectuat de AGE prvede tratarea riscurilor reziduale de nivel „înalt” și „mediu” pe următoarele domenii pentru îmbunătățiri:

- Organizarea sistemului intern de securitate cibernetică/informațională;
- Cerințe minime obligatorii de securitate cibernetică de nivelul 2;

- 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 securității spațiului informațional-cibernetic și investigarea criminalității informatice**			
2/3	Elaborarea mecanismelor și a metodelor de prevenire și contracarare a pericolelor în spațiul cibernetic, generate de serviciile informaționale prestate de către persoanele fizice și juridice	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Serviciul de Informații și Securitate.*

Pe parcursul perioadei de referință, Serviciul de Informații și Securitate a recepționat și a analizat propunerile autorităților publice – MEI, MAI, ANRCETI, cu referință la Proiectul de lege pentru modificarea art. 64 din Legea 241/2007 privind comunicațiile electronice, în scopul realizării obiectivului privind asigurarea securității și integrității rețelelor de comunicații electronice, precum și eliminării sau diminuării numărului abonaților serviciilor de comunicații electronice depersonalizați. Proiectul a fost remis Cancelariei de Stat pentru promovare, care însă nu a fost promovat, din motivul lipsei analizei impactului de reglementare. Actualmente, experții Serviciului identifică soluții pentru elaborarea și promovarea unui nou proiect de lege pe aspectele menționate supra.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securității spațiului informațional-cibernetic și investigarea criminalității informatice**			
2/4	Identificarea unui mecanism legal de interacțiune între autoritățile publice competente și persoanele fizice și juridice, indiferent de tipul de proprietate, în vederea acordării de către acestea a accesului la codul-sursă al aplicațiilor elaborate, comercializate și distribuite pentru autoritățile publice	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituții responsabile: *Serviciul de Informații și Securitate, Ministerul Afacerilor Interne.*

În perioada de raportare, ofițerii SIS au continuat studierea cadrului normativ european în vederea acordării accesului la codul-sursă al aplicaţiilor elaborate, comercializate şi distribuite pentru autorităţile publice.

Pentru implementarea unui nivel superior de securitate în cadrul infrastructurii naționale Centrul unic de certificare a Guvernului – PKI *(Public Key Infrastructure)*, a fost modificat cadrul normativ prin care prestatorii de servicii în domeniul semnăturii electronice au fost obligați să prezinte codul sursă pentru produsele de program ce urmează a fi avizate spre utilizare.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
2/5	Coordonarea cu Centrul Național pentru Protecția Datelor cu Caracter Personal a măsurilor de protecție a datelor cu caracter personal, care să asigure aplicarea principiului protecției datelor începînd de la conceperea acestora și	Perioada 2019-2020, cu verificarea anuală a indicatorilor de progres	Realizat

	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	

Instituția responsabilă: *Autorităţile administraţiei publice.*

Pe parcursul anului 2020, **Centrul Naţional pentru Protecţia Datelor cu Caracter Personal** (CNPDCP) a avizat **65** proiecte de acte normative prezentate spre examinare de către autorităţile administraţiei publice.

În cadrul **Serviciului de Informaţii şi Securitate** sunt respectate prevederile Ordinului Directorului SIS nr. 50/2015 cu privire la aprobarea Politicii de asigurare a securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale ale SIS al RM, cadrul normativ intern fiind în corespundere cu legislația în vigoare.

Agenția Servicii Publice – 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. Actualmente, sunt înregistrate 13 sisteme informaționale ce prelucrează date cu caracter personal, iar 3 sisteme sunt în proces de coordonare.

Ministerul Finanțelor – în anul 2020, conform prevederilor Legii nr.133/2011 privind protecţia datelor cu caracter personal, Ministerul Finanțelor, în coordonare cu CNPDCP a elaborat:

- Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a resurselor umane;
- Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă.

În context, a fost inițiat procesul de notificare și înregistrare în Registrul de evidenţă a operatorilor de date cu caracter personal a sistemelor informaționale gestiunate de minister (Ordinul MF nr. 44 din 13.03.2020) și identificate sistemele informaționale (SIA) și registrele aflate la balanța Ministerul Finanțelor, care se bazează pe prelucrarea datelor cu caracter personal și care au fost aprobate prin Registrul de evidență a sistemelor informaționale electronice (SIA) și registrele electronice/ologrefe în care se prelucrează date cu caracter personal gestionate de Ministerul Finanțelor.

La fel, a fost asigurată elaborarea Regulamentului privind prelucrarea și protecția informațiilor ce conțin date cu caracter personal în SIA „Registrul electronic al cererilor de acordare a compensațiilor” în cadrul Programului „Prima Casă” (Ordinul MF nr. 119 din 23.09.2020). Totodată, la CNPDCP a fost depusă notificarea cu nr. 201009CI1216 din 09.10.2020 privind înregistrarea în Registrul de evidenţă a operatorilor de date cu caracter personal a SIA „Registrul electronic al cererilor de acordare a compensațiilor” în cadrul Programului „Prima Casă”.

Serviciul Fiscal de Stat – urmare a depunerii la data de 11.11.2019, a notificării nr. 1573469322419 de înregistrare în calitate de operator la CNPDCP,

Serviciul Fiscal de Stat a fost înregistrat în Registrul de evidență al operatorilor de date cu caracter personal (nr. 0000118-004 din 06.02.2020). În acest context, a fost aprobat Ordinul SFS nr. 138 din 28.02.2020 privind actualizarea Regulamentului privind prelucrarea și protecția informațiilor ce conțin date cu caracter personal în cadrul SFS.

Inspecția Financiară – conform acordului încheiat cu CNPDCP, Inspecţia Financiară este operator autorizat pentru prelucrarea datelor cu caracter personal, nr. 0000112. Astfel, în scopul exercitării atribuțiilor funcționale, instituția poate utiliza 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.

Pe parcursul anului 2020 au fost aprobate ordine cu privire la modul de utilizare a sistemelor informaționale, după cum urmează:

- Ordinul IF nr.15 din 04.12.2020 cu privire la aprobarea Regulamentul privind supravegherea prin mijloace video şi asigurarea securităţii informaţiilor ce conţin date cu caracter personal din cadrul Inspecției Financiare, care are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei, precum şi stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate, urmărind asigurarea protecţiei drepturilor şi libertăţilor fundamentale ale persoanei fizice, conform legislației în vigoare;
- Ordinul IF nr.17 din 04.12.2020 cu privire la aprobarea Politicii de Securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Inspecția Financiară.

MECC – a fost elaborată și aprobată Hotărârea Guvernului nr. 601/2020 cu privire la concepția Sistemului informațional de management în educație. Centrul Național pentru Protecția Datelor cu Caracter Personal a participat la avizarea proiectului hotărârii respective, iar propunerile acestuia au fost acceptate și incluse în actul normativ.

Totodată, pe parcursul lunilor august-octombrie 2020, au fost desfășurate ședințe de lucru cu Centrul Național pentru Protecția Datelor cu Caracter Personal cu privire la utilizarea sistemelor externe în procesul educațional și pașii necesari pentru a proteja elevii în mediul online.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
3/1	Delimitarea şi atribuirea rolurilor şi a responsabilităţilor privind apărarea cibernetică ce revin sistemului de organe ale securităţii statului şi sistemului naţional de apărare	Perioada 2019-2020, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituții responsabile: *Ministerul Apărării, Serviciul de Informații și Securitate.*

În conformitate cu obiectivul acțiunii, este în proces de elaborare proiectul Strategiei de apărare cibernetică a Republicii Moldova.

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	Parţial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate*

Pe parcursul anului 2020, Serviciul de Informații și Securitate a acordat suport Ministerului Apărării și Administrației Naționale a Penitenciarelor în vederea elaborării și stabilirii cadrului normativ ce ține de cerințele minime de securitate a sistemului informatic și de comunicații, creării structurii de securitate pentru tehnologia informației și a comunicațiilor (SSTIC).

Concomitent, în perioada de referință experții SIS au perfectat și remis **34 de 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.

La fel, în 2020, specialiștii SIS au studiat practica UE privind cerințele de securitate pentru sisteme informaționale la prelucrarea informației clasificate și în acest sens au fost formulate propuneri de modificare a cadrului normativ național (HG 1176/2010) pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice.

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.*

Experții SIS au participat la elaborarea ***Conceptului tehnic pentru sistemul de comunicații guvernamentale***, care ulterior a fost aprobat.

Concomitent, a fost elaborat și actul normativ intern cu privire la modul de sigilare a echipamentelor aferente tehnologiilor informaționale și comunicațiilor electronice din cadrul SIS al RM.

În anul 2020, Serviciul a efectuat controale privind respectarea regimului secret a sistemelor IT în cadrul autorităților publice. Ca efect, au fost revizuite actele normative interne care reglementează securitatea informațională, secretul de stat și funcționarea sistemelor pentru determinarea nivelului de corespundere cu actele normative naționale și cu standardul ISO 27000.

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-	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

	organizatorice întreprinse pentru asigurarea securităţii cibernetice		

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În anul de raport de către SIS au fost realizate 2 misiuni de audit intern a sistemelor speciale de comunicații:

- a fost efectuată evaluarea vulnerabilităților în scopul identificării lacunelor sistemului nou creat pentru Direcția Secretariat;
- a fost efectuat auditul pentru un sistem special de comunicații, fiind elaborat raportul de audit.

În context, specialiștii SIS au analizat rapoartele de audit parvenite de la alte instituții, fiind prezentate concluziile și propunerile de rigoare conducerii Serviciului în acest sens.

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	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În anul 2020 a fost revizuit ***Regulamentul cu privire la telecomunicațiile speciale***, aprobat prin Hotărârea Guvernului nr. 735/2002, fiind propusă includerea în Regulament a normei care va asigura obținerea gratuită a liniilor de telecomunicații de la *„Moldtelecom”*. La fel, Serviciul a avizat proiectul Hotărârii Guvernului pentru modificarea punctului 26 din ***Regulamentul cu privire la sistemele speciale de telecomunicații ale Republicii Moldova***, aprobat prin Hotărîrea Guvernului nr. 735/2002.

Concomitent, SIS a elaborat proiectul de Lege pentru modificarea art. 64 din ***Legea comunicațiilor electronice nr. 241/2007***, în scopul realizării obiectivului privind asigurarea securității și integrității rețelelor de comunicații electronice precum și eliminării sau diminuării numărului abonaților serviciilor de comunicații electronice depersonalizați.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
4/5	Stabilirea măsurilor de asigurare a protecției datelor cu caracter personal în contextul asigurării securității cibernetice	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Parțial realizat

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

Centrul Naţional pentru Protecţia Datelor cu Caracter Personal a promovat în anul 2020 proiectul de lege elaborat de CNPDCP privind protecţia datelor cu caracter personal, ce a fost votat în prima lectură de către Parlamentul RM la 30 noiembrie 2018. Proiectul respectiv prevede reglementări cu privire la măsurile de

asigurare a protecţiei datelor cu caracter personal în cadrul persoanelor juridice de drept public şi de drept privat.

Procuratura generală a avizat proiectul de modificare a HG nr. 735 din 11.06.2002 cu privire la sistemele speciale de telecomunicaţii ale Republicii Moldova.

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	Realizat

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

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

MAEIE a elaborat proiectul HG cu privire la modificarea Hotărârii Guvernului nr. 697/2017 cu privire la organizarea şi funcţionarea Ministerului Afacerilor Externe şi Integrării Europene, prin care se propune crearea Secţiei securitate şi integritate. La 10.12.2020 Cancelaria de Stat a restituit proiectul pentru definitivare. Acesta urmează a fi promovat pentru aprobare pe parcursul anului 2021.

Nr *(din Plan)*	Acțiunea	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

Instituția responsabilă: *Serviciul de Informaţii şi Securitate.*

În perioada de referință de către experții SIS au fost examinate dispozitivele speciale care urmează a fi utilizate în infrastructura națională **Centrul unic de certificare a Guvernului** – PKI *(Public Key Infrastructure)*.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
5/2	Dezvoltarea sistemelor de monitorizare a importului mijloacelor de protecţie a informaţiei	Perioada 2020-2023, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informaţii şi Securitate.*

În cadrul Grupului de lucru, creat prin Ordinul Directorului SIS nr. 36 din 13.04.2017, au fost examinate o serie de solicitări privind mijloacele tehnice, care urmau a fi importate de agenți economici *(7/2-1655 din 19.06.2020)*.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Urmare a evaluării cadrului normativ European care reglementează cerințele pentru serviciile de certificare a cheilor publice *(Regulamentul UE 910/2014, Decizia UE 2015/1505, Decizia UE 2015/1506, Decizia UE 2016/650)* și a elaborării de către SIS a proiectului Legii pentru transpunerea Regulamentului UE 910/2014, expediat Cancelariei de Stat, continuă procesul de elaborare a analizei impactului sectorial al acestuia.

Nr *(din Plan)*	Acțiunea	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 progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de referință, a fost realizată acreditarea prestatorului de servicii de certificare din cadrul IP STISC. S-a desfășurat controlul în domeniul semnăturii electronice, fiind elaborat avizul privind respectarea de către prestator a cerințelor în domeniul semnăturii electronice.

A fost realizată certificarea cheii publice a prestatorului serviciilor de certificare de nivelul doi din cadrul IP STISC, cu utilizarea unei noi funcții, care a permis extinderea termenului de valabilitate a cheii private și publice a utilizatorului semnăturii electronice de la 1 an la 2 ani.

În procesul de monitorizare permanentă a activității prestatorilor de servicii de certificare în scopul depistării încălcărilor actelor normative în domeniul semnăturii electronice, SIS a constatat **2 încălcări**, ce țin de utilizarea contrar prevederilor cadrului normativ a soluției de creare/verificare a semnăturii electronice fără deținerea avizului organului competent. În rezultat, prestatorul a fost avertizat privind necesitatea respectării cadrului normativ în vigoare.

Concomitent, a fost remisă atenționarea autorităților publice și a prestatorilor de servicii de certificare a cheilor publice, privind necesitatea respectării procedurii de identificare a solicitantului serviciilor.

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.*

Pe parcursul anului 2020 au fost instruiți **32** de angajați ai Ministerului Afacerilor Interne în cadrul a 32 de cursuri și webinare.

În perioada de raport, ofițerii Direcției investigare infracțiuni informatice a INI al IGP al MAI au participat și acordat suport Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism din România la destructurarea grupului infracțional organizat internațional intitulat „Pentaguard", specializat în săvârșirea infracțiunilor de operațiuni ilegale cu dispozitive și programe informatice, acces ilegal la un sistem informatic, alterarea integrității datelor informatice și fals informatic.

Procuratura Generală – numărul de procurori din procuraturile specializate și teritoriale specializați în domeniu: 9 persoane; numărul de persoane instruite: 10 persoane; numărul de cauze transmise în judecată: 37 cauze. În perioada anului 2020, de către instanțele de fond au fost pronunțate 28 sentințe de condamnare: 1) Art. 177 CP – 5 sentințe de condamnare și 2) Art. 2081 CP – 22 sentințe de condamnare.

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 Poliției), Procuratura Generală.*

În perioada 15-17.07.2020, 50 de angajați ai Inspectoratelor de poliție teritoriale, inclusiv ofițeri ai Direcției investigare infracțiuni informatice a INI a IGP au participat în regim online, la cursul de formare profesională continuă cu tematica „*Combaterea infracţiunilor cibernetice*", organizat de către Centrul integrat de pregătire pentru aplicarea legii al MAI al RM.

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	Parţial realizat

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

Pe parcursul anului 2020, Direcția investigații infracțiuni informatice a INI a IGP a fost dotată cu echipament și softuri specializate pentru investigarea infracțiunilor informatice în sumă totală 74.446 USD. Activele nemateriale au fost primite cu titlu gratuit din partea Ambasadei SUA în RM.

În perioada de referință Serviciul de Informații și Securitate a realizat măsuri de competență pentru documentarea tentativelor de infectare cu ***cyber threats*** a rețelelor și resurselor IT guvernamentale.

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	Anul 2020	Realizat

Instituția responsabilă: *Ministerul Finanţelor, Ministerul Afacerilor Interne.*

Sistemul actual de salarizare poartă un caracter unitar, transparent, echitabil, nediscriminatoriu, salarizarea proporțională cu contribuția, capabil să reflecte și să remunereze performanța profesională din domeniul de activitate, orientat spre durabilitatea financiară. Totodată, conform prevederilor legislative, Ministerul Finanțelor evaluează sistemic cel puțin o dată la 5 ani funcțiile în sectorul bugetar pentru a elimina eventualele discrepanțe atestate. O astfel de reevaluare este preconizată de a fi realizată pentru anul 2022. Astfel, la acea etapă Ministerul Finanțelor va analiza în complex modificarea condițiilor salariale în sensul asigurării tratamentului egal și a remunerării egale pentru munca de valoare egală, în funcție de disponibilitățile financiare ale bugetului de stat.

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 Poliţiei), Procuratura Generală.*

Pe parcursul perioadei ianuarie-decembrie 2020, Direcția investigații infracțiuni informatice a INI a participat la 15 activități de dezvoltare a capacităților profesionale, dintre care 5 la nivel național și 10 activități internaționale.

În context au fost investigate **43** cazuri, după cum urmează:

-art.208^1 Cod penal (*Pornografia infantile*) – 37 cazuri;
-art.173 Cod penal (*Hărţuirea sexuală*) – 2 cazuri;
-art. 175 Cod penal (*Acţiuni perverse*) – 2 cazuri;
-art.175^1 Cod penal (*Ademenirea minorului în scopuri sexuale*) – 2 cazuri.

Numărul copiilor protejați, precum și celor care beneficiază de asistență - total **15 minori**:

- realizată audierea a 4 minore cu participarea psihologului din cadrul CI „La Strada”;
- organizat un interviu de protecție pentru 8 minori cu participarea psihologului în condiții speciale în incinta CI „La Strada”;

- organizată evaluarea psihologică pentru 3 minore cu participarea psihologului în condiții speciale în incinta CI „La Strada”.

Procuratura Generală – pentru art. 208[1] din Codul penal al Republicii Moldova a fost înregistrat un număr de 45 de cazuri.

Cauze transmise în judecată – 22.

Sentințe de condamnare în număr de 21.

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 Poliţiei), Procuratura Generală.*

Cazuri investigate grooming de către IGP al MAI – 2.

Procuratura Generală – pentru anul 2020 de către instanțele de judecată a fost pronunțată o singură sentință de condamnare în baza art. 173 din Codul penal al Republicii Moldova.

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 Poliţiei), Procuratura Generală.*

Ministerul Afacerilor Interne:

1. Participarea reprezentantului IGP în calitate de invitat-specialist la seminarul instructiv-metodic cu genericul „Bullying-ul - formă de violență în mediul școlar”, desfășurat în cadrul LT „Iuliana Hașdeu”, mun. Chișinău;
2. Participarea reprezentantului IGP în calitate de specialist, la lecția publică în cadrul căreia 30 studenți ai Facultății de Drept din cadrul Universității de Stat din Moldova, au fost familiarizați despre provocările la cercetarea cazurilor de exploatare prin tehnologii informaționale;
3. Participarea reprezentantului IGP în perioada 06-08.11.2020 în calitate de mentor și membru al juriului în cadrul primului Hackathon privind Antitrafic și Siguranța online a copiilor, organizat de OSCE;
4. În perioada de raport pe pagina web a Poliției, precum și pe pagina Facebook au fost plasate 3 comunicate de presă privind prevenirea și combaterea delicvenței juvenile.

Totodată, au fost desfășurate 2 campanii de sensibilizare, după cum urmează:

- În contextul Zilei siguranței pe internet, celebrată în fiecare an în toată lumea la începutul lunii februarie, s-au desfășurat 2 lecții de informare cu caracter preventiv privind siguranța copiilor în mediul online În contextul campaniei menționate nu au

fost implicați careva parteneri. În cadrul campaniei au fost informați aproximativ 300 de copii, în raza mun. Chișinău;

- Participarea în cadrul campaniei organizată de către CNPDCP și IGP, cu genericul „*Protejează-ți copilul în mediul on-line*”, în scopul informării părinților despre riscurile pe care le pot întâlni copiii în mediul online, precum și recomandările care ar exclude aceste riscuri. Campania a fost organizată în incinta DGETS „Botanica” și au participat în jur de 50 părinți. Evenimentul a fost mediatizat atât pe pagina oficială a Poliției, cât și de către mass-media.

Procuratura Generală – la data de 20.10.2020 în cadrul campaniei naționale „*Săptămâna de luptă împotriva traficului de ființe umane*”, în incinta Universității de Stat din Moldova, procurorii au participat la masa rotundă cu genericul „*Traficul de ființe umane comis în mediul online*”, la care au participat mediul academic, practicieni, masteranzi și studenți.

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

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

În scopul combaterii fraudelor săvârșite cu utilizarea mijloacelor de plată electronice, Direcția investigații infracțiuni informatice a IGP permanent efectuează schimb de informații cu Departamentele de securitate ale instituțiilor financiare.

Totodată, la 21.02.2020, reprezentanții IGP au participat la ședința comună cu reprezentanții BNM, pe marginea modificării Acordului privind schimbul de informații între BNM și IGP, cu înaintarea propunerilor privind schimbul de informații de tip nou.

Urmare a examinării oportunității de extindere a spectrului de informații ce constituie obiect al Acordului, părțile au concluzionat, reieșind din complexitatea informației, că furnizarea unor informații suplimentare decât cele prevăzute în formatul actual al schimbului de date, va fi efectuată la necesitatea și cererea expresă a părților, conform prevederilor Acordului (cap. II), fără modificări suplimenatre ale acestuia.

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 privința bancomatelor (ATM-urilor) la nivel de hardware și software	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

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

Reprezentanții IGP al MAI au participat în perioada 15-16.10.2020 la atelierul de lucru și discuții despre fraudele online, veniturile criminalității și mecanismele de

raportare, cu participarea instituțiilor financiare, în special Banca Națională, Serviciul spălarea banilor.

Menționăm că în urma unei colaborări eficiente cu exponenții centrelor de procesare a instituțiilor financiare au fost întreprinse măsuri de prevenire, de blocare a diferitor tranzacții frauduloase, efectuate prin intermediul băncilor comerciale.

Totodată, în scopul promovării unor măsuri de securitate sporită în privința bancomatelor (ATM-urilor) la nivel de hardware și software, băncile au întreprins măsuri privind diminuarea numărului de ATM-uri ce rulează pe sisteme de operare ce nu mai dispun de suport din partea furnizorilor (Windows XP) de la 525 la 428, diminuându-se cu 19%. Adițional, au fost implementate controale ce se referă la instalarea sistemului de securitate specializat pe ATM-uri, revizuirea conturilor de acces și resetarea parolelor de securitate la ATM, implementarea controlului asupra aplicațiilor, asigurarea riscurilor la compania de asigurare, detectarea și prevenirea modificărilor neautorizate, respectarea prevederilor standardelor PCI-DSS.

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	Parțial realizat

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

Analiza datelor privind numărul și valoarea fraudelor înregistrate și raportate în adresa BNM, relevă faptul că pe parcursul anului 2020, fraudele cu cardurile contrafăcute sunt în descreștere în raport cu anii precedenți, fiind înregistrate 8 cazuri în sumă totală de 33.482 lei.

De asemenea, se atestă și o creștere a fraudelor cu carduri pierdute/furate, fiind înregistrate 183 de cazuri la o instituție financiară, în sumă totală de 32.887 lei.

Pe parcursul anului 2020 s-au înregistrat fraude cu utilizarea numărului cardului (*card not present*) – 3000 de cazuri în sumă totală de 2.899.549 lei.

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.*

În perioada de referință a fost creată o rețea de persoane din cadrul subdiviziunilor teritoriale ale IGP, responsabile de domeniul prevenirii și combaterii crimelor cibernetice, inclusiv a exploatării sexuale a copiilor.

Totodată, pe parcursul perioadei de raport în cadrul Direcției de poliție a mun. Chișinău a fost creat Serviciul specializat, responsabil de investigare

infracțiunilor informatice, la fel a fost mărit numărul ofițerilor responsabili de investigarea crimelor informatice din cadrul Direcției investigarea crimelor informatice a INI de la 30 la 35 de salariați.

La fel, a fost creată subdiviziunea specializată – Biroul antitrafic și de inverstigare a crimelor cibernetice din cadrul PCCOCS. A fost creată Secția exercitare a urmăririi penale din cadrul Procuraturii mun. Chișinău Oficiul Principal, a fost aprobat Regulamentul de activitate a Procuraturii mun. Chișinău prin Ordinul Procurorului General nr.74/26 din 31.07.2020. A fost elaborată Dispoziția cu privire la crearea birourilor specializate din cadrul PCCOCS. Ponderea cauzelor penale transmise în instanțele de judecată: 37. Ponderea sentințelor de condamnare: 12.

Pe parcursul perioadei de raportare, în cadrul SIS s-au realizat măsuri pentru consolidarea capacităților operațional-analitice și de asigurare tehnică pe profilul asigurării securității cibernetice și combaterii criminalității informatice.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
9/2	Crearea unei baze de date naţionale privind evoluţia fenomenului criminalităţii informatice	2022, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Procuratura Generală, Serviciul de Informatii și Securitate, Ministerul Afacerilor Interne.*

În perioada de referință a fost inițiat procesul de creare a unei baze de date naționale privind fenomenul criminalității informatice.

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 (Serviciul Tehnologia Informației).*

Actualmente, 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 în anul 2020.

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 „Programul național în domeniile cercetării și inovării pentru anii 2020-2023 și a Planului de realizare a acestuia”, aprobat prin Hotărârea Guvernului nr. 381/2019, Ministerul Educației, Culturii și Cercetării a stabilit prioritatea strategică „Competitivitate economică și tehnologii inovative” cu direcția strategică de cercetare „Tehnologia informației și dezvoltare digitală” pentru următorii 4 ani.

Nr ***(din Plan)***	**Acțiunea**	**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 modem. 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 17-18 februarie 2020, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” în parteneriat cu I.P. „Agenţia de Guvernare Electronică” şi „Academia de e-Guvemare” din Estonia au organizat Workshop-ul „Gestiunea Incidentelor Cibernetice”, pentru specialişti TI şi responsabili de securitatea cibernetică şi/sau informaţională din cadrul instituţiilor publice şi private. Workshop-ul a avut drept scop, analiza tendinţelor, ameninţărilor şi vulnerabilităţilor prezente în spaţiul cibernetic. Sub ghidarea experţilor, participanţii au examinat taxonomii comune pentru descrierea incidentelor şi cele mai bune metode de identificare şi investigare a acestora, inclusiv tehnici de contracarare şi răspuns, practici operaţionale, precum şi alte aspecte organizatorice şi juridice. Totodată, pentru participanţi a fost organizat şi un exerciţiu de simulare a unui atac cibernetic, precum şi investigarea acestuia în timp real.

La 27 februarie 2020, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” a desfăşurat o lecţie informativă pentru elevi ai Liceului Teoretic „Gheorghe Asachi” cu genericul „Siguranţa copiilor în mediul Online”. Prin intermediul instruirilor, circa 300 mici exploratori ai lumii virtuale au învăţat cum să utilizeze corect şi sigur telefonul mobil, cum să-şi securizeze informaţiile din dispozitivul inteligent, ce înseamnă o reţea socială şi care sunt recomandările pentru

folosirea acesteia, evitarea comunicării cu persoanele necunoscute, dar şi despre regulile de bază referitoare la furnizarea datelor personale pe Internet. Fiecare elev a primit materiale informative despre cele „8 reguli de siguranţă pe Internet, care trebuie ştiute de fiecare copil” şi un prospect despre Securitatea cibernetică pentru adulţi şi adolescenţi, studierea căror îi poate îndruma şi ajuta în prevenirea riscurilor din mediul Online.

La data de 17 Octombrie 2020, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” în parteneriat cu Universitatea Tehnică a Republicii Moldova a organizat tradiţionalul concurs. Capture the Flag (CTF) în vederea susţinerii tuturor tinerilor talentaţi şi pasionaţi de domeniul IT şi schimbului de bune practice alături de specialiştii angrenaţi în eforturile de a asigura securitatea cibernetică. Ediţia din anul 2020, din cauza pandemiei şi situaţiei epidemiologice din ţară, concursul s-a desfăşurat strict în mediul online. Chiar şi aşa, competiţia şi-a păstrat formatul, regulile şi probele concursului fiind pe măsura aşteptărilor.

În perioada 25 - 27 Noiembrie 2020, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” a organizat cea de-a 8-a ediţie Moldova Cyber Week 2020, în format online, cu genericul „Dezvoltarea unei infrastructuri puternice de securitate cibernetică în noile condiţii de normalitate”. Evenimentul online reprezintă o platformă de discuţii pentru specialişti locali şi internaţionali în domeniu, oferind numeroase oportunităţi de cunoaştere, schimb de idei şi experienţe, colaborări de succes, pentru identificarea unor soluţii inovatoare şi eficiente care ar putea fi integrate în strategiile locale şi globale. Evenimentul se desfăşoară sub patronajul Guvernului Republicii Moldova, fiind organizat de I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” şi Universitatea Tehnică a Moldovei cu sprijinul Uniunii Internaţionale pentru Comunicaţii şi Consiliul Europei. Peste 40 de experţi în domeniu s-au întrunit online alături de oficiali de rang înalt, reprezentanţi ai misiunilor diplomatice, profesionişti locali şi internaţionali din peste 12 ţări precum: Australia. România, SUA, Elveţia, Israel, Ucraina, Spania, Rusia şi altele.

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.

Astfel, 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 obiect 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 a fost axată activitatea I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”.

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.*

În cadrul Moldova Cyber Week 2020, cu implicarea experţilor în domeniu au fost organizate o serie de Webinare practice, la care au participat peste 200 de specialişti în domeniu din sectorul public, privat şi mediul academic, principalele subiecte de interes sunt:

Webinar: Identificarea ameninţărilor si răspunsul la incidente. În cadrul acestui webinar, participanţii din sectorul public, privat, mediul academic, precum şi alţi invitaţi din străinătate, au fost instruiţi despre tehnicile şi metodele utilizate pentru răspunsul la incidentele cibernetice, care sunt cheile pentru identificarea indicatorilor malware şi a tiparelor de activitate pentru a genera informaţii precise privind ameninţările. Aceste date pot fi utilizate ulterior pentru a detecta intruziunile actuale şi viitoare de către echipele de răspuns la incidente cibernetice. Sesiunea a acoperit elementele fundamentale ale identificării şi analizei ameninţărilor cibernetice şi se referă la aspect precum: planificarea unui program de analiză în propriul mediu; modul de identificare, definire şi execuţie a unei misiuni de acest gen, utilizarea instrumentelor oportune pentru investigarea ameninţărilor.

Webinar: Platforma Cisco SecureX. În cadrul acestui webinar, expertul CISCO a oferit o abordare tehnică pentru a proteja infrastructura critică, explicând modul în care Platforma Cisco SecureX reduce radical timpul de staţionare a ameninţărilor cibernetice şi volumul sarcinilor executate de persoană pentru a menţine infrastructura organizaţiei conformă şi a contracara eventualele ameninţări. Platforma Cisco SecureX reprezintă o soluţie ce poate fi conectată la întreaga infrastructură de securitate a unei organizaţii maximizând eficienţa operaţională cu fluxuri de lucru automatizate.

Webinarz: Securitatea SCADA si Sisteme de control industrial (ICS). În cadrul webinarului "Principiile directoare de securitate SCADA" s-a desfăşurat un exerciţiu practic cu privire la diferite tipuri de provocări de securitate la care sunt expuse sistemele SCADA, printre care pierderea autorizaţiei, utilizatori neprivilegiaţi, interceptări şi intruziuni.

Webinar: Managementul riscurilor de securitate în era informaţiei. În cadrul acestui webinar complex, experţi căruia au împărtăşit tehnici si metode de implementare, menţinere şi auditare a sistemelor de management al securităţii informaţionale şi al sistemelor de calitate, de gestiune a proiectelor de securitate cibernetică, precum şi modalităţile de depistare a ameninţărilor informaţionale.

Webinar: îmbunătăţirea abilităţilor de prevenire a ameninţărilor, utilizând regulile Yara. în cadrul acestui webinar s-a desfăşurat un exerciţiu practic în care a relatat şi demonstrat practicile de detectare, neutralizare şi răspuns la ameninţările avansate persistente (APT) utilizând regulile YARA.

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 vederea fortificării şi consolidării securităţii cibernetice, I I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetica' în colaborare cu Centrul pentru Combaterea Crimelor Informatice a Inspectoratului Naţional de Investigaţii, au organizat şi desfăşurat la 6 noiembrie 2020 o şedinţă de instruire online, în aspecte ce vizează unele elemente de securitate cibernetică în procesul implementării programelor cu finanţare externă, destinată funcţionarilor autorităţilor publice.

În cadrul şedinţei, au avut loc discuţii pe marginea înşelătoriilor frauduloase şi evitării compromiterii e-mail-urilor, mesajelor de phishing, apelurilor de asistenţă false şi alte înşelătorii pe diverse dispozitive. De asemenea, au fost abordate şi subiecte precum conceptul de layring, tipurile de ameninţări cibernetice, atacuri de tip scam, în urma cărora au fost identificate şi propuse măsuri de securitate şi recomandări de bune practici.

În contextul *Lunii europene a securităţii cibernetice*, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" s-a alăturat campaniei organizate de ENISA prin elaborarea materialelor informative despre măsurile de securitate împotriva ameninţărilor din mediul online pentru autorităţile publice. În acest sens, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" se autosesizează şi se obligă să stabilească o cultură a conştientizării securităţii cibernetice, care pune accent pe securitate ca un standard pentru o instituţie sau o organizaţie de succes, oferind recomandări şi măsuri de securitate în vederea reducerii numărului de atacuri cibernetice.

Răspuns rapid la un atac cibernetic este la fel de importantă precum stabilirea şi implementarea unei strategii de reacţie pentru a preveni o ameninţare sau un potenţial incident de securitate cibernetică. Elaborarea eronată a planului de răspuns la incidentele cibernetice poate conduce în cazurile gestionării incorecte la un rezultat final ce poate afecta cu o severitate mai ridicată resursa, decât riscul inerent al incidentului. Drept urmare, pentru a ajuta utilizatorii vigilenţi să identifice cu precizie eventualele incidente cibernetice şi să fie pregătiţi să acţioneze prompt şi corect pentru ele, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" prezintă spre consultare un Set informativ despre atacurile de tip phishing şi un Ghid de bune practici privind securitatea cibernetică.

Nr *(din Plan)*	**Acţiunea**	**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	În proces de realizare

Instituții responsabile: *Agenția Guvernare Electronică.*

În contextul dezvoltării sistemului informațional de învățare la distanță, și în contextul Campaniei de comunicare a AGE, desfășurată cu prilejul a 10 ani de e-Guvernare, la data de 17.11.2020 a fost organizat un eveniment live în cadrul căruia a fost prezentat noul proiect al AGE – Platforma guvernamentală de instruire la distanță *(e-Learning)*. Platforma respectivă urmează a fi mecanismul eficient, fiabil și modern de instruire a angajaților prin crearea, dezvoltarea și punerea la dispoziție online a resurselor de instruire, precum și de acordare a accesului angajaților la informațiile destinate dezvoltării lor profesionale, inclusiv pe aspecte de securitate cibernetică.

Pe platforma menționată, au fost dezvoltate 4 module de instruire electronică Moodle pentru diferite roluri în instituțiile publice (manageri, utilizatori, administratori IT, dezvoltatori) pentru a:

- consolida cunoștințele și abilitățile de bază în domeniul informațiilor și principiilor de securitate cibernetică și cele mai bune practici în rândul autorităților publice centrale;
- crea o cultură a securității între autoritățile publice centrale și continuarea sporirii capacităților în domeniul securității cibernetice.

Cele 4 module dedicate securității cibernetice sunt:

1. Instruire generală privind securitatea cibernetică;
2. Instruire în domeniul securității cibernetice pentru manageri;
3. Instruire privind securitatea cibernetică pentru administratorii de sistem;
4. Instruire în domeniul securității cibernetice pentru dezvoltatori.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I			
Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice			
11/6	Organizarea unor campanii de sensibilizare şi informare privind pericolele din spaţiul cibernetic şi măsurile de protecţie ce pot fi luate de către persoanele fizice şi juridiceşi desfăşurarea atelierelor de lucru în domeniul securităţii cibernetice pentru personalul din sectorul public şi privat deţinători de elemente de infrastructură critică	Perioada 2020-2022, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituţii responsabile: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică.*

În vederea consolidării pregătirii specialiştilor calificaţi în domeniu securităţii cibernetice, I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” a participat ca formator alături de „Centrul de Instruire în Finanţe” şi Universitatea de Stat de Medicină şi Farmacie „Nicolae Testemiţanu”, în cadrul seminarului de instruire cu genericul „Securitate informaţională şi instrumente IT în activitatea auditului intern” organizat pe 11 decembrie 2020 de către Centrul de Tehnologii Informaţionale în Finanţe, în aspecte ce vizează măsurile de asigurare a securităţii cibernetice în activitatea auditului intern.

În cadrul seminarului, au avut loc discuţii despre: cerinţele minime de securitate, măsuri necesare pentru asigurarea securităţii cibernetice în cadrul instituţiilor, rolul şi necesitatea sistemelor de management al securităţii

informaţionale şi a instrumentelor IT în asigurarea securităţii informaţionale. De asemenea, au fost relatate măsuri de securitate şi bune practici, precum şi promovate recomandări şi soluţii oportune pentru lucrul de la distanţă şi gestiunea sarcinilor în cadrul instituţiei.

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	În proces de realizare

Instituţii responsabile: *Ministerul Educaţiei, Culturii şi Cercetării.*

În anul 2020 a fost continuat procesul de elaborare a planurilor de studii şi conţinuturilor pentru unele discipline de nivel de licenţă şi master în domeniul Securităţii informaţiei, fiind acreditate Programele de studii corespunzătoare palierului respectiv.

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*

Din cauza pandemiei de COVID-19, organizarea cursurilor de instruire tematică în domeniul securității cibernetice pentru angajații instituțiilor publice a fost suspendată. În contextul dezvoltării sistemului informațional de învățare la distanță, și în contextul Campaniei de comunicare a AGE, desfășurată cu prilejul a 10 ani de e-Guvernare, la data de 17.11.2020 a fost organizat un eveniment live în cadrul căruia a fost prezentat noul proiect al AGE: Platforma guvernamentală de instruire la distanță (e-Learning).

Platforma respectivă urmează a fi mecanismul eficient, fiabil și modern de instruire a angajaților prin crearea, dezvoltarea și punerea la dispoziție online a resurselor de instruire, precum și de acordare a accesului angajaților la informațiile destinate dezvoltării lor profesionale, inclusiv pe aspecte de securitate cibernetică. Pe platforma menționată, au fost dezvoltate 4 module de instruire electronică Moodle pentru diferite roluri în instituțiile publice (manageri, utilizatori, administratori IT, dezvoltatori) pentru a:

- consolida cunoștințele și abilitățile de bază în domeniul informațiilor și principiilor de securitate cibernetică și cele mai bune practici în rândul APC;
- crea o cultură a securității între autoritățile publice centrale și continuarea sporirii capacităților în domeniul securității cibernetice.

Cele 4 module dedicate securității cibernetice sunt:

1. Instruire generală privind securitatea cibernetică;
2. Instruire în domeniul securității cibernetice pentru manageri;
3. Instruire privind securitatea cibernetică pentru administratorii de sistem;

4. Instruire în domeniul securității cibernetice pentru dezvoltatori.

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	Parțial realizat

Instituții responsabile: *Autoritățile administrației publice.*

În contextul asigurării securității spațiului informațional-mediatic, SIS a identificat sectoare vulnerabile sub aspect de subiecte de interes naţional, pe care este necesară o comunicare strategică cu autoritățile abilitate.

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	În proces de realizare

Instituții responsabile: *Consiliul Audiovizualului.*

În anul de referință, **IP Compania „Teleradio-Moldova”** a pus în sarcina producătorilor de emisiuni TV/Radio controlul obligatoriu al realizării sarcinilor ce se referă la difuzarea informației care:

- conține secrete de stat;
- are drept scop desfășurarea războiului informațional;
- intenționează transmiterea către publicul larg a mesajelor psihologice destructive;
- combate informația despre activitatea organelor extremiste și teroriste, a organizațiilor criminale internaționale, a grupurilor sau persoanelor orientate spre obținerea accesului neautorizat la resursele de rețea și informații.

Prin aplicarea prevederilor actelor normative de uz intern, au fost întreprinse consecvent acțiuni și măsuri de materializare a prerogativelor prevăzute pentru neadmiterea:

- prezentării manipulatorii a informației pe intern, combaterea în emisie a elementelor manipulatorii ale informației în plan extern;
- dezvăluirea scopului real al evenimentelor care ar putea avea un impact negativ în ce privește interesele naționale ale statului;
- combaterea știrilor false care pot genera panică, tensiuni sau conflicte în societate;
- difuzarea materialelor cu caracter extremist, a pornografiei infantile, a mesagelor psihologic destructive, etc.

Informația de acest gen a fost reflectată prin reportaje, interviuri, știri în programele informaționale TV ”Mesager” și Radio “Panorama zilei”, în buletinele de știri difuzate oră de oră, în emisiunile de ciclu cu diverse tematici.

TV Moldova 1 a desfășurat o amplă activitate pentru a asigura o informare corectă și echidistantă a publicului privind cele mai importante evenimente din societate. În anul 2020 s-a insistat pe realizarea unui șir de priorități, printre care:

- informarea și instruirea producătorilor, editorilor și reporterilor privind necesitatea verificării informațiilor din mai multe surse și documentarea judicioasă, astfel încât să fie prevenite știrile false și informația manipulatorie;
- asigurarea condițiilor pentru informarea echidistantă a telespectatorilor, prin instituirea unor reguli stricte în cazul emisiunilor de dezbateri: invitarea în studio a tuturor părților, oferirea condițiilor pentru dreptul la replică etc. ;
- difuzarea comunicatelor structurilor organelor de ocrotire a normelor de drept în jurnalul de sinteză informațională a zilei „Mesager";
- difuzarea constantă a informațiilor privind măsurile de combatere a terorismului de orice gen la nivel național și internațional;
- realizarea unor reportaje și interviuri, unor discuții în platou, care se referă la educarea populației, vin cu detalii privind protecția datelor cu caracter personal etc.

Drept exemplu pot servi și plasarea pe post în emisiunile de dezbateri a discuțiiilor cu temele „Infodemia, mai periculoasă decât virusul COVID-19", „Combaterea fenomenului traficului de persoane" etc. Totodată, în cadrul emisiunii „Miezul zilei" și în jurnalele de știri au fost incluse sistematic materiale care vizau campaniile și operațiunile de depistare și tragere la răspundere a persoanelor implicate în acte de încălcare a securității și ordinii publice**.**

Tot în anul 2020, Moldova 1 a organizat dezbateri electorale pentru alegerile prezidențiale, cu participarea candidaților la funcția de Președinte al Republicii Moldova, înscriși în cursa electorală. Dezbaterile televizate s-au desfășurat sub genericul „MĂ INFORMEZ ȘI VOTEZ! DEZBATERI ELECTORALE LA MOLDOVA 1" și au fot organizate în perioada 19 octombrie – 28 octombrie 2020. Au fost organizate și două emisiuni informative privind condițiile de participare la scrutin și măsurile de protecție împotriva COVID-19, în data de 29 și 30 octombrie. Postul public de televiziune Moldova 1 a reflectat scrutinul electoral conform Declarațiilor IP Compania „Teleradio-Moldova" privind politica editorială în perioada alegerilor și în conformitate cu Codul electoral, concepțiile CA și Regulamentele CEC și CA.

În rapoartele de monitorizare a activității posturilor de televiziune antrenate în campania electorală, pregătite și 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 același timp, potrivit monitorizărilor independente (Centrul pentru Jurnalism Independent și Coaliția pentru Alegeri Libere și Corecte), postul public Moldova 1 a reflectat echidistant și imparțial ambele campanii electorale, fără a favoriza sau defavoriza evident unul dintre candidați.

Radio Moldova a rezervat suficient timp pentru reflectarea războiului informațional, care capătă amploare în ultimul timp, în cadrul emisiunii „Loc de dialog", fiind invitați reprezentanți ai diferitelor partide, experti și analiști politici. Difuzarea mesajelor psihologice destructive, a știrilor false care pot genera panică,

tensiuni sau conflicte în societate, a materialelor cu caracter extremist, a pornografiei infantile este exclusă.

Campaniile electorale sunt reflectate corect, în conformitate cu Codul electoral, concepția CA și Regulamentele CEC și CA. Au fost organizate dezbateri electorale în cadrul campaniei „Alegeri prezidențiale". La dezbaterile electorale au participat candidaţii la alegeri sau reprezentanţii acestora. Tematica dezbaterilor electorale a fost stabilită şi anunţată odată cu invitarea la dezbateri. Procedura de stabilire a ordinii în care au fost invitaţi participanţii la dezbateri, precum şi gruparea acestora a fost stabilită în Declaraţia privind politica editorială a IP Compania „Teleradio-Moldova", cu respectarea principiului egalităţii de şanse pentru fiecare participant, precum şi a principiilor transparenţei şi imparţialităţii.

Moderatorii, în cadrul dezbaterilor, le-au asigurat participanţilor posibilitatea de a-și expune punctele de vedere asupra temelor abordate. Pe parcursul dezbaterilor, participanţilor li s-au asigurat condiții egale pentru libera exprimare a opiniilor.

MAEIE – comunicarea strategică este inclusă în Planul anual de activitate al ministerului. De asemenea, MAEIE asigură participarea reprezentanților săi în grupurile comunicatorilor la nivel național și internațional:

a) Consiliul Național de Comunicare constituit pe lângă Parlamentul Republicii Moldova;

b) Grupul de comunicare strategică pe lângă Guvernul Republicii Moldova;

c) Grupul Național de Comunicare COVID-19;

d) Taskforce East StratCom al Serviciul european de acțiune externă;

e) Grupul de lucru al comunicatorilor al SM GUAM.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
14/1	Evaluarea spaţiului Internet din perspectiva identificării entităţilor/ subiecţilor implicaţi în producerea şi diseminarea conţinutului media on-line şi a altor intermediari şi servicii auxiliare ce au impact pentru securitatea informaţională	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

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

SIS – în perioada de referință au fost acumulate și analizate date de interes pe dimensiunile de competență ale Serviciului, în scopul evaluării conținutului media on-line, cu potențial de prejudiciere a securității informaționale a Republicii Moldova, care s-au integrat în produse informativ-analitice expediate conducerii țării și beneficiarilor legali.

În contextul pandemiei COVID -19 s-a accentuat tendința unor resurse web de a promova știri false cu potențial de periclitare a securității informaționale.

La acest capitol, evidențiem următoarele rezultate:

1. A fost elaborat studiul cu privire la *„fenomenul fake-news și manipulări în spațiul mediatic al RM în contextul răspândirii COVID-19”*, prezentat membrilor Comisiei pentru Situații Excepționale a RM.
2. Pe parcursul perioadei stării de urgență, Serviciul a dispus **sistarea accesului la 61 de resurse on-line** (site-uri și bloguri), care promovau știri false. Listele cu resursele supuse blocării au fost plasate pe site-ul sis.md și pe pagina oficială de Facebook a instituției.
3. A fost elaborat Ghidul de identificare a știrilor false în vederea promovării consumului calitativ al știrilor de către societate. Ghidul a fost plasat pe site-ul oficial www.sis.md și pe pagina Facebook a instituției.
4. Subunitatea responsabilă de procesarea analitică a elaborat un material analitic de suport în contextul dezideratului de promovare a unor amendamente legislative.
5. SIS a elaborat și expediat proiecte de Dispoziție a Comisiei pentru Situații Excepționale a Republicii Moldova de instituire a Grupului de analiză a informațiilor publice pe lângă Secretarul Comisiei pentru Situații Excepționale a RM, cu rol de depistare, prevenire și contracarare a știrilor false, cît și cel de comunicare strategică.

MAEIE – Raportul anual de activitate al Biroului de presă al MAEIE a consemnat că pe tot parcursul anului 2020 au fost recepționate 95 de solicitări de acreditare din partea a 29 de instituții de presă din următoarele țări: România, Ucraina, Belarus, Rusia, Franța, Spania, Olanda, Marea Britanie, Letonia, Estonia, Finlanda, Georgia, Turcia. MAEIE, în cooperare cu instituțiile abilitate, a identificat în procedura de acreditare mai mulți jurnaliști străini implicați în producerea și diseminarea conținutului media fals sau manipulatoriu *(portaluri de știri, formatori de opinie)* pe subiecte precum restricționarea circulației internaționale a persoanelor, combaterea pandemiei Covid-19, ajutoarele umanitare oferite de partenerii externi, alegerile prezidențiale din RM din noiembrie 2020.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Consolidarea capacităților operaționale**			
15/2	Ajustarea cadrului legal în vederea eficientizării colectării de date pentru identificarea provenienței mijloacelor financiare și a proprietății ale subiecților implicați în activități de dezinformare, manipulare și propagandă ce subminează securitatea informațională	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.*

Din considerentul că actualmente nu există o concepție în cadrul legal pe dimensiunea audiovizualului cu privire la definirea acțiunilor și fenomenelor de dezinformare, manipulare și propagandă ce subminează securitatea informațională, 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 II **Consolidarea capacităților operaționale**			

15/3	Interacţiunea cu instituţiile de drept în ceea ce priveşte analiza riscurilor şi a ameninţărilor din domeniul mass-mediei, cu scopul de a monitoriza evoluţia ameninţărilor depistate, de a investiga activitatea subversivă sau penală în spaţiul informaţional şi de a stabili sursele de finanţare a factorilor de risc	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Serviciul de Informaţii şi Securitate.*

În perioada de referință, SIS a mediatizat mai multe măsuri executorii privind înlăturarea cauzelor și condițiilor ce contribuie la realizarea amenințărilor securității de stat, capabile să afecteze securitatea informațională a Republicii Moldova. Printre acestea se includ măsurile de identificare și blocare a surselor cu conținut online care promovează știri false cu privire la evoluția COVID-19.

La fel, pe acest palier SIS a remis demersuri către Președintele RM și Ministerul Justiției în scopul stabilirii unui sistem de sancționare pentru răspândirea cu bună știință a știrilor false.

În adresa Președintelui RM, Serviciul a înaintat spre examinare și eventuală promovare proiectul Legii pentru modificarea unor acte legislative, ce prevede instituirea unei noi atribuții Serviciului, și anume contracararea răspândirii informațiilor false ce afectează securitatea națională.

În anul 2020 Procuratura Generală a elaborat un studiu cu privire la actele de reacționare inițiale urmare a autosesizărilor din mass-media și rezultatele acțiunilor întreprinse de către procurori.

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 realizarea sarcinilor de depistare, prevenire şi contracarare a riscurilor şi ameninţărilor la adresa securităţii informaţionale	Anul 2019	Parțial realizat

Instituţia responsabilă: *Serviciul de Informaţii şi Securitate*.

Grupul de lucru creat sub egida SIS a elaborat Statutul Consiliului coordonator pentru asigurarea securității informaționale, constituit din reprezenanți 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”*.

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 Excelenţă TEKWILL, str. Studenţilor 9/11 din mun. Chişinău a fost aprobat proiectul de Hotărâre de Guvern, ce urmează a fi aprobat de către Guvernul Republicii Moldova.

Suplimentar, pe parcursul anului, Grupul de lucru a examinat suplimentar proiectul Hotărârii de Guvern enunțate în scopul definitivării versiunii finale a acesteia.

În context, pe data de 16.06.2020, în incinta SIS al RM, a fost desfășurată o ședință de lucru cu participarea reprezentanților mass-media și societății civile la subiectul extinderii reprezentativităţii palierului mediatic al Consiliului coordonator pentru asigurarea securităţii informaţionale.

Totodată, a fost realizată o comunicare cu autoritățile vizate în Planul SSI și Aparatul Președintelui RM pe marginea subiectului privind aprobarea creării Consiliului coordonator pentru asigurarea securității informaționale prin Decretul Președintelui RM și modificarea pct. 26 al proiectului Statutului respectiv prin care lucrările de secretariat al Consiliului urmau a fi asigurate de către Serviciul Consiliului Suprem de Securitate din cadrul Aparatului Președintelui RM.

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	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Serviciul de Informații și Securitate a elaborat propunerile legislative pe domeniul combaterii știrilor false și le-a remis în adresa Președintelui Republicii Moldova. Ulterior, proiectul a fost expediat de la Președinție către Ministerul Justiției unde a fost contramandat și inițiată procedura nouă de elaborare a setului de legi ce ar contracara știrile false ce amenință securitatea statului.

MAEIE – În anul 2020 RM a continuat acțiunile menite să asigure operaționalizarea Acordului RM – UE privind procedurile de securitate pentru schimbul de informații clasificate.

1. În perioada 4 – 7 februarie 2020, la Chișinău, a avut loc misiunea de evaluare a experților UE în domeniul protecției informațiilor clasificate, în vederea evaluării măsurilor de protecție în vigoare, aspectelor juridice, securității documentelor și personalului, securității fizice și informatice.
2. În noiembrie 2020, UE a transmis Raportul final de evaluare a mecanismului de protecție a informațiilor atribuite la secretul de stat din RM, elaborat de experții UE în contextul operaționalizării Acordului SIA. Raportul reflectă rezultatele evaluării efectuate în februarie 2020, precum și conține o serie de recomandări privind consolidarea regimului de protecție în vederea corespunderii cu standardele UE.

3. În ianuarie 2021, printr-o scrisoarea oficială – UE a anunțat despre finalizarea pregătirilor pentru operaționalizarea Acordului SIA și disponibilitatea sa de a iniția procesul de schimb a informațiilor clasificate.

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	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

SIS a elaborat Ghidul de identificare a știrilor false în vederea promovării consumului calitativ al știrilor de către societate, care a fost plasat pe site-ul „sis.md” și pe pagina de „Facebook” a instituției.

Conținutul ghidului:

- *acțiuni recomandate în cazul identificării de către consumatori a știrilor false și a conturilor false utilizate pe rețelele de socializare în distribuirea intensă a dezinformărilor;*
- *pași necesari de întreprins înainte de a lua decizia de a aprecia sau distribui o știre;*
- *exemple de știri false cu privire la evoluția COVID-19 și măsurile de protecție și prevenire care au stat la baza blocării unor resurse anonime.*

MAEIE – desfășurarea pe parcursul perioadei de raportare a campaniilor tematice pentru consultarea surselor oficiale pe platformele MAEIE, MDOC, pe rețele sociale și în interacțiunea cu mass-media.

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 Informaţii şi Securitate	Trimestrul II, III, IV, anul 2019	Realizat în 2019

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În cadrul Serviciului de Informații și Securitate a fost creată unitatea analitico-informațională specializată pe amenințările hibride de securitate.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
17/2	Crearea reţelei naţionale a autorităţilor responsabile de combaterea ameninţărilor hibride de securitate	Anul 2020	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de raportare a continuat procesul de creare a reţelei naţionale a autorităţilor responsabile de combaterea ameninţărilor hibride de securitate, fiind instituit un Grup de lucru interinstituțional în acest sens

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
17/3	Elaborarea unor protocoale operaționale de interacțiune între autoritățile responsabile și factorii de decizie în cazul unor amenințări hibride de securitate	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Pe parcursul anului de referință a fost inițiat procesul de elaborare a protocoalelor operaţionale de interacţiune între autorităţile responsabile şi factorii de decizie în cazul unor ameninţări hibride de securitate.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
17/4	Consolidarea gradului de cunoaştere şi înţelegere a concepţiei ameninţărilor hibride de securitate la nivelul organelor abilitate cu asigurarea securităţii informaţionale şi consolidarea mediului general de securitate	Perioada 2021-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Serviciul de Informații și Securitate a elaborat un algoritm de identificare a caracteristicilor distincte ale unei amenințări de natură hibridă pentru consolidarea nivelului de cunoaștere și excluderea neclarităților și confuziilor la acest subiect. Acest produs urmează a fi promovat la prima etapă la nivel instituțional și ulterior interinstituțional.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
17/5	Efectuarea exerciţiilor pentru dezvoltarea capacităţilor autorităţilor specializate în combaterea ameninţărilor hibride de securitate	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

SIS – Pe parcursul anului 2020, ofițerii SIS au participat în cadrul unor grupuri de lucru interinstituționale dedicate problematicii amenințărilor hibride.

La solicitarea MAEIE, Serviciul a elaborat și a remis un Chestionar-matrice cu referire la reziliența Republicii Moldova la anticiparea și contracararea amenințărilor hibride.

La fel, prin prisma evaluărilor de competență, au fost elaborate materiale informative, care au reliefat factorii de risc cu potenţial de amenințări hibride.

MAEIE – În perioada 18-19 februarie 2020, MAEIE a găzduit seminarul TAIEX, cu privire la amenințările hibride, în cadrul căruia o echipă de experți din Finlanda a împărtășit experiența și bunele practici în instituirea cadrului interinstituțional pentru identificarea și combaterea amenințărilor hibride. Obiectivul principal al evenimentului a fost familiarizarea experților RM cu experiența Finlandei în domeniul combaterii amenințărilor hibride și promovarea cooperării dintre instituțiile vizate din RM, privind (re)inițierea procesului creării

cadrului interinstituțional în RM. La seminar au participat circa 20 de persoane din cadrul instituțiilor naționale relevante (SIS, STISC, MAI, MA, MEI și Administrația Președintelui RM, etc.).

La fel, în anul 2020, în cadrul MAEIE a fost organizat un atelier privind amenințările hibride.

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	Parțial realizat

Instituția responsabilă: *Ministerul Apărării*

În perioada de referință a derulat procesul de achiziție a echipamentului necesar creării entității responsabile de apărarea cibernetică, care este preconizată pentru anul 2021.

De asemenea, în anul 2020, experții SIS au participat la ședințe comune cu reprezentanții Marelui Stat Major al Armatei Naționale cu tematici ce vizează securitatea cibernetică a rețelelor informaționale instituționale.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
18/2	Consolidarea capacităților 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.*

În legătură cu situația pandemică COVID-19, instruirile în masă au fost sistate. În context, au fost organizate cursuri de la distanță, după cum urmează:

- Participarea la eveniment în domeniul securităţii cibernetice desfăşurat de compania TUV, Austria (06.02.2020, mun. Chişinău) - 2 militari;
- Participarea la Cursul terorismul cibernetic (08-14.02.2020, or. Ankara, Turcia) - 2 militari;
- Participarea la Seminarul „Cyber Endeavor Regional seminar FY20” (09-13.03.2020, or. Bled, Slovenia) - 2 militari;
- Participarea la cursul la distanţă „Analiza traficului de reţea”(14.09-15.11.2020, Germania, or. Oberammergau) - 1 militar;
- Desfăşurarea Cursului „Mobile Penatration Devices” cu suportul echipei mobile de instruire Naval Postgraduate School, Monterey (20-24.07.2020 - 25.09.2020-online) cu implicarea 29 participanţi (MA-24 mil., SIS-2 part., STISC-2 part. şi FISC-1 part.);
- Participarea la Conferinţa anuală online „Moldova Cyber Week 2020” (25-27.11.2020) - 2 militari;
- Desfăşurarea Cursului de specializare în domeniul securităţii informaţionale online (07-18.12.2020, AMFA)- 12 militari.

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.*

Serviciul de Informații și Securitate a elaborat un produs analitic în adresa I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică” cu referire la vulnerabilitățile identificate în resursele informaționale de stat, fiind înaintat un set de recomandări pentru înlăturarea și minimalizarea deficiențelor sesizate.

În perioada de raportare au fost desfășurate ședințe de lucru comune ale experților SIS și Ministerului Apărării în vederea elaborării mecanismului de cooperare cu entitatea responsabilă de apărare cibernetică din cadrul Forţelor Armate.

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	Realizat în 2019

Instituţia responsabilă: *Ministerul Justiţiei, Consiliul Audiovizualului.*

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
19/2	Stabilirea atribuţiilor organelor competente privind depistarea şi contracararea mesajelor manipulatorii şi de dezinformare din reţeaua globală Internet	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Experții SIS au analizat cadrul legal în vigoare ce vizează diseminarea informației ce nu corespunde adevărului, fiind înaintate propunerile corespunzătoare pentru ajustarea acestuia.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
20/1	Elaborarea şi aprobarea cadrului legal privind identificarea şi desemnarea infrastructurilor critice naţionale, inclusiv a celor ce ţin de sistemele informaţionale de importanţă vitală	Perioada 2019-2021, 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)*.

Concomitent, SIS a elaborat și definitivat proiectul Programului și Planului național cu privire la Infrastructura Critică și l-a remis în adresa MAI pentru a fi prezentat la Guvern conform procedurii.

SIS a avizat Proiectul Legii Nr. 370 din 10.06.2020 privind protejarea obiectelor de infrastructură esențială pentru asigurarea securității naționale și a ordinii publice *(inițiativă legislativă nr. 163 din 21.04.2020)*.

La fel, în perioada anului 2020, SIS a coordonat activitatea de protecție a Infrastructurii Critice în temeiul HG 701 din 11.07.2018, HG 996 din 17.10.18, Ordinul Directorului SIS nr. 50 din 24.10.18, Ordinul Directorului SIS nr. 20 din 15.05.19.

În conformitate cu prevederile HG 701 din 11.07.2018, este creată baza de date a Infrastructurii Critice, iar în prezent se elaborează cadrul normativ departamental corespunzător.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Mecanismul de evaluare și raportare privind starea şi nivelul de securitate ale obiectivelor de infrastructură critică din perspectiva securităţii informaţionale este elaborat și prezentat spre examinare și aprobare în adresa Guvernului.

Totodată, pe parcursul anului 2020 Centrul Antiterorist al SIS a realizat cinci teste antiteroriste.

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 complexe la adresa securităţii informaţionale	Perioada 2020-2022, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de raportare experții SIS au evaluat cadrul normativ de referință, care urmează a fi supus modificărilor în scopul armonizării legislației.

Pe palierul contracarării acțiunilor extremiste în spațiul informațional, Serviciul a sesizat PG privind activitatea unor entități.

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	În proces de realizare

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.*

În perioada anului 2020, în cadrul Serviciului de Informații și Securitate au fost realizate studii și analize pe aspectele securității informaţionale, pe fiecare compartiment în parte: *mass-media, tehnologii informaţionale, apărare, ordine publică şi contrainformaţii*, cu scopul evaluării nivelului de pregătire a ofițerilor de informații și securitate pe dimensiunile de competență.

Totodată, pe parcursul anului 2020 au fost realizate o serie de evenimente pe platforme online *(cursuri de instruire, conferințe, exerciții practice)* la care au participat ofițeri SIS.

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 incluși cu prioritate în programele noi de instruire a resurselor umane în domeniul vizat	Anul 2021, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Autorităţile administraţiei publice*

SIS – A fost continuat procesul de instruire a ofițerilor de informații și securitate în baza modulului de instruire privind securitatea cibernetică și informațională, elaborat în corespundere cu prevederile Strategiei securității informaționale și a Planului de acțiuni pentru implementarea acesteia.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
24/1	Evaluarea nivelului actual al cooperării dintre Republica Moldova şi organizaţiile internaţionale ce îşi desfăşoară activitatea în domeniul asigurării securităţii informaţionale şi elaborarea unor acţiuni privind intensificarea cooperării respective	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituția responsabilă: *Autorităţile administraţiei publice*

În vederea realizării obiectivului de asigurare a cooperării internaționale în domeniul securității informaționale, SIS a întreprins o serie de activități bi/ multilaterale ce vizează interacțiunea cu serviciile partenere *(schimb de informații,*

întrevederi la nivel de conducere şi la nivel de experţi cu reprezentanţi oficiali ai serviciilor speciale străine, acreditaţi pentru RM, webinare, conferinţe online).

Astfel, în scopul preluării experienței la nivel bilateral, au fost realizate ședințe cu reprezentanții serviciilor partenere, cu abordarea subiectelor ce țin de prevenirea, depistarea și contracararea amenințărilor hibride de securitate în spațiul informațional, etc.

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	În proces de realizare

Instituția responsabilă: *Autorităţile administraţiei publice*

SIS – În contextul dinamizării dialogului politic RM – UE, a fost activizată cooperarea cu instituțiile europene pe segmentul amenințărilor hibride. În acest sens, în formatul proiectului ***„EEAS Hybrid Risk Survey for Partner States”*** au fost reflectate evoluțiile pentru perioada 2016-2020 înregistrate la nivel național în contextul acțiunilor de răspuns, cu tangență la domeniile stabilite în chestionar *(reziliență, infrastructură critică, mecanisme de gestionare a crizelor, etc.)*.

MAEIE – Urmare a vizitei efectuate în iulie 2019 de către echipa de evaluare a corporației MITRE *(mandatată de Departamentul de Stat SUA)*, în primul semestru al anului 2020 a fost redactată versiunea finală a raportului preliminar privind capacitățile cibernetice ale Republicii Moldova, care a luat în calcul în cvasitotalitate sugestiile și modificările de text propuse pe marginea proiectului de către MEI, STISC, AGE și MAEIE. Versiunea finală a raportului preliminar a fost prezentată MAEIE pe data de 24.08.2020 și transmisă instituțiilor vizate, spre informare și uz în activitate. Totodată, pe 24.09.2020 a avut loc o ședință online la subiectul securitatea cibernetică a experților de la Oficiul pentru Coordonarea problemelor cibernetice, DoS și reprezentanții MITRE, CERT, STISC, AGE *(Notă: O nouă misiune de evaluare a corporației MITRE era preconizată pentru luna martie 2020, însă, din cauza restricțiilor impuse în contextul pandemiei COVID-19, vizita a fost contramandată)*.

În contextul negocierilor pe marginea noii Agende de Asociere, MAEIE în cooperare cu alte instituții abilitate, a promovat includerea în proiectul documentului a prevederilor cu privire la cooperarea RM-UE în sfera contracarării amenințărilor hibride și dialogului RM-UE în sfera securității cibernetice. Negocierile încă nu au fost finalizate, dar este cert că Agenda de Asociere 2021-2027 va conține astfel de prevederi și va fi baza pentru dezvoltarea cooperării.

Un obiectiv prioritar al Planului Individual de Acțiuni al Parteneriatului (IPAP) RM-NATO pentru anii 2017-2019, aplicat și în 2020, a fost dezvoltarea cooperării bilaterale în domeniul securității cibernetice și informaționale. În acest sens, a fost promovat dialogul la nivel înalt cu oficialii Alianței precum și la nivel de experți. A

fost implementat proiectul „Dezvoltarea capacităților de apărare cibernetică ale Forțelor Armate ale RM”, ceremonia oficială de încheiere a proiectului a fost organizată online pe 21.01.2021 cu participarea Secretarului General adjunct al NATO, Mircea Geoană.

De asemenea, reprezentanții autorităților naționale au continuat să beneficieze din participarea la conferințe, seminare, ateliere de lucru, cursuri de instruire, exerciții practice la tematica securității cibernetice organizate de NATO, dar şi de statele partenere ale Alianței.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
25/1	Crearea/ implementarea cadrului de cooperare interinstituţională pe domeniul apărării cibernetice	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Ministerul Apărării, Serviciul de Informaţii şi Securitate, Ministerul Economiei şi Infrastructurii, Serviciul Tehnologia Informației şi Securitate Cibernetică, Procuratura Generală, Ministerul Afacerilor Interne.*

În perioada de referință, experții SIS au participat la ședința consultativă privind crearea/implementarea cadrului de cooperare interinstituțională pe domeniul apărării cibernetice.

Pe parcursul anului 2020, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică,, a acordat suport şi consultanţă în vederea constituiri a Centrului de Reacţie la Incidente Cibernetice (CRIC) al Armatei Naţionale, care a fost deschis la 21 ianuarie 2021.

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	În proces de realizare

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

MAEIE a examinat, de comun acord cu MAI, și a acordat asistența necesară pentru adoptarea la data de 06 iulie 2020 a Decretului privind aprobarea semnării Memorandumului de cooperare între statele-membre ale Organizației pentru Democrație și Dezvoltare Economică – GUAM în domeniul securității cibernetice.

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”	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

	și a bazei de date privind exploatarea sexuală a copiilor (ICSE) a OIPC INTERPOL		

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

Au fost examinate în Sistemul Informațional „Protecția Copiilor” pe c/p pornite în anul curent peste 380 dispozitive de stocare a datelor, fiind depistate și excluse din circuit în rețeaua Internet peste 42 mii de imagini și 15 mii fișiere video cu conținut de pornografie infantilă.

Au fost introduse în baza de date ICSE a OIPC Interpol și analizate fișiere imagini și video depistate în dispozitivele ridicate: 1.017 fișiere foto, 92 fișiere video, analizate serii de imagini cu adăugarea a peste 1.500 comentarii pentru contribuire la identificarea victimelor.

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.*

În calitate de punct de contact 24/7 prin Convenția privind criminalitatea informatică și a punctului de contact G 7 24/7, Direcția investigații infracțiuni informatice a INI a **IGP** asigură și recepționează solicitările privind asistențe imediate pentru investigațiile referitoare la infracțiunile informatice.

Astfel, pe parcursul perioadei de raportare au fost recepționate:

•solicitări recepționate - 4 (1 Regatul Țărilor de Jos, 3 Ucraina);
•transmise răspunsuri - 5 (2 Ucraina, 1 Regatul Țărilor de Jos, 2 Germania);
•transmise solicitări - 3 (1 SUA, 1 Regatul Țărilor de Jos, 1 Rusia);
•cereri de conservarea datelor parvenite -18 (7 SUA, 2 Spania, 3 Republica Cehă, 2 Ucraina, 1 Franța, 3 Germania, 1 Armenia);
•răspunsuri de conservarea datelor - 10 (4 SUA, 2 Cehia, 2 Ucraina, 2 Spania, 1 Armenia).
-BKBOP:
•solicitări recepționate - 1;
• transmise răspunsuri - 1;
• trimise solicitări - 2.

Totodată, datorită stabilirii noilor contacte la nivel internațional, precum și a promovării Direcției prin participarea la instruiri, evenimente și operațiuni internaționale, au fost înregistrate următoarele rezultate privind cooperarea internațională:

•transmise solicitări - 51 (18 Facebook, 8 webmoney, 1 avast software, 1 youtube, 1reg.ru, 1 OVH, 1 Qiwi, 1Alfa, 3 western Union, 1 Qiwi, 2 Apple, 2 Moneygram, 4 Paypal, 1Paymaster, 1 Ali Express, 3 Google, 1 Skype, 1 Coulfare);
• primite răspunsuri - 20 (8 Facebook, 3 western union, 8 webmoney, 1 Apple)

• trimise scrisori cu caracter informativ: BKPOP - 1.

În anul 2020, Secția tehnologii informaționale și combaterea crimelor cibernetice a **Procuraturii Generale** a examinat 40 comisii rogatorii parvenite de la autoritățile competente din: Italia, Slovenia, Polonia, Olanda, SUA, Belgia, România, Germania, Franța, Belarus, Ucraina, Armenia Turcia și Cehia, cât și a primit solicitări din partea altor țări 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.*

La data de 05.05.2020, un reprezentant al IGP a participat în cadrul a 2 webinar-uri, unul privind cooperarea digitală, organizat de HLPDC a ONU și unul cu privire la utilizarea platformei Centrului Național pentru Copii Dispăruți și Exploatați din SUA (NCMEC), în vederea identificării cazurilor de pornografie infantilă, abuz și exploatare sexuală online a copiilor.

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	Anul 2021, cu verificarea anuală a indicatorilor de progres	În proces de realizare

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

Prin intermediul Centrului cooperare polițienească al IGP în total au fost expediate și recepționate 17 solicitări și răspunsuri, dintre care:

1. OEP EUROPOL Oficiul Central – 2;
2. OEP EUROPOL Belgia – 1;
3. OEP EUROPOL Spania – 1;
4. OEP EUROPOL Regatul Țărilor de Jos – 1;
5. OEP EUROPOL Polonia – 1;
6. BNC Interpol Secretariatul General – 1;
7. BNC Interpol Washington – 1;
8. BNC Interpol Norvegia – 1;
9. BNC Interpol Paris – 2;
10. BNC Interpol Tirana – 1;
11. BNC Interpol Moscova – 1;
12. BNC Interpol Dublin - 1
13. Proiectul de Analiză Europol AP TWINS – 1;

14.Centrul de Inovații al Secretariatului General Interpol – 1;
15.SELEC – 1.

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.*

MAEIE asigură coordonarea participării experților naționali la activitățile organizate în cadrul proiectului „Acțiunea privind criminalitatea informatică pentru reziliența cibernetică în regiunea Parteneriatului Estic", denumit generic CyberEast, finanțat de Comisia Europeană și implementat de Consiliul Europei (CoE) prin intermediul Oficiului pentru Programul de combatere a criminalității informatice al CoE din București (C-PROC). Astfel, în decursul anului 2020 a fost facilitată participarea experților naționali la următoarele activități:

- Reuniunea internațională privind cooperarea cu prestatorii străini de servicii de Internet (ISPs) (Tbilisi, 28 – 29 februarie 2020), 5 participanți;
- Atelier de lucru privind elaborarea Procedurilor Operaționale Standard pentru cooperarea CSIRT și organele de aplicare a legii (14 – 16 septembrie 2020), 25 participanți;
- Atelier de lucru cu privire la fraudele comise online, veniturile obținute de pe urma infracțiunilor și mecanismele de raportare (15 – 16 octombrie 2020); 60 participanți;
- Exercițiu practic privind cooperarea între organele de aplicare a legii și furnizorii de servicii internet (2-4 decembrie 2020); 17 participanți;
- Atelier de lucru comun privind cooperarea internațională pe dimensiunea combaterii criminalității cibernetice și privind dovezile electronice (8-9 decembrie 2020); 3 participanți.

De asemenea, MAEIE a facilitat desemnarea punctelor focale din cadrul MAI, INJ și PG de a coopera cu Grupul european de instruire și educare în domeniul criminalității cibernetice (ECTEG).

Un alt rezultat important al proiectului a fost admiterea a trei experți din RM la Programul de master „Forensic Computing and Cybercrime Investigation" în cadrul University College Dublin, finanțat din proiectul CyberEast.

Reprezentanţii **IGP** al **MAI**, responsabili de contracararea criminalităţii informatice au participat la 15 instruiri la nivel internațional, fiind instruiţi 17 specialiști în acest domeniu, după cum urmează:

1. În perioada 12-15.02.2020, Participarea la Reuniunea proiectului regional CoE-UE, cu tematica "*Acțiunea privind criminalitatea informatică pentru reziliența cibernetică în regiunea Parteneriatului Estic - CyberEast*", or. Kiev, Ucraina;

2. La 18.02.2020, Participarea la ședința de lucru cu experții Uniunii Europene, eveniment desfășurat în cadrul **Proiectului Improving Cyber Resilience the Eastern Partnership Countries**, la sediul Delegației Comisiei Europene în RM;
3. La 20.02.2020, Participarea la ședința cu reprezentanții Uniunii Europene, în cadrul **Poiectului „Improving Cyber Resilience the Eastern Partnership Countries**";
4. La 27.05.2020, a fost desfășurată întâlnirea online în cadrul proiectului CoE „EndOCSEA" (oprirea exploatării sexuale online a copiilor).
5. La 04.06.2020 Webinar-ul cu tematica: „*Interferența electorală, atacuri asupra sistemelor informaționale critice*", organizat de către Consiliul Europei în cadrul proiectului "CyberEast;
6. La 30.06.2020, participarea la ședința online de lansare a proiectului CoE privind combaterea violenței, inclusiv sexuale, asupra copiilor ;
7. La 06.07.2020, participarea la ședința grupului de lucru al ODDE-GUAM în domeniul securității cibernetice în format de videoconferință;
8. La 09.07.2020, participarea la ședința de lucru, în cadrul proiectului CyberEast 2020, eveniment organizată de către Consiliul Europei și desfășurat online;
9. În perioada 16-17.07.2020, participarea în cadrul în cadrul ședinței virtuale din cadrul operațiunii cu genericul Operation In Our Sites (IOS) XI (comercializarea prin intermediul internetului a bunurilor contrafăcute);
10. La 01.10.2020, ședința on-line privind proiectul dezvoltarea softului de tip Web crowler, pentru identificarea cazurilor de abuz și exploatare sexuală cu utilizarea Internetului, gestionat de reprezentantul poliției din Regatul Țărilor de Jos;
11. La 12.10.2020, participarea la ședința on-line privind implementarea Convenției Lanzarote;
12. În perioada 22-28.10.2020, participarea la grupul de lucru on-line cu autoritățile de aplicare a legii din SUA și Germania;
13. În perioada 02-13.11.2020, Atelierul de lucru „Victim Identification Task-Force 8 (VIDTF8)", organizat de către EUROPOL în regim online;
14. La 18.11.2020, ședința on-line a Biroului Comitetului Lanzarote;
15. În perioada 02-04.12.2020, atelierul de lucru online, organizat de către Uniunea Europeană și Consiliul Europei în baza Proiectului CyberEast, cu tematica: *„Acces eficient la date: exercițiu practic pentru forțele de ordine și furnizorii de servicii de Internet"*.

Pe parcursul anului 2020, personalul **Procuraturii Generale** au avut mai multe seminare de instruire organizate de Consiliul Europei în domeniul prevenirii și combaterii criminalității informatice:
1. Workshop Development of Standard Operating Procedures for Cooperation between CSIRTs and Law Enforcement, 14-16 septembrie 2020 (online);
2. Workshop on Online Fraud, Crime Proceeds and Reporting Mechanisms, 15-16 octombrie 2020 (online);
3. Effective Access to Data Programme: practical exercise for law enforcement and Internet service providers, 2-4 decembrie 2020 (online).

REFLECTAREA INDICATORILOR DE PROGRES CONFORM PRIORITĂŢILOR

Urmare a unei evaluări preparative a implementării Planului, se atestă o diminuare a randamentului acţiunilor realizate de către instituţiile responsabile şi partenere în anul 2020 prin prisma priorităţilor prevăzute de SSI, cauzată primordial de situația pandemică COVID-19 la nivel național și internațional.

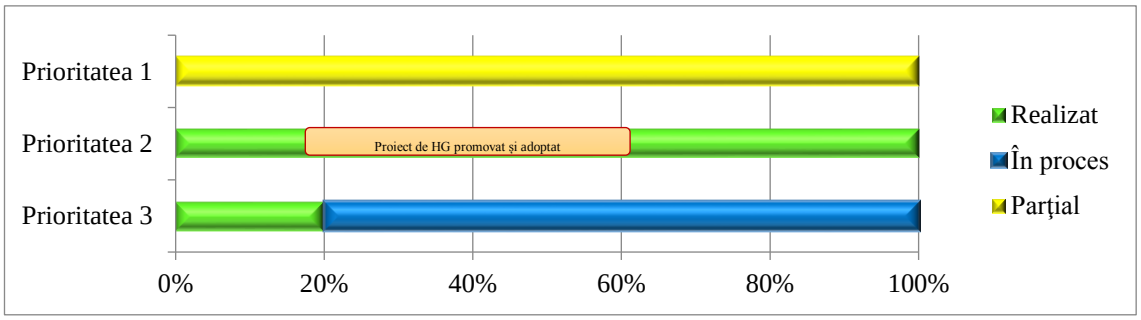
Totodată, este de menţionat că patru acţiuni stabilite de Plan sunt primordiale întregului proces de implementare a Strategiei.

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

Ponderea procentuală a realizării priorităţilor pe parcursul anului 2020 sunt prezentate în graficile 1, 2 şi 3, elaborate prin prisma indicilor de rezultat ale acestora.

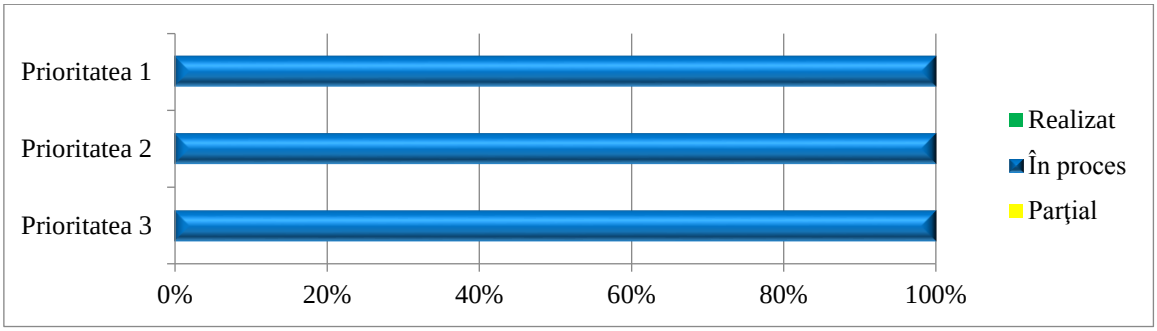
Pilonul I. Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice	
Priorităţile pilonului	**Indicatori de rezultat**
1. Crearea Centrului naţional de reacţie la incidente de securitate cibernetică (CERT naţional)	1. Centrul naţional creat, care elaborează 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 determinarea statutului juridic al publicaţiilor periodice, al agenţiilor de presă şi al altor entităţi care activează în spaţiul media din Internet	2. Lege de modificare a cadrului juridic existent
3. Crearea resursei/ platformei informaţionale de comunicare strategică	3. Resursă/ platformă informaţională de comunicare strategică creată

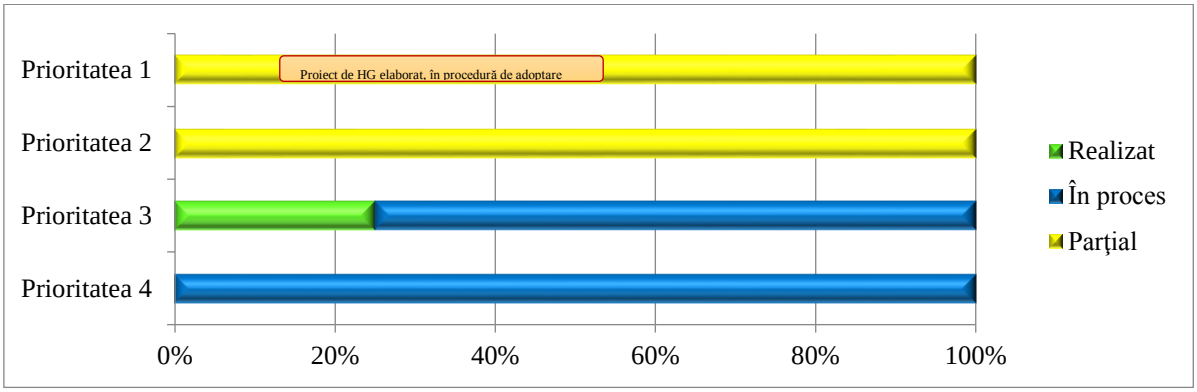
Grafic 2. Ponderea procentuală de realizare a priorităţilor Pilonului II



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

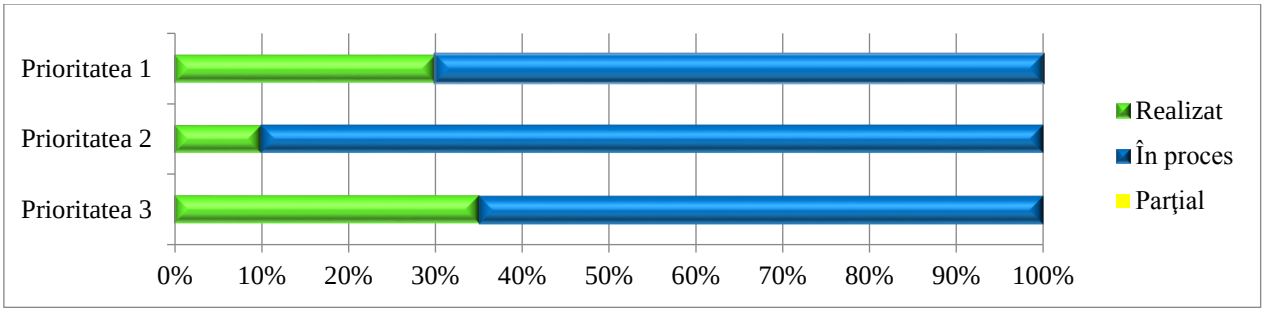
Grafic 3. Ponderea procentuală de realizare a priorităţilor Pilonului III



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	1. Specialişti instruiţi în baza practicilor UE

angajaţilor cu atribuţii de investigare şi urmărire penală în spaţiul informaţional	
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 prevederilor Strategiei securității informaționale impune implicarea plenară a componentelor societății informaționale, care prin executarea acțiunilor planificate și coordonate să impulsioneze realizarea obiectivelor Strategiei. Concomitent, obiectivele și acțiunile trasate pentru realizarea lor, au o dimensiune transectorială și necesită aportul instituțiilor din domeniul civil, mass media, TIC, cât și cu implicarea instituțiilor din domeniile de securitate, apărare, de drept și ordine publică.

Din considerentul caracterului complex al acțiunilor prevăzute de Planul SSI 2019-2024, au fost stabilite mai multe riscuri ale procesului de implementare a Strategiei, unele necesitând o atenție sporită și identificate soluții pentru înlăturarea sau diminuarea acestora.

În scopul de a fi accentuate și soluționate, riscurile indentificate au fost divizate în trei categorii după cum urmează:

<u>Categoria I</u>: Riscuri la nivelul managementului asociat procesului de implementare a Planului de acțiuni al SSI 2019-2024:

- Pe parcursul anului 2020, similar anului 2019, a fost observată poziția superficială în adoptarea documentelor de politici la nivel instituțional sau sectorial ce derivă din Strategia SSI 2019-2024 din partea managementului strategic al unor instituții responsabile sau partenere conform prevederilor Planului;
- De asemenea persistă o cooperare diminuată între echipele de specialiști în materie de securitate informațională din cadrul instituțiilor de drept public și privat, vizate în Planul SSI 2019-2024 și managementul decizional al acestora, care în astfel de circumstanțe pot decide unilateral modificarea sau excluderea anumitor acțiuni și obiective din Strategie, reprofilându-le sub alte documente de politici instituționale, reducând din caracterul unitar în implementarea Planului de acțiuni.

<u>Categoria II</u>: Riscuri operaționale la implementarea Planului de acțiuni al SSI 2019-2024:

- Lipsa sau insuficiența specialiștilor în domeniul tehnologiilor informaționale în subdiviziunile responsabile de asigurarea securității informaționale în cadrul autorităților publice, în special la funcționarea și dezvoltarea Centrelor de reacție la incidentele de securitate cibernetică – CERT departamental;
- Dotarea slabă a CERT-urilor instituționale cu sisteme operaționale și tehnică specializată pentru asigurarea securității cibernetice conform cerințelor internaționale de securitate informațională.

<u>Categoria III</u>: Riscuri de natură exepțională și complementară proceselor de implementare a Planului de acțiuni al SSI 2019-2024:

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

➢ Caracterul imprevizibil al evoluției pandemiei COVID-19 și efectul acesteia asupra proceselor și activităților oamenilor, inclusiv din domeniile vizate în Planul de acțiuni: civic, media, publice și privat.

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

CONCLUZII ŞI RECOMANDĂRI

Procesul de monitorizare realizat pe parcursul anului 2020 şi prezentat în Raportul pentru al doilea an de implementare, relevă importanța Strategiei, prioritățile de securitate informațională stabilite în SSI fiind în continuare conforme trendului de evoluție a societății informaționale la nivel național şi global.

Evaluarea detaliată a indicatorilor prezentați de instituțiile responsabile prin prisma atribuțiilor şi a acțiunilor din Plan, implementate de fiecare instituție separat sau prin interacțiune cu alte autorități partenere, raportați la obiectivele şi scopul SSI, reflectă un **progres relativ redus** în atingerea integrală a acestora, determinat inclusiv și de factori excepționali, cum este pandemia de COVID-19 și repercusiunile acesteia asupra vieții societății contemporane.

Riscurile de securitate şi criminalitate cibernetică, cât și evoluția **noilor forme de amenințări** la adresa **securității informaționale – războiul informațional, amenințările hibride, dezinformarea, propaganda, manipularea,** care **sunt în vizorul Strategiei securității informaționale** încă **nu au fost micșorate**.

Totuși, se atestă o conștientizare a problemelor de securitate informațională din partea reprezentanților insitituțiilor de drept public şi privat, cu stabilirea corespunzătoare vulnerabilităților și riscurilor pe anumite domenii, fapt ce **confirmă indicatorii de progres reflectați**.

Totodată, mai multe realizări, raportate de autoritățile vizate de Plan, se suprapun pe cadrul de competență instituțională și activitatea acestora în mod ordinar. Astfel, devine imperativ să percepem obiectivele și acțiunile Planului SSI vizavi de activitatea autorităților pe atribuții și competențe.

La fel, în rapoartele prezentate pe activități nu se atestă o conlucrare eficientă între instituțiile responsabile și cele partenere, fapt ce denotă în continuare lipsa de coerență interinstituțională, chiar dacă pentru rezolvarea problemelor de securitate informațională sunt necesare soluții complexe, cu aplicabilitate în toate domeniile de drept public și privat, părți ale societății informaționale în ansamblu.

Analiza rezultatelor acțiunilor scadente în anul 2020 şi a celor cu termen permanent de implementare, prezentate de instituțiile responsabile și cele partenere, urmează a fi examinată în cadrul următoarelor ședințe ale Grupului de lucru din cadrul SIS și persoanele desemnate de instituțiile incluse în Plan. Concomitent, este imperios să fie abordat și rolul ministerelor responsabile sau partenere în procesul de promovare a actelor normative aferente implementării Strategiei securității informaționale 2019-2024.