R A P O R T

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

Perioada de raportare: 2021

SERVICIUL DE INFORMAȚII ȘI SECURITATE

Elaborat – martie 2022

CUPRINS:

LISTA DE ABREVIERI ***3***

REZUMAT EXECUTIV ***4***

DESCRIEREA PROGRESELOR ACȚIUNILOR REALIZATE ÎN PERIOADA ANULUI 2021 ***7***

REFLECTAREA INDICATORILOR DE PROGRES CONFORM PRIORITĂŢILOR ***54***

DESCRIEREA RISCURILOR DE IMPLEMENTARE ***57***

CONCLUZII ŞI RECOMANDĂRI ***59***

LISTA DE ABREVIERI

- AGE – Agenţia de Guvernare Electronică
- AGEPI – Agenţia pentru Protecţia Proprietăţii Intelectuale
- ANCD – Agenţia Naţională pentru Cercetare şi Dezvoltare
- ANRCETI – Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei
- ASP – Agenţia Servicii Publice
- BNM – Banca Naţională a Moldovei
- CCA – Consiliul Coordonator al Audiovizualului
- CERT – Centru de reacție la incidentele de securitate cibernetică
- CMT – Centru Militar Teritorial
- CNA – Centrul Naţional Anticorupţie
- CNPDCP – Centru Național pentru Protecția Datelor cu Caracter Personal
- CSS – Consiliul Suprem de Securitate
- CTIF – IP „Centrul de Tehnologii Informaționale în Finanțe”/MF
- HG – Hotărîrea Guvernului
- HP – Hotărîrea Parlamentului
- IGP – Inspectorat General de Poliție
- MA – Ministerul Apărării
- MAEIE – Ministerul Afacerilor Externe şi Integrării Europene
- MAI – Ministerul Afacerilor Interne
- ME – Ministerul Economiei
- MECC – Ministerul Educaţiei, Culturii şi Cercetării
- MF – Ministerul Finanţelor
- MJ – Ministerul Justiţiei
- MMPS – Ministerul Muncii şi Protecţiei Sociale
- PG – Procuratura Generală
- SIS – Serviciul de Informaţii şi Securitate
- SSI/Strategia – Strategia securităţii informaţionale a Republicii Moldova
- STI – Serviciul Tehnologia Informației
- STISC – IP „Serviciul Tehnologia Informației și Securitate Cibernetică”
- SV – Serviciul Vamal/MF
- TIC – Tehnologii Informaționale și Comunicații

REZUMAT EXECUTIV

Raportul de monitorizare a implementării Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024 *(în continuare SSI/Strategie)* este o evaluare complexă a acţiunilor realizate şi rezultatelor înregistrate pe parcursul anului 2021 la executarea Planului de acţiuni al Strategiei, adoptat prin Hotărîrea Parlamentului nr. 257 din 22.11.2018.

În conformitate cu prevederile art. art. 2 şi 3 al HP nr. 257 din 22.11.2018 şi a pct. 115 din Strategie, Serviciul de Informaţii şi Securitate al Republicii Moldova este autoritatea responsabilă de monitorizarea şi coordonarea procesului de implementare a Planului de acţiuni al SSI.

Astfel, obiectivul central al Strategiei securității informaționale a Republicii Moldova pentru anii 2019 – 2024 constă în corelarea juridică și integrarea sistemică a domeniilor prioritare cu responsabilităţi şi competenţe în asigurarea securităţii informaţionale a țării noastre, bazată pe reziliența cibernetică și informațională pe dimensiunea de securitate, întru protejarea suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

Planul de acţiuni al SSI *(în continuare Plan)* însumează complexul de acţiuni elaborate de instituţiile de drept public şi privat, care sunt parte a societăţii informaţionale, pentru implementarea 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 capacităţilor instituţionale în combaterea criminalităţii informatice;*
9. *Efectuarea unor cercetări ştiinţifice aplicative în domeniul securităţii informaţionale;*
10. *Dezvoltarea capacităților 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 şi 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 şi combaterii criminalităţii informatice.*

Pe parcursul anului 2021, care este al treilea an de implementare a HP nr. 257, Serviciul de Informații și Securitate, de comun cu instituțiile responsabile, au realizat acțiuni orientate la executarea Planului, în special fiind organizate discuții între reprezentanții Secretariatului Grupului de monitorizare și persoanele responsabile, desemnate de instituțiile vizate pentru implementarea Planului cu referință la acțiunile de competență prevăzute în ultimul.

Potrivit principiilor 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 realizate de către autorităţi prin prisma prevederilor Planului SSI şi a Planurilor instituționale elaborate;
- Măsurare a progresului cantitativ şi calitativ al realizării SSI 2019-2024;
- Reflectarea indicatorilor de impact în al treilea an de implementare, conform aprecierilor insitituţiilor responsabile şi a indicatorilor prezentaţi în rapoarte;
- Identificarea riscurilor pentru implementarea Planului şi a recomandărilor date.

Totodată, raportul include:

1. Analiza acţiunilor şi progreselor prezentate de instituţiile responsabile, conform rapoartelor remise în adresa Secretariatului Grupului de monitorizare creat în cadrul Serviciului de Informaţii şi Securitate;
2. Evaluarea calitativă şi cantitativă a realizării acţiunilor în baza indicatorilor de progres şi a rezultatelor propuse, corelate cu obiectivul Strategiei;
3. Expunerea riscurilor pentru realizarea acţiunilor scadente la finele perioadei de evaluare;
4. Prezentarea impactului realizării SSI conform indicatorilor de progres, a obiectivelor generale şi a scopului Strategiei, conform discuțiilor bilaterale şi multilaterale organizate la nivelul instituţiilor responsabile şi partenere.

În procesul de analiză și evaluare a rezultatelor şi indicatorilor de progres, în scopul aprecierii rezultatelor acţiunilor executate, au fost utilizate următoarele calificative: „Realizat”, „Parţial realizat” şi „În proces de realizare”.

DESCRIEREA PROGRESELOR ACȚIUNILOR REALIZATE ÎN PERIOADA ANULUI 2021

Capitolul reflectă progresul executării acţiunilor scadente în anul 2021 şi a celor cu termen permanent de implementare, pe fiecare palier și punct 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 entităţii care va exercita rolul de Centru naţional de reacţie la incidente de securitate cibernetică şi care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autorităţile publice competente şi persoanele fizice şi juridice: a) elaborarea şi promovarea cadrului normativ relevant; b) crearea Centrului naţional de reacţie la incidente de securitate cibernetică	Perioada 2019-2021, cu verificarea anuală a indicatorilor de progres	Parţial realizat

Instituții responsabile: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Cancelaria de Stat, Ministerul Finanţelor, Ministerul Economiei.*

Pe data de 24 septembrie 2021 a fost desfășurată o ședință de lucru interinstituțională referitoare la crearea CERT-lui național și CERT-urilor departamentale, prezidată de către Viceprim-ministrul pentru digitalizare, dl. Iurie ȚURCANU, cu participarea reprezentanților I. P. Agenției de Guvernare Electronică, I. P. Serviciului Tehnologia Informaţiei şi Securitate Cibernetică și Serviciului de Informații și Securitate.

Riscurile aferente lipsei entității naționale responsabile pe domeniul securității cibernetice au fost evaluate de către Serviciul de Informații și Securitate, fiind elaborată o notă informativă în adresa beneficiarilor legali.

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

Instituții responsabile: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică, Cancelaria de Stat.*

În conformitate 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 HG nr. 414/2018, I.P. Serviciul Tehnologia Informaţiei şi Securitate Cibernetică a fost desemnat în calitate de Centru guvernamental de reacţie la incidente de securitate cibernetică (CERT Gov).

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
1/3	Stabilirea de către Centrul naţional de reacţie la incidente de securitate cibernetică a indicatorilor din domeniul securităţii cibernetice: a) sistematizarea datelor statistice la capitolul securităţii cibernetice, analiza şi evaluarea acestora	Perioada 2021-2023, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică.*

În conformitate cu HG nr. 482 din 08.07.2020, a fost convenit și stabilit un mecanism interinstituțional de remitere în adresa SIS a datelor statistice relevante privind incidentele de securitate cibernetică din spaţiul cibernetic Guvernamental, consecinţele cărora comportă riscuri de securitate cibernetică asupra entităţilor publice care deţin infrastructuri și sisteme de tehnologia informaţiei şi comunicaţii.

Informațiile și datele privind incidentele de securitate cibernetică survenite în spaţiul cibernetic, ale căror consecinţe afectează securitatea cibernetică a infrastructurilor TIC gestionate de către SIS, sunt analizate și sistematizate în regim continuu de către Echipa de răspuns la incidentele de securitate cibernetică a Serviciului.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
1/4	Elaborarea mecanismelor de creare şi consolidare a centrelor departamentale de reacţie la incidente de securitate cibernetică şi informaţională, atât de drept public, cât şi de drept privat	Perioada 2021-2023, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică.*

În calitate de Centru guvernamental de reacţie la incidente de securitate cibernetică (CERT–GOV), I. P. STISC în limitele competențelor funcționale, a solicitat oficial pe parcursul anului 2021 autorităților publice desemnarea persoanelor responsabile pentru colaborarea cu acestea pe aspecte ce țin de securitate cibernetică.

SIS a întreprins măsurile necesare pentru consolidarea capacităților instituționale de răspuns la incidente de securitate cibernetică.

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

Instituția resonsabilă: *Ministerul Economiei.*

Cu suportul experților proiectului Uniunii Europene „Cybersecurity East”, un obiectiv al căruia este asistarea țărilor-membre ale Parteneriatului Estic în transpunerea Directivei NIS, de către Ministerul Economiei a fost elaborată redacția inițială a proiectului de lege-cadru 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 UE (Directiva NIS). Actualmente proiectul respectiv este în proces de translare în limba română și ajustare la rigorile naționale.

Totodată, în contextul realizării Acordului de parteneriat încheiat între proiectul „Future Technologies Activity” al USAID Moldova și Ministerul Economiei privind stabilirea unui cadru de cooperare pentru dezvoltarea unui mediu de afaceri favorabil pentru sectoarele IT și inginerie, economia digitală și comerțul electronic, a fost solicitată asistența tehnică și expertiză în scopul realizării Analizei de impact la proiectul de lege privind securitatea rețelelor și sistemelor informaționale, conform HG nr. 23/2019, cât și elaborării documentelor necesare aplicării prevederilor proiectului de lege.

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

Instituții responsabile: *Agenţia de Guvernare Electronică; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică.*

În contextul sistematizării datelor privind statutul implementării recomandărilor de audit, în conformitate cu pct. 10 subpct. 4) și pct.11 subpct. 11) și 13) din Statutul AGE, aprobat prin HG nr. 760/2010, cu modificările introduse prin HG nr. 414/2018 „Cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat”, AGE a solicitat în trimestrul III al anului 2021 de la entitățile auditate să informeze referitor la realizarea recomandărilor misiunii de audit de securitate cibernetică, cu prezentarea dovezilor concludente (raport detaliat sau sumativ privind remedierea neconformităților).

Până în luna decembrie 2021, din 13 entități auditate – 5 entități au prezentat statutul remedierii neconformităților, 2 entități au informat că urmează să elaboreze un plan de acțiuni în contextul modificărilor structurale guvernamentale, iar 6 entități nu au răspuns la solicitarea AGE.

Ca urmare a solicitării repetate, au răspuns 2 entități: Ministerul Agriculturii și Industriei Alimentare – a raportat despre lipsa specialiștilor în domeniu, iar Ministerul Mediului a informat despre inițierea unor măsuri de securitate cibernetică, care urmează a fi implementate în anul 2022.

Ca rezultat al evaluării preliminare, conform celor raportate de autoritățile publice, se constată că unele entități au reacționat prompt și au planificat/ realizat o parte considerabilă din recomandările misiunilor de audit (CS, MAEIE, MA, CTIF și MF).

În anul 2021, SIS a avizat 2 documente privind politica de asigurare a securității cibernetice în cadrul Ministerului Afacerilor Externe și Integrării Europeneși Ministerul Justiției.

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 contextul serviciilor electronice publice, prestate de către autoritățile și instituțiile guvernamentale, evaluarea aplicării Cerințelor minime de securitate cibernetică de nivelul II în cadrul acestora, s-a efectuat prin corelarea recomandărilor misiunilor de audit, efectuate în 2019 în autoritățile publice, cu cerințele HG nr. 201/2017 și furnizarea soluțiilor/recomandărilor de remediere a neconformităților identificate în rapoartele de audit pentru fiecare entitate auditată.

Cu referință la serviciile electronice publice prestate de către AGE, au fost contractate serviciile unei companii de consultanță, specializate în domeniu, pentru testarea securității sistemelor informaționale aflate în gestiunea AGE, în conformitate cu standardele și practicile internaționale, care acoperă cerințele de securitate cibernetică stipulate în HG nr. 201/2017.

Astfel, au fost efectuate teste de securitate, inclusiv de penetrare și evaluare a codului sursă, pentru sistemele MPay, MNotify și MPower, iar rezultatele testelor cu recomandările de rigoare au fost preluate în lucru pentru înlăturarea neconformităților identificate.

Totodată, în trimestrul IV al anului 2021 au fost efectuate teste de securitate pentru alte 3 sisteme: SI „Înregistrarea cu Statut de Șomer”, SI „Determinarea Dizabilității și Capacității de Muncă”, SI „Registrul Unităților de Instruire a Conducătorilor de Vehicule și Formabililor”. Rezultatele testelor efectuate sunt în proces de coordonare cu responsabilii/ managerii produselor respective și urmează

definitivarea acțiunilor de remediere a neconformităților, în termenii și modul stabilit în cadrul AGE.

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	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de referință, experții Serviciului de Informații și Securitate au efectuat patru întrevederi cu persoanele responsabile din subdiviziunile specializate ale companiilor de telecomunicații/ agențiile mass-media şi alţi furnizori de servicii informaţionale privind stabilirea mecanismului de sesizare reciprocă în scopul prevenirii şi combaterii pericolelor în spaţiul cibernetic.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
2/4	Identificarea unui mecanism legal de 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 2020-2022, cu verificarea anuală a indicatorilor de progres	Parțial realizat

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

Acțiunea este reglementată la nivel normativ de HG nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică, pentru achiziția de către autoritățile publice a sistemelor informaționale noi sau actualizarea celor existente. Totodată, Ordinul Directorului SIS nr. 25/2017 Regulamentul cu privire la avizarea dispozitivelor și produselor asociate semnăturii electronice, stabilește procedura de obținere a accesului la codul sursă al produselor de program utilizate în procesul prestării serviciilor de certificare a cheii publice.

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 protecția implicită a datelor atunci cînd se elaborează, se proiectează, se selectează și se utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează astfel de date în corespundere cu legislația privind protecția datelor cu caracter personal	Perioada 2019-2020, cu verificarea anuală a indicatorilor de progres	Realizat

Instituția responsabilă: *Autoritățile administrației publice.*

Cu referință la 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 începând de la conceperea acestora și protecția implicită a datelor atunci când se elaborează, se proiectează, se selectează și se utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează astfel de date în corespundere cu legislația privind protecția datelor cu caracter personal, în perioada anului 2021 CNPDCP a avizat proiectele de acte normative, prezentate spre examinare de catre autoritățile administrației publice, prin care a intervenit cu propuneri în vederea implementării principiilor de protecție a datelor cu caracter personal, prevăzute de Legea nr. 133/2011.

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

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

Conform obiectivului acțiunii, pe parcursul anului 2021 s-au realizat următoarele acțiuni:

- la data de 25.11.2021 a avut loc ședința comună a reprezentanților MA, SIS, STISC pentru discutarea mecanismelor și metodelor de asigurare a securității cibernetice;
- s-a propus includerea în legea 345/2003, cu privire la apărarea națională, a atribuțiilor Ministerului Apărării și Marelui Stat Major al Armatei Naționale pe domeniul securității și apărării cibernetice.

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

În perioada de referință, SIS a identificat vulnerabilități și riscuri în sistemele interne de comunicații și informatică ale Armatei Naționale. Pe aspectele menționate, SIS a informat Ministerul Apărării și a înaintat propuneri de remediere a situației în ansamblu.

Potrivit experților SIS, elaborarea măsurilor de securitate cibernetică pentru infrastructurile critice naționale urmează a fi realizate după aprobarea cadrului normativ aferent infrastructurii critice naționale.

În anul 2021, Serviciul a definitivat și remis în adresa Guvernului RM „Proiectul Programului național de consolidare și realizare a măsurilor de protecție antiteroristă a obiectivelor infrastructurii critice pentru anii 2021-2025” și „Proiectul Planului de implementare a Programului național de consolidare și realizare a măsurilor de protecție antiteroristă a obiectivelor de infrastructură critică pentru anii 2021-2025”. În context, SIS a expediat scrisoarea nr. 7/3-4197 din 08.11.2021 în adresa MIDR, desemnat ca instituție responsabilă de definitivarea și avizarea proiectelor menționate.

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	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate*

În perioada de referință, SIS a elaborat proiectul „Ghidului privind modalitatea de evaluare și autorizare/certificare a sistemelor informaționale ce prelucrează informații atribuite la secret de stat”. Acesta urmează a fi publicat după operarea unor modificări la HG 1176/2010 pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice.

Pe parcursul anului 2021, Serviciul a acordat suport de competență subdiviziunilor de protecție a secretului de stat şi a componentei TIC ce țin de sistemele de apărare naţională, fiind perfectate 26 de avize.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de referință, SIS a achiziționat o serie de echipamente ce urmează să consolideze securitatea sistemelor speciale de comunicații electronice.

Concomitent, Serviciul a evaluat sistemele de comunicații speciale ale Forțelor Armatei Naționale, care necesită aplicarea unor mecanisme de protecție criptografică și tehnică.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de referință au fost efectuate modificări la cadrul normativ intern al Serviciului pentru operaționalizarea subunității specializate în efectuarea controalelor și misiunilor de audit de securitate a sistemelor speciale de comunicații electronice.

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.*

Pe parcursul anului 2021, în adresa SIS nu au parvenit solicitări de revizuire și modificare a cadrului normativ, dat fiind faptul că ultimele actualizări au avut loc 2020, prin HG nr. 965/2020.

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 protecţiei datelor cu caracter personal în contextul asigurării securităţii cibernetice	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Parțial realizat

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

Prin Legea nr. 175/2021 pentru modificarea unor acte normative, în vigoare din 10.02.2022, au fost introduse modificări la Legea nr. 133/2011 privind protecția datelor cu caracter personal. Astfel, prin actul normativ menționat supra, au fost stabilite reglementări cu privire la obligația desemnării persoanelor responsabile cu protecția datelor cu caracter personal în cadrul persoanelor juridice de drept public și de drept privat și instituirea obligației privind evaluarea impactului asupra protecției datelor.

În cadrul SIS protecția datelor cu caracter personal este asigurată în conformitate cu prevederile actelor normative interne.

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.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

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

Totodată, în perioada vizată, de către experții SIS a fost verificată conformitatea condițiilor de licențiere a **6 agenți economici** cu genul de activități aferente importului și comercializării produselor de protecție criptografică și prestarea serviciilor de protecție criptografică.

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 protecție a informației	Perioada 2020-2023, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În anul 2021, SIS a continuat implementarea acțiunilor ce țin de cooperarea cu Serviciul Vamal în vederea stabilirii unui sistem fiabil de monitorizare a importului mijloacelor de protecție a informației.

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 a indicatorilor de progres în cazul realizării înainte de termen	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În rezultatul elaborării de către SIS în anul 2020 a proiectului Legii privind identificarea electronică și serviciile electronice de încredere, înregistrat la Cancelaria de Stat cu nr. 480/2020, acesta a fost remis Guvernului RM pentru avizare și promovare.

Prin aprobarea proiectului de lege expus, se va transpune Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului Europei din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

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 anul 2021 a fost realizat un control al prestatorului de servicii de certificare din cadrul I.P. STISC.

În semestrul I al anului 2021, SIS a recepționat „Raportul de activitate a prestatorilor de servicii de certificare în domeniul aplicării tuturor tipurilor de semnături electronice pentru perioada anului 2020". În rezultatul analizei efectuate, Serviciul a informat Cancelaria de Stat privind utilizarea neconformă de către I.P. AGE și I.P. STISC a certificatelor de securitate în cadrul sistemelor informaționale guvernamentale, neconformitățile fiind ulterior eliminate de către entitățile publice.

Concomitent, în rezultatul controlului efectuat la prestatorul de servicii de certificare din cadrul I.P. STISC au fost depistate 3 încălcări ale Cadrului normativ în domeniul aplicării semnăturii electronice. În acest sens, Serviciul a emis o prescripție de remediere a deficiențelor depistate, care, ulterior, în cadrul controlului repetat, s-a constatat că prestatorul le-a eliminat.

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

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției), Procuratura Generală.*

În anul 2021 au fost instruiți **51** de angajați ai Ministerului Afacerilor Interne în cadrul a 21 de cursuri și webinare.

Totodată, în perioada de referință, ofițerii Direcției investigare infracțiuni informatice a INI al IGP al MAI au participat și acordat suport în cadrul a 3 acțiuni comune de investigații cu caracter internațional, după cum urmează:

- Suport acordat Departamentului Național de Investigații Criminale al Unității Naționale Olandeze, în vederea identificării și acumulării probelor

necesare pentru documentarea unui grup infracțional specializat în comercializarea drogurilor și anabolizantelor prin intermediul platformei DutchMasters din Darknet. Activitatea grupării a fost documentată de mai mult timp de forțele de ordine din Olanda, perioadă în care au fost acumulate o parte din informațiile pertinente, care demonstrează activitatea infracțională a membrilor grupării, manifestată prin comercializarea drogurilor prin intermediul Darknet. Astfel, au fost documentați șase membri ai grupului infracțional, originari din Amsterdam, Diemen și Assendelft, cu vârsta cuprinsă între 33 și 51 de ani;

- Suport acordat autorităților de aplicare a legii din Republica Federală Germania privind blocarea accesului la 9 servere hostate la o companie de hosting din Republica Moldova, pe care activa o platformă DarkNet. Această platformă este cunoscută la nivel internațional infractorilor pentru posibilitatea comercializării-achiziționării în principal a drogurilor, mijloace valutare contrafăcute, date despre carduri de credit furate sau contrafăcute, carduri SIM anonime și programe malware. Astfel, coordonarea acțiunilor a fost efectuată în baza solicitării de asistență juridică internațională parvenită din partea autorităților germane, precum și în urma unei colaborări eficiente cu Departamentul Central de Investigații Criminale din orașul german Oldenburg;

- Suport acordat autorităților de aplicare a legii din Republica Franceză. În urma măsurilor întreprinse, studierii fluxului de tranzacții realizate de pe anumite portofele electronice a fost identificat un cetățean moldovean. Drept rezultat au fost efectuate 2 percheziții în RM.

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: 34.

În perioada anului 2021, de către instanțele de fond au fost examinate 34 cauze penale cu pronunțarea sentințelor: Art. 177 CP – 6 cauze penale; Art. 208^1 CP – 26 cauze penale; Art.185^1 CP- 1 cauză penală și Art.185^2 CP- 1 cauză penală.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securității spațiului informațional-cibernetic și investigarea criminalității informatice**			
6/2	Acordarea ajutorului metodico-practic subdiviziunilor teritoriale privind investigarea infracțiunilor informatice	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției), Procuratura Generală.*

În perioada anului 2021, angajații Poliției au participat în calitate de formatori în cadrul a 8 sesiuni de instruire, fiind instruite 55 de persoane.

Procuratura Generală a elaborat proiectul „Ghidului privind metodica de investigare a infracțiunilor informatice și în domeniul telecomunicațiilor”.

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	Realizat

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției), Procuratura Generală.*

Procuratura Generală – a fost modificat art. 270 lit. c) din Codul de procedură penală al Republicii Moldova, competența exclusivă a procurorului la exercitarea urmăririi penale pe domeniul crimelor informatice și de telecomunicații.

- A fost creată subdiviziunea specializată Secția tehnologii informaționale și combaterea crimelor cibernetice din cadrul Direcției urmărire penală și criminalistică a Procuraturii Generale.

- Constituit Biroul anti-trafic și de investigare a crimelor cibernetice din cadrul PCCOCS.

- 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.

SIS – Mecanismul de cooperare cu partenerii externi este funcțional. În perioada de referință au fost realizate întrevederi cu reprezentații serviciilor speciale partenere, ce au rezultat în schimb de informații pe aspecte de interes comun și preluarea de bune practici în domeniul combaterii criminalității informatice.

În perioada de bilanț, de către SIS au fost instrumentate un șir de investigații în domeniul criminalității informatice. A fost inițiat 1 dosar penal, demarate 3 procese penale și 1 dosar contravențional.

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

Instituții responsabile: *Ministerul Finanţelor, Ministerul Afacerilor Interne.*

Cadrul legal actual de salarizare poartă un caracter unitar, transparent, echitabil, nediscriminatoriu, capabil să reflecte și să remunereze performanța profesională din domeniul de activitate. 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 pentru anul 2022, urmând a fi analizată în complex

modificarea condițiilor salariale în sensul asigurării tratamentului egal și a remunerării echitabile 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

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliției), Procuratura Generală.*

În perioada anului 2021 au fost înregistrate și investigate 37 cazuri de abuz sexual în mediul online asupra copiilor, comparativ cu 43 cazuri în anul 2020, dintre care:

-art.208[1] Cod penal (*Pornografia infantile*) – 31 cazuri;
-art.173 Cod penal (*Hărțuirea sexuală*) – 3 cazuri;
- art. 174 Cod penal *(Raportul sexual cu o persoană care nu a împlinit vârsta de 16 ani)* – 1 caz;
-art. 175 Cod penal (*Acțiuni perverse*) – 1 caz;
-art.175[1] Cod penal (*Ademenirea minorului în scopuri sexuale*) – 1 caz.

Numărul copiilor protejați, precum și a celor care beneficiază de asistență:

În perioada de raport de către angajații poliției a fost acordată asistență pentru 2 minori și audierea cu participarea psihologului din cadrul CI „La Strada” a 5 minori.

Subsecvent, în perioada anului 2021, de către angajații Poliției au fost realizate 22 activități de instruire, în cadrul cărora au fost instruiți 16 ofițeri.

Totodată, ofițerii Direcției investigare infracțiuni informatice (DIII) a INI al IGP al MAI au participat în calitate de formatori la instruirile organizate pentru judecători și procurori, după cum urmează:

1. La 02.06.2021, un ofițer al DIII a participat în calitate de formator în cadrul cursului de instruire online „Metodici și tactici de investigare și examinare a cauzelor privind infracțiunile cu caracter sexual comise prin intermediul tehnologiilor informaționale. Aspecte privind abuzul online a minorilor”, care s-a desfășurat în incinta Institutului Național al Justiției;

2. La 03-04.06.2021, doi ofițeri din cadrul DIII, dintre care 1 în calitate de formator, au participat în cadrul evenimentului regional de instruire online privind investigarea cazurilor de exploatare și abuz sexual asupra copiilor în mediul online pentru organele de drept, organizat de CoE în cadrul proiectului „EndOCSEA@Europe;

3. La 14.06.2021, un reprezentat al DIII a participat în calitate de formator în cadrul cursului de instruire online „Metodici și tactici de investigare și examinare a cauzelor privind infracțiunile cu caracter sexual comise prin intermediul tehnologiilor informaționale. Aspecte privind abuzul online a minorilor”, organizat de Institutului Național al Justiției;

4. La 15.06.2021, un reprezentant al DIII a participat în calitate de formator în cadrul cursului de instruire online „Investigarea infracțiunilor cu caracter sexual săvârșite de minori și împotriva minorilor”, organizat de Institutului Național al Justiției;

5. La 23-25.06.2021, un reprezentant al DIII a participat în calitate de formator în cadrul Cursului introductiv de instruire pentru judecători și procurori în domeniul criminalității informatice și al probelor electronice, Organizat de către Institutul Național al Justiției cu suportul proiectului „CyberEast” al CoE.

Procuratura Generală – pentru art. 208[1] din Codul penal al RM în 2021 a fost înregistrat un număr de 40 de cazuri. Cauze transmise în judecată – 26. Sentințe de condamnare – 34.

Ministerul Educației și Cercetării – în colaborare cu Centrul Intenațional „La Strada” au desfășurat cu regularitate activități de informare a elevilor, părinților, cadrelor didactice, psihologilor școlari despre riscurile online la care se pot expune copiii și măsuri de protecție a acestora. Au fost promovate reguli de securitate online, instrumente practice și utile în filtrarea conținuturilor dăunătoare și ilegale ce pot fi accesate de copii, dar și recomandări pentru siguranța copilului online. Au fost elaborate materiale informaționale cu recomandări despre siguranța copilului online, resurse didactice, ghiduri pentru profesori, adaptate categoriei de vârstă a copilului. A fost promovat continuu portalul informațional și serviciul de consiliere a copiilor în situații de risc online www.siguronline. md.

Mii de copiii au fost informați direct, de către specialiștii Centrului Internațional „La Strada” despre cum sa recunoască riscurile online și să le facă față. Elevii au beneficiat de o abordare adaptată categoriei de vârstă și au aflat despre următoarele aspecte ale siguranței online: imaginea și reputația online, comunicarea și prieteniile online, relațiile online, etc.

A fost desfășurată în continuare Campania cu privire la prevenirea violenței în școală, precum și în mediul online, în colaborarea cu UNICEF, CA Coliseum și TN „M.Eminescu”. În perioada 2020-2021 (cu întrerupere din cauza pandemiei) au fost prezentate elevilor, gratuit 20 de spectacole „Corp de copil”. A fost creat un nou spectacol tematic „1000 de îngeri”, bazat pe cazuri reale care au avut loc.

În februarie-martie 2021 a fost desfășurat concursul pentru elevi „Pentru un internet mai bun”, în colaborare cu CI „La Strada”. La fel, în octombrie, anual, în cadrul instituțiilor de învățământ general din țară se desfățoară lunarul Securității cibernetice.

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

Instituţii responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei), Procuratura Generală.*

Cazuri investigate grooming de către IGP al MAI – în perioada anului 2021, subdiviziunea DIII a înregistrat 3 cazuri de hărțuire sexuală a copiilor în mediul online.

Procuratura Generală – Pentru art. 175[1] din Codul penal al RM, în anul 2021, au fost pronunțate 2 sentințe față de 2 persoane.

Pentru anul 2021, de către instanțele de judecată au fost pronunțate 12 sentințe de condamnare în baza art. 173 Cod 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 şi încurajarea raportărilor prin proiecte informaţionale specializate	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei), Procuratura Generală.*

În perioada de raport, de către angajații poliției au fost realizate următoarele acțiuni:

- La 23.04.2021, un ofițer a participat în cadrul elaborării documentelor curriculare la disciplina opțională „Educație pentru socializare juridică” pentru clasa a XI-a, fiind pregătită și transmisă informația cu tematica „Prevenirea infracțiunilor online”;
- La 14.05.2021, un ofițer a realizat o prezentare privind siguranța online a copiilor în cadrul evenimentului online privind ”Ziua internațională a familiei”, organizat de USM, subiectul abordat în anul curent fiind ”Familia digitală”;
- În perioada 23-24.06.2021, reprezentanții Poliției au participat la atelierele și conferința de finalizare a primului an de pilotare a disciplinei opționale „Educație pentru socializare juridică” pentru clasa a XI-a, organizată de „PH International”, în incinta Institutului Muncii;
- La 30.07.2021, au fost realizate activități de informare a copiilor privind riscul abuzului sexual online, în cadrul acțiunilor de prevenire în comun cu CCTP al INI și INSP, în or. Vadul lui Vodă și r-ul Ialoveni;
- La 28-29.12.2021, un ofițer a participat la atelierul de lucru în cadrul proiectului „Socializare juridică în școli”.

Subsecvent, în perioada anului 2021, de către subdiviziunea DIII au fost desfășurate 4 acțiuni de prevenire și informare, după cum urmează:

- La 30.01.2021, un ofițer al DIII în comun cu un reprezentant al Secției siguranță minori a INSP au realizat o lecție de prevenire privind riscurile online în privința copiilor, la organizația de tineret din cadrul Crucii Roșii din Moldova;
- La 15.02.2021, un ofițer a participat în calitate de specialist la lecția de informare, cu tematica „Securitatea în mediul virtual”, desfășurată on-line pentru elevii claselor a VII-a din cadrul LT „Prometeu”;
- La 19.02.2021, 2 ofițeri au realizat o lecție privind siguranța online a copiilor pentru elevii clasei a V-a din cadrul Liceului „Mihai Viteazul”, din mun. Chișinău. Participanți - 20 elevi;

- La 20.02.2021, un ofițer din cadrul DIII a participat în calitate de formator la training-ul organizat de către Crucea Roșie Moldova cu tematica: „Securitatea online pentru tineri și copii” în mun. Chișinău;

De asemenea, pe pagina oficială a poliției au fost publicate 4 comunicate privind siguranța copiilor în internet, și 4 participări la emisiuni/interviuri, după cum urmează:

- La 28.01.2021 a fost elaborat un comunicat de presă privind riscurile transmiterii de către copii a datelor personale către utilizatorii necunoscuți din Internet, inclusiv urmate de abuz sexual online, precum și privind infracțiunile informatice comise cu utilizarea datelor personale. Comunicatul este elaborat în contextul Zilei Europene a Protecției Datelor, sărbătorită anual pe 28 ianuarie https://politia.md/ro/content/28-ianuarie-ziua-europena-protectiei-datelor;
- La 11.02.2021 a fost plasat un comunicat de presă pe pagina web a Poliției în contextul „Zilei siguranței pe internet” https://politia.md/ro/content/ziua-sigurantei-pe-internet-2021
- La 02.08.2021 pe pagina oficială a IGP și Facebook a IGP, INI, DIII a fost mediatizată informația: Mii de fișiere cu pornografie infantilă, ridicate de ofițerii de investigații https://politia.md/ro/content/siguranta-copiilor-lumea-virtuala-sute-de-copii-instruiti-de-politisti ;
- La 16.11.2021, pe pagina oficială a IGP și Facebook a IGP și INI, a fost mediatizat comunicatul: 18 noiembrie - Ziua Europeană pentru Protecția Copiilor împotriva Exploatării Sexuale https://politia.md/ro/content/18-noiembrie-ziua-europeana-pentru-protectia-copiilor-impotriva-exploatarii-sexuale

Interviuri:

- La 14.01.2021, un ofițer din cadrul secției nr. 3 IIPI a acordat un interviu pentru postul de televiziune „Prime TV”, Primele Știri cu referire la siguranța online a copiilor, sediul INI;
- La 04.02.2021, un ofițer din cadrul DIII a oferit două interviuri cu tematica: ”Sustrageri frauduloase de pe carduri”, TV8, Canal 2;
- La 24.02.2021, un ofițer din cadrul DIII a oferit un interviu telefonic la radio ”Sputnik”, emisiunea ”Atitudini”, cu tematica: Siguranța în mediul online – cum prevenim riscurile și protejăm copiii de pericolele internetului; https://sputnik.md/20210224/Emisiunea-ATITUDINI-33753583.html
- La data de 28.03.2021, un ofițer din cadrul DIII a acordat interviu pentru portalul „Oameni și Kilometri”, cu referire la fenomenul de abuz sexual online asupra copiilor https://oamenisikilometri.md/copiii-abuzului-sexual-online/

În cadrul Institutului Național al Justiție, Procuratura Generală în calitate de formator, semestrial desfășoară cursuri de instruire cu tematica „Metodici și tactici de identificare, investigare și judecare a infracțiunilor săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale”; „Particularitățile urmăririi penale și judecării cauzelor privind infracțiunile în domeniul informaticii și telecomunicațiilor”.

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

Instituții responsabile: *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 efectuează permanent schimb de informații cu Departamentele de securitate ale instituțiilor financiare.

De asemenea, la data de 12.08.2021, Șeful Secției Investigații mijloace de plată electronice din cadrul DIII, de comun cu reprezentanți ai Secției prevenire a INSP al IGP, au realizat o ședință comună cu reprezentanții Băncii Naționale a Moldovei, în cadrul căreia s-a discutat asupra necesității intervenției comune în vederea informării populației și prevenirii cazurilor de fraude cu utilizarea cardurilor de plată și altele, prin semnarea unui acord comun.

Inspectoratul General al Poliției își propune planificarea și organizarea la nivel național, a unei campanii de informare a comunității, care va avea drept scop diminuarea considerabilă a numărului de persoane care au devenit victime a sustragerilor de bani de pe carduri.

Drept rezultat, la 22.09.2021, prin scrisoarea nr. 27-001/38/2832, BNM s-a expus pozitiv supra celor discutate în cadrul ședinței și a informat DIII a INI a IGP privind colaborare benefică prin întreprinderea unor acțiuni comune în vederea creșterii nivelului de culturalizare financiară a populației, elaborarea de către BNM a unor broșuri informative despre sistemul de plăți online, organizarea unor ateliere comune, precum și desfășurarea unor vizite comune în toate zonele Republicii Moldova.

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

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei), Procuratura Generală.*

În perioada de referință, angajații poliției au desfășurat următoarele activități comune cu instituțiile bancare, după cum urmează:

- La 12.03.2021, a fost organizată o ședință comună cu reprezentanții IGP-BNM – Asociația Băncilor, la care a participat Guvernatorul Băncii Naționale, Octavian ARMAȘU, unde s-a decis crearea unui grup comun de lucru privind fraudele bancare.

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

- La 21.12.2020, a fost efectuată o sesizare în adresa BNM, Asociației Băncilor din Republica Moldova privind creșterea în domeniul fraudelor cu utilizarea cardurilor bancare, solicitând implementarea unor noi masuri de securitate.

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	Realizat

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei), Procuratura Generală.*

Evaluarea datelor privind numărul și valoarea fraudelor înregistrate și raportate BNM, relevă faptul că pe parcursul primelor 6 luni ale anului 2021, fraudele cu cardurile contrafăcute sunt în descreștere în raport cu anii precedenți în perioada similară, 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 instituția financiară B.C. Moldova – Agroindbank, în sumă totală de 32.887 lei.

Procuratura Generală de comun cu Banca Națională a Republicii Moldova, în acordul privind schimbul de informații a prevăzut mecanismele comune de combatere a fraudelor cu card și fără card.

Totodată, Procuratura Generală a elaborat proiectul de lege pentru modificarea unor acte normative prin care s-au propus instituirea răspunderii penale pentru primirea, deținerea sau folosirea în instituțiile penitenciare, de către deținuți a telefoanelor mobile, altor mijloace de comunicare la distanță, cartele SIM și suporturi de stocare a datelor, care pot fi folosite în tranzacțiile cu card și fără card.

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

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei), Procuratura Generală, Serviciul de Informatii și 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, creată prin ord. IGP 429 din 07.11.2019.

Totodată, pe parcursul perioadei de raport, în cadrul Direcției de poliție a mun. Chișinău, a fost creat un serviciu specializat, responsabil de investigarea 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.

Procuratura Generală - a fost creată subdiviziunea specializată- Biroul anti-trafic și de investigare 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.

Capacitățile SIS în combaterea criminalităţii informatice sunt funcționale și în proces de modernizare, îmbunătățire și dezvoltare continuă. În anul 2021, în vederea consolidării capacităților instituționale în combaterea criminalității informatice, de către Institutul Național de Informații și Securitate „Bogdan, Întemeietorul Moldovei” au fost formulate și înaintate propuneri pentru promovarea unor Programe de instruiri specializate adresate angajaților SIS.

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 naționale privind evoluția fenomenului criminalității informatice	2022, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Procuratura Generală, Serviciul de Informatii și Securitate, Ministerul Afacerilor Interne.*

Procuratura Generală a planificat și a inclus în Planul de activitate a Procuraturii, pentru anul 2022, crearea unei baze de date naționale privind evoluția fenomenului criminalității informatice.

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

Instituția responsabilă: *Ministerul Afacerilor Interne (Serviciul Tehnologia Informației).*

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.

Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
9/4	Elaborarea cadrului normativ care să reglementeze instituirea Sistemului informaţional automatizat „E-dosar” în cadrul organelor implicate în efectuarea urmăririi penale şi judecarea cauzelor, precum şi implementarea, dezvoltarea şi interconectarea acestuia	Perioada 2019-2021, cu verificarea anuală a indicatorilor de progres	Realizat

Instituţia responsabilă: *Procuratura Generală.*

Procuratura Generală a elaborat și implementat cadrul normativ care reglementează instituirea Sistemului informațional automatizat „E-dosar”, prin modificarea art. 8 și art.11 ale Legii nr.3 din 25.02.2016 cu privire la Procuratură.

În cadrul organelor implicate la efectuarea urmăririi penale și judecarea cauzelor, precum și implementarea, dezvoltarea și interconectarea acestuia:

1. Ordinul comun Procuratura Generală, Ministerul Afacerilor Interne, Ministerul Justiției, Serviciul Vamal, Centrul Național Anticorupție, nr.27/310/956/361-0/154 din 05.10.2016 privind formarea Grupului de lucru pentru implementarea sistemului informațional automatizat E-dosar.

2. Ordinul comun Procuratura Generală, Ministerul Afacerilor Interne, Ministerul Justiției, Centrul de Telecomunicații Speciale, nr. 922/57/315/31 din 26.10.2017 cu privire la formarea Grupului de lucru pentru asigurarea interoperabilității PIGD cu alte sisteme informaționale guvernamentale.

Pe parcursul anului 2021, în cadrul SIS au fost perfectate documentele necesare privind accesul la Sistemul informațional automatizat „E-dosar”. În acest context, Serviciul va iniția procedura de interconectare la SIA „E-dosar” după darea în exploatare a acestuia.

Concomitent, a fost perfectat *Acordul de colaborare cu Agenția de Administrare a Instanțelor Judecătorești (AAIJ)*, cu privire la accesul la portalul național al Instanțelor de judecată.

Nr *(din Plan)*	**Acţiunea**	**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	Realizat

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

În conformitate cu Programul național în domeniile cercetării și inovării pentru anii 2020-2023 și a Planului de actiuni privind implementarea acestuia, aprobat prin HG nr. 381/2019, realizarea cercetărilor științifice în domeniile tehnologiei informaționale și comunicaționale, orientate spre dezvoltarea tehnologiilor și sistemelor informatice avansate și a soluțiilor inovative, are loc in conformitate cu una dintre prioritățile strategice – „COMPETITIVITATE ECONOMICĂ și TEHNOLOGII INOVATIVE”, în cadrul căreia este în derulare proiectul realizat de către Institutul de Matematică și Informatică „Vladimir Andrunachievici” – Sisteme informatice inteligente pentru soluționarea

problemelor slab structurate, procesarea cunoștințelor și volumelor mari de date, conducător științific – dr. hab. Constantin GAINDRIC.

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

Instituții responsabile: *Serviciul Tehnologia Informației și Securitate Cibernetică.*

În perioda de referință de către I. P. STISC au fost realizate următoarele acțiuni:

- A fost lansată o campanie de informare în domeniul securității cibernetice dedicate Lunii europene a securității cibernetice;
- Au fost plasate 2 ghiduri de informare pe pagina web oficială https://stisc.gov.md;
- Au fost publicate 2 anunțuri pe rețelele de socializare și pagina oficială a STISC;
- Au fost desfășurate 2 sesiuni de instruire în colaborare cu Crucea Roșie cu privire la igiena cibernetică a copiilor și tinerilor.

În calitate de partener la realizarea acțiunii respective, Agenția de Guvernare Electronică a continuat în anul 2021 acțiunile de sensibilizare şi informare a societății privind amenințările, vulnerabilitățile şi riscurile la adresa securității cibernetice.

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

La inițiativa SIS, au fost lansate mai multe campanii de informare a societății civile, beneficiarilor legali, mass-media, prin intermediul rețelei de socializare „Facebook”. Tematicile abordate au avut la bază subiecte de informare a grupurilor țintе, privind pericolele din spațiul informațional și în contextul asigurării securității cibernetice, după cum urmează:

- *Atacurile cibernetice SMISHING;*
- *Shopping online;*
- *Fenomenul știrilor de senzație (Breaking News);*
- *Protejarea rețelelor de socializare;*
- *Rețele WI-FI publice;*
- *Practici benefice de securitate cibernetică;*
- *Securitatea online și offline;*
- *Reguli de securitate online pentru copii.*
- *Tipuri de atacuri cibernetice;*
- *Amprenta digitală;*
- *Dark Web;*
- *Știri false și dezinformarea;*
- *Serviciile Cloud.*

În scopul monitorizării amenințărilor la adresa spațiului cibernetic național privind distribuirea știrilor false în contextul evoluției COVID-19 *(în perioada stării de urgență),* a fost elaborat al II-lea „***Ghid în vederea promovării consumului calitativ al știrilor de către societate”,*** plasat la 07.04.2021 pe site-ul **www.sis.md** și pe pagina de „Facebook” a instituției.

În anul 2021, MEC a elaborat și aprobat Standardele pentru protecția și siguranța copiilor/elevilor în mediul online (ordinul MEC nr. 872 din 12.07.2021). Standardele sunt menite să asigure implementarea Modelului de Școală Sigură Online – abordare comprehensivă a siguranței copiilor online în școală, preluată din bunele practici internaționale în domeniu.

În anul de studii 2021-2022 Standardele sunt pilotate în 6 instituții de învățământ din țară. După pilotare vor fi analizate rezultatele și dacă va fi cazul, acestea vor deveni obligatorii pentru toate instituțiile de învățământ din țară.

De menționat că implementarea acestor standarde va contibui și la atingerea obiectivelor stabilite în diverse acte normative naționale, dar și angajamente internaționale. În context, Convenția de la Lanzarote, ratificată de Republica Moldova în anul 2012, implementarea căreia constituie un angajament asumat pentru țara noastră.

Nr *(din Plan)*	**Acțiunea**	**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

Instituția responsabilă: *Serviciul Tehnologia Informației și Securitate Cibernetică.*

În perioada 27-29 septembrie 2021, I.P. STISC, în parteneriat cu „EU4Digital: Îmbunătățirea rezilienței cibernetice în țările Parteneriatului Estic” a organizat atelierul de lucru cu genericul „Offensive Social Engineering”.

În perioada 04-08 octombrie 2021, a fost desfășurat atelierul de instruire „CompTIA Cyber security Analyst (CySA+)”, în parteneriat cu CyberSecurity EAST project.

În perioada 16-17 noiembrie 2021, a fost organizat atelierul de lucru privind utilizarea eficientă a modelului de maturitate SIM3 pentru dezvoltarea capacităților de gestionare a incidentelor de securitate a informațiilor (CSIRT). Evenimentul a fost realizat în cadrul Programului „EU4Digital: Îmbunătățirea rezilienței cibernetice în țările Parteneriatului Estic”.

Pe parcursul anului 2021, reprezentanții Procuraturi generale au participat la următoarele evenimente:

- Masă rotundă cu referire la subiectul contractării amenințărilor hibride, 26.11.2021.
- Masă rotundă cu privire la politicile RM privind criminalitatea și securitatea cibernetică, 19.03.2021.
- ILEA Investigarea Crimelor Informatice, 24.08.2021- 26.08.2021.

În perioada 30.05.2021 - 01.06.2021, ofițerii SIS au participat la exercițiul online TTX „Coherent Resilience 2020”, organizat de Ucraina – NATO.

Nr *(din Plan)*	Acțiunea	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

Instituția responsabilă: *Serviciul Tehnologia Informației și Securitate Cibernetică.*

În perioada 20-21 Octombrie 2021, de către I.P. STISC a fost desfășurat atelierul de instruire pe tematica Protecția sistemelor de infrastructură critică, iar la data de 07 decembrie 2021, a fost desfășurat workshop despre practicile internaționale privind implementarea Regulamentului privind protecția datelor (DGPR).

În perioada de referință, au fost instruiți 10 ofițeri ai SIS, care au participat la 10 instruiri în domeniul asigurării securității cibernetice.

Reprezentanții Procuraturii Generale au participat la următoarele ateliere de lucru:

- Proiectul regional Acțiunea privind criminalitatea informatică pentru reziliența cibernetică în regiunea Parteneriatului Estic- CyberEast, 10.06.2021.
- The Role of the EU Cyber Ecosystem în Global Cybersecurity Stability, 17.05.2021-21.05.2021.
- Ședința de lucru a programului EU Digital, Improving Cyber Resilience in the Easter Partnership Countries, 17.12.2021.
- Atelier de lucru privind Cooperarea internațională privind Criminalitatea cibernetică, 01.03.2021-02.03.2021.

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

Instituția responsabilă: *Agenția Guvernare Electronică.*

În anul 2021 a fost continuat procesul de implementare a proiectului AGE – Platforma guvernamentală de instruire la distanță *(e-Learning)*, fiind un mecanism eficient și modern de instruire a angajaților prin crearea, dezvoltarea și punerea la dispoziție online a resurselor de instruire, cât și de acordare a accesului angajaților la informațiile destinate dezvoltării lor profesionale, inclusiv pe aspecte de securitate cibernetică.

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

Instituția responsabilă: *Serviciul Tehnologia Informației și Securitate Cibernetică.*

În anul 2021, I.P. Serviciul Tehnologia Informaţiei şi Securitate Cibernetică a lansat o campanie de informare în domeniul securității cibernetice dedicate Lunii europene a securității cibernetice.

În context, au fost plasate 2 ghiduri de informare pe pagina web oficială https://stisc.gov.md.

La fel, au fost publicate 2 anunțuri pe pagina Facebook a STISC.

Subsidiar, au fost desfășurate 2 sesiuni de instruire în colaborare cu Crucea Roșie cu privire la igiena cibernetică a copiilor și tinerilor.

Pe parcursul anului 2021, I. P. Agenția de Guvernare Electronică a continuat acțiunile de sensibilizare și informare a societății privind amenințările, vulnerabilitățile și riscurile la adresa securității cibernetice. În context, a oferit instruiri în acest domeniu pentru grupuri de persoane interesate, copii, tineri etc, sub formă de ateliere, webinare, la solicitare, și adaptate la nivelul de înțelegere și pregătire al beneficiarului.

În special, în luna octombrie 2021, acțiunile de sensibilizare s-au desfășurat sub sloganul „Gândește-te înainte de a da click” #ThinkB4UClick, iar Agenția de Guvernare Electronică (AGE) s-a alăturat acestui demers și, pe lângă activitățile curente desfășurate în acest sens, a participat la diverse evenimente organizate în sprijinul asigurării unui nivel înalt de securitate cibernetică al sistemelor informaționale publice și dezvoltării nivelului de cultură cibernetică al utilizatorilor, în contextul digitalizării intense și al trecerii pe online al activităților în perioada pandemiei.

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	Realizat

Instituția responsabilă: *Ministerul Educației și Cercetării.*

Pe parcursul anului 2021, a fost continuat procesul de elaborare a planurilor de studii și conținuturilor pentru anumite discipline de nivel de licență și master în domeniul Securității informației, fiind acreditate Programele de studii corespunzătoare palierului respectiv.

Concomitent, a fost desfășurat în continuare Programul „Intersecție. Zona Sigură Online”, care întrunește o comunitate de peste l000 cadre didactice. Programul este menit să susțină sistemul educațional în promovarea comportamentelor sigure ale copiilor în mediul online. În cadrul acestuia, în perioada anului 2021, au fost desfășurate mai multe activități, conferințe și ateliere de lucru în domeniul securității informaționale.

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

Instituția responsabilă: *Agenția Guvernarea Electronică*

În semestrul II al anului 2021, de către I. P. AGE a fost definitivată și dată în exploatare Platforma guvernamentală de instruire la distanță e-Learning (elearning.gov.md), fiind dezvoltate și publicate mai multe cursuri/module, printre care patru cursuri dedicate securității cibernetice, pentru diferite funcții din cadrul instituțiilor publice (manageri, utilizatori, administratori IT, dezvoltatori), și anume:

- Conștientizare generală în materie de securitate;
- Securitatea Informației pentru managerii instituțiilor publice;
- Securitatea Informației pentru administratorii de sistem;
- Securitatea Informației pentru dezvoltatori.

Pînă la data 31 decembrie 2021, erau înregistrați circa 440 de utilizatori la cursul „Conștientizare generală în materie de securitate”, dintre care 335 au finalizat cursul și au susținut testul final.

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	Realizat

Instituții responsabile: *Autoritățile administrației publice.*

În scopul asigurării securității spațiului informațional-mediatic, SIS a elaborat studiul analitic cu titlul: *„Comunicarea strategică în asigurarea securității naționale a Republicii Moldova”*. Studiul atestă că obiectivele de comunicare strategică pentru realizarea intereselor naționale ale Republicii Moldova urmează să contribuie pozitiv şi direct la realizarea cu succes a operațiunilor, misiunilor şi activităților SIS, prin integrarea în procesul de planificare strategică a a.n. *„STRATCOM-uri instituționale şi interinstituționale”*.

În perioada vizată, pe subiectele de interes național au fost identificate vulnerabilități cu caracter mediatic și informațional, cum ar fi:

- *amplificarea fenomenului „fake news”;*
- *extinderea activității extremiste pe dimensiunea spațiului informațional;*

- utilizarea tehnologiilor „new social-media" ce se află sub auspiciul centrelor ostile în scopul difuzării produselor de „fake news" cu caracter mediatic, propagandă agresivă şi mesaje extremiste în spaţiul online;
- lipsa bazei legislative relevante, ce ar permite în procesul comunicării strategice depistarea, prevenirea şi contracararea fenomenelor în sectorul mediatic şi informaţional.

În contextul evaluării provocărilor ce ţin de securitatea informaţională au fost elaborate studii şi produse analitice, în adresa beneficiarilor legali fiind remise informaţiile relevante privind:
- *vulnerabilităţile legislative;*
- *muşamalizarea veniturilor de pe piaţa mediatică;*
- *conexiunile cu factorul extern;*
- *conflicte de interese între companiile de publicitate şi televiziunile asociate.*

Nr *(din Plan)*	Acţiunea	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

Instituţia responsabilă: *Consiliul Audiovizualului.*

Comunicarea strategică este inclusă în Planul anual de activitate al MAEIE. De asemenea, Serviciul de presă al MAEIE a valorificat şi extins reţeaua de contacte, precum şi intensificat interacţiunea şi coordonarea interinstituţională cu următoarele grupuri a comunicatorilor de la nivel naţional şi internaţional:
- Consiliul Naţional de Comunicare constituit pe lângă Parlamentul Republicii Moldova;
- Grupul de comunicare strategică pe lângă Guvernul Republicii Moldova;
- Grupul Naţional de Comunicare COVID-19;
- Taskforce East StratCom al Serviciul european de acţiune externă;
- Reţeaua europeană pentru diplomaţie digitală;
- Grupul de lucru al comunicatorilor al SM GUAM, inclusiv crearea din septembrie 2021 a Grupului de comunicare strategică al SM GUAM;
- Reţeaua informală a purtătorilor de cuvânt al MAE din statele Trio Asociat (Georgia, Moldova, Ucraina);
- Reţelele naţionale de combatere a ştirilor false (CIJ, StopFals, API ş.a.).

Nr *(din Plan)*	Acţiunea	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.*

În perioada de referință, SIS a realizat un „Studiu privind activitatea unor persoane pe paginile web care au conținut propagandist, extremist sau distructiv din punct de vedere moral-spiritual”, fapt ce afectează securitatea națională a Republicii Moldova. Materialele studiului enunțat au fost diseminate beneficiarilor legali.

De asemenea, SIS a realizat și un „Studiu pe componenta de combatere a ştirilor false conexe COVID-19”.

În temeiul acestora, au fost elaborate produse informativ-analitice, expediate în adresa beneficiarilor legali, care au vizat evaluarea mediului on-line, cu impact asupra securității informaționale a RM, inclusiv fenomenul „Fake – news”.

În procesul evaluării conținutului media on-line cu potențial de periclitare a securității informaționale, a fost întocmită lista entităților/ subiecților implicați în producerea și diseminarea informațiilor false cu completare continuă.

Concomitent, în perioada vizată, de către SIS a fost identificat un site, care disemina informații de tip „Fake – news” în scopul subminării credibilității instituțiilor de stat ale Republicii Moldova.

Biroul de presă al MAEIE a consemnat că pe tot parcursul anului 2021, au fost recepționate 108 de solicitări de acreditare din partea a 31 de instituții de presă din următoarele țări: România, Ucraina, Belarus, Rusia, Franța, Spania, Olanda, Marea Britanie, Letonia, Turcia etc.

În cadrul alegerilor parlamentare anticipate din 11 iulie, MAEIE a identificat o acțiune concertată din partea unui grup de persoane identificate ca „jurnaliști naționali”, sesizând organele competente.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
14/2	Elaborarea și ajustarea cadrului legal funcțional în scopul reglementării juridice a raporturilor dintre reprezentanții mass-mediei care colectează și difuzează informații în Internet, societate și autoritățile cu atribuții de asigurare a securității informaționale, în conformitate cu recomandările Comisiei Europene și bunele practici europene	Perioada 2021-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Serviciul de Informaţii şi Securitate; Ministerul Justiției; Consiliul Coordonator al Audiovizualului; autorităţile administraţiei publice.*

Pe parcursul anului 2021, juriștii SIS au analizat cadrul normativ, cu identificarea actelor unde urmează a se interveni cu modificări, inclusiv cu evaluarea bunelor practici ale țărilor din regiune.

În contextul armonizării legislației, experții SIS au elaborat două proiecte de legi, care prevăd reglementarea competențelor Serviciului de contractare a materialelor cu caracter extremist și a informațiilor false ce afectează securitatea

statului, inclusiv și sancționarea pentru încălcarea legislației privind combaterea știrilor false și a materialelor extremiste.

La etapa actuală, proiectele sunt transmise pentru promovare în adresa Președinției Republicii Moldova și Ministerului Justiției.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securității spațiului informațional-mediatic**			
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.*

Acțiunea este în proces de implementare, urmând a fi examinat și racordat cadrul normativ în vigoare cu privire la definirea acțiunilor și fenomenelor de dezinformare, manipulare și propagandă ce subminează securitatea informațională.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securității spațiului informațional-mediatic**			
15/3	Interacțiunea cu instituțiile de drept în ceea ce privește analiza riscurilor și a amenințărilor din domeniul mass-mediei, cu scopul de a monitoriza evoluția amenințărilor depistate, de a investiga activitatea subversivă sau penală în spațiul informațional și de a stabili sursele de finanțare a factorilor de risc	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informaţii şi Securitate.*

În anul 2021, 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, inclusiv acțiuni de identificare și blocare a surselor cu conținut online care promovează știri false cu impact asupra securității Republicii Moldova.

Procuratura Generală a participat la Ședința de dezbateri publice privind răspândirea și căile de contracarare în RM a infracțiunilor de falsificare (clonare), uzurpare a identității în spațiul online, de difuzare a știrilor false și denigratoare, în special în adresa persoanelor publice, 05.10.2021.

Conform atribuțiilor prevăzute în regulamentul Procuraturii aprobat prin Ordinul Procurorului General nr. OPG 24/28 din 24.09.2016, modificat prin Ordinul Procurorului General nr. OPG84/8/1 din 11.11.21 și publicat în Monitorul Oficial nr. 369-378 din 28.10.2016, MO315-324/24.12.21, în vigoare 11.11.21, Procuratura Generală monitorizează spațiul informațional în scopul identificării, reacționării prompte la semnale, eventuale intervenții instituționale și prevenirii unor abateri de la lege. De asemenea, semestrial efectuează analiza riscurilor și a amenințărilor din domeniul mass-mediei, cu scopul monitorizării evoluției

factorilor de risc identificați, investigării activităților subversive sau penale în spațiul informațional pentru a stabili sursele de finanțare a factorilor de risc.

Pentru anul 2021, a fost elaborată o notă informativă cu privire la actele de reacționare inițială 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 național, a entității cu competențe de promovare și coordonare a politicilor de securitate informațională într-o societate democratică în funcție de dezvoltarea tehnologiei, raporturile juridice și de altă natură din sectorul societății informaționale la nivel național și internațional (Consiliul coordonator pentru asigurarea securității informaționale): a) identificarea și integrarea componentelor existente cu funcții și atribuții în domeniul cibernetic și mediatic, a autorităților administrației publice locale, precum și a componentelor care vor fi create pe parcurs; b) determinarea liniei de activitate pentru fiecare componentă inclusă în cadrul Consiliului coordonator pentru asigurarea securității informaționale, în funcție de atribuțiile și funcțiile deținute din perspectiva asigurării securității informaționale; c) elaborarea și adoptarea cadrului normativ de interacțiune pentru realizarea sarcinilor de depistare, prevenire și contracarare a riscurilor și amenințărilor la adresa securității informaționale	Anul 2019	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Pe parcursul anului 2021, SIS a elaborat proiectul definitivat al Hotărîrii Guvernului „Cu privire la crearea Consiliului coordonator pentru asigurarea securității informaționale”, căruia anterior i-a fost atribuit număr unic de înregistrare 239/MEI/2020 și care urmează să fie promovat de către Ministerul Economiei.

Astfel, în rezultatul consultărilor cu autoritățile și instituțiile interesate, precum și cu membrii grupului de lucru din cadrul societății civile, a fost completat și modificat Statutul și componența Consiliului.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
16/2	Elaborarea, promovarea și coordonarea politicilor de securitate informațională în conformitate cu Concepția, cu prezenta Strategie și cu alte documente de politici de nivel național și internațional ce se referă la societatea informațională	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Urmare a evaluării cadrului normativ, experții SIS au constatat *lipsa unor reglementări* de natură să determine statutul unor entități virtuale.

În acest sens, experții SIS au înaintat propuneri de completare a actelor normative, după cum urmează:

- *Legea 64/2010 cu privire la libertatea de exprimare;*
- *Legea 54/2003 cu privire la contracararea activității extremiste;*

- *Legea nr. 753/1999 privind Serviciul de Informaţii şi Securitate al Republicii Moldova;*
- *Legea nr. 241/2007 comunicațiilor electronice;*
- *Codul contravențional*.

Prin prisma modificărilor enunțate, Serviciul își va extinde competențele în contracararea răspândirii informațiilor false ce afectează securitatea națională și a materialelor cu tentă extremistă.

Măsurile sunt necesare, în vederea includerii anumitor obligaţii pentru difuzorii de informaţii, în ceea ce priveşte caracterul şi calitatea produselor multimedia distribuite prin Internet, analogic cu prevederile ce se referă la securitatea informațională prevăzute de Codul Audiovizualului.

Modificările şi completările înaintate ar asigura controlul corespunderii cerințelor de legalitate, inclusiv în raport cu informațiile diseminate prin intermediul rețelei Internet.

Pe parcursul anului de referință, MAEIE a continuat acțiunile menite să valorifice oportunitățile inerente ale Acordului RM – UE privind procedurile de securitate pentru schimbul de informaţii clasificate.

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. Astfel, a fost posibilă utilizarea mecanismului de transfer al informațiilor clasificate în cadrul unui proiect pentru furnizarea Poliției de Frontieră a RM cu expertiză adițională menită sa eficientizeze depistarea falsurilor în actele prezentate la PTF-uri, inclusiv la aeroportul Chișinău.

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 Informaţii şi Securitate.*

SIS a informat publicul privind modalităţile de prevenire şi contracarare a riscurilor şi ameninţărilor la adresa securităţii informaţionale, inclusiv fenomenul „fake-news” prin intermediul site-ului „sis.md” şi paginii de „Facebook” a instituției.

MAEIE a desfășurat campaniile tematice pentru consultarea surselor oficiale pe platformele ministerială și MDOC, pe rețele sociale și în interacțiunea cu mass-media. Comunicatele și ieșirile la presă au fost însoțite cu mesaje care să diminueze impactul știrilor false.

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

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 rețelei naționale a autorităților responsabile de combaterea amenințărilor hibride de securitate	Anul 2020	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Pe parcursul anului 2021, a continuat procesul de creare a rețelei naționale a autorităților responsabile de combaterea amenințărilor hibride de securitate, acțiunea fiind coordonată de către Grupul 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	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Pe parcursul anului 2021, SIS a elaborat și expediat în adresa beneficiarilor legali și membrilor grupului de lucru pe domeniul amenințărilor hibride, constituit prin Decizia Prim-ministrului nr. 60 din 05.12.2018 două documente complexe de utilitate inter-instituțională:

1. „Cadrul interinstituțional de referință privind amenințarea hibridă în Republica Moldova”, menit să uniformizeze cunoașterea la nivel național asupra conceptului și specificului amenințărilor hibride.

2. „Modele de influență hibridă în contextul vulnerabilităților interne”, care conține referințe la principalele vulnerabilități naționale.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
17/4	Consolidarea gradului de cunoaștere și înțelegere a concepției amenințărilor hibride de securitate la nivelul organelor abilitate cu asigurarea securității informaționale și 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.*

În perioada de referință, SIS a elaborat proiectul „Protocolului operațional de interacțiune între autoritățile responsabile și factorii de decizie în cazul unor

ameninţări hibride de securitate” (acţiune ce rezidă din obiectivul 17, pilonul III din Planul de acțiuni), care urmează a fi definitivat/ coordonat cu instituțiile naționale în anul 2022.

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.*

Pe parcursul anului 2021, pe tematica vulnerabilităţilor, riscurilor şi ameninţărilor hibride, în adresa beneficiarilor naționali și externi, de către SIS au fost remise 35 de comunicate şi elaborate 7 studii analitice.

Pe parcursul anului, s-a participat la mai multe ședințe interinstituționale dedicate consolidării capacităților şi a cunoaşterii în domeniul gestionării ameninţărilor hibride. Pe platforma respectivă au fost supuse dezbaterii unele studii elaborate de către SIS, cât şi abordate perspective ale implementării Planului de acţiuni pentru implementarea SSI (compartimentul „ameninţări hibride de securitate”).

În perioada 18-19 februarie 2021, la MAEIE a fost organizat un seminar, prin intermediul TAIEX, cu privire la amenințările hibride la care au participat circa 20 de persoane din instituțiile naționale. Evenimentul a urmărit două obiective principale: familiarizarea părții moldovenești cu experiența finlandeză în domeniul combaterii amenințărilor hibride și promovarea dialogului dintre instituțiile din Republica Moldova privind punerea în aplicarea a unui mecanism național adaptat la realitățile țării noastre, inclusiv prin (re)inițierea procesului creării cadrului interinstituțional în RM.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
17/6	Asocierea Republicii Moldova la Centrul European de Excelență pentru Combaterea Amenințărilor Hibride și la Centrul de Excelență pentru Comunicare Strategică al NATO	Perioada 2022-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

MAEIE – În anul 2021, Centrul Baltic de Excelență în Media din Riga, în baza programului finanțat de către MAE leton, a implementat proiectul de studiu privind „O abordare cuprinzătoare și avansarea alfabetizării mediatice pentru a spori rezistența societății împotriva dezinformării în Letonia și în țările PaE”.

La 18-19.02.2021, MAEIE a găzduit seminarul online TAIEX privind amenințările hibride, cu participarea experților finlandezi și moldoveni.

Urmare a înțelegerilor în cadrul consultărilor politice interministeriale moldo-finlandeze (18.11.2021), se vor organiza exerciții de simulare pentru experții din

RM (SIS ș.a.) oferite de Centrul European de Excelență pentru Combaterea Amenințărilor Hibride din Helsinki.

La 30 iunie 2021, Ambasada R. Lituania în RM a organizat un workshop cu tematica „Consolidarea rezistenței societății moldovenești în combaterea amenințărilor hibride: rolul ONG-urilor" *(cu participarea experților lituanieni/ Departamentului de Comunicare Strategică al Forțelor Armate Lituaniene și reprezentanții Centrului de Investigații Jurnalistice, comunității WatchDog.md, Asociației pentru Politica Externă din Moldova, Centrului de Informare și Documentare privind NATO în Moldova și Institutului de Politici Publice).*

În perioada 06-15 decembrie 2021, a avut loc vizita de studiu la Vilnius a reprezentanților RM (inclusiv MAEIE) cu obiectivul studierii bunelor practici de combatere a dezinformării în Lituania (inclusiv Letonia și Estonia) pentru preluarea experienței țărilor baltice, care s-au confruntat cu fenomenul dezinformării în ultimii ani și au elaborat o legislație cuprinzătoare pentru a răspunde acestei provocări.

De asemenea, un obiectiv important promovat de MAEIE este dezvoltarea cooperării cu NATO în domeniul comunicării strategice cu scopul consolidării capacităților de comunicare strategică la nivel național. Acest obiectiv este reflectat în noul Plan Individual de Acțiuni al Parteneriatului Republica Moldova-NATO (IPAP) pentru anii 2022-2023, elaborat de autoritățile naționale în comun cu Alianța.

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	Realizat

Instituția responsabilă: *Ministerul Apărării*

Pe parcursul anului 2021, în cadrul MA s-au întreprins următoarele acțiuni:

- s-a lucrat asupra dezvoltării capabilităţilor de apărare cibernetică şi identificării potenţialelor cooperări pe domeniu atât din ţară cât şi peste hotare;

- s-a elaborat planul de implementare a capabilităţilor de apărare cibernetică ale Ministerului Apărării (este în proces de aprobare);

- s-a elaborat planul de acţiuni al Ministrului Apărării pentru implementarea strategiei securităţii informaţionale;

- la data de 28 ianuarie 2021 a fost inaugurat oficial crearea Centrului de Reacții la Incidente Cibernetice (CRIC);

- la finele semestrului II al anului 2021, CRIC-ul Armatei Naționale a fost operaționalizat.

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

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

În anul 2021, MA a desfășurat următoarele activități:

- Participarea efectivului Armatei Naționale la conferința online de totalizare a exercițiului Cyber Shield 2021 desfășurat în SUA;
- Desfășurarea a 2 workshop-uri cu partenerii militari ai Carolinei de Nord;
- Participarea a trei persoane din cadrul Armatei Naționale la cursurile organizate de către partenerii externi.

În luna noiembrie 2021, reprezentanții SIS au participat la ședința de lucru cu reprezentanții I.P. STISC și Ministerului Apărării. Subiectul ședinței s-a axat pe cooperarea dintre entitățile vizate pe domeniul securității cibernetice, fiind stabilite mecanisme de interacțiune și schimb de informații.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În cadrul reuniunii experților SIS – MA din luna noiembrie 2021, au fost abordate aspecte ce țin de cooperarea inter-instituțională pe domeniul apărării cibernetice, fiind stabilite mecanismele de interacțiune, schimbului de informații și de avertizare timpurie cu privire la elementele de risc la adresa obiectivelor de infrastructura critică.

În cadrul întrunirii, au fost puse în discuție aspectele ce țin de identificarea și stabilirea instituției coordonatoare pe domeniul dat, precum și intensificarea acțiunilor între entități, pentru elaborarea și implementarea unei /Platforme digitale/, prin care se va efectua schimbul de informații în ceea ce privește incidentele, amenințările, soluțiile de aplanare ale acestora.

Subsidiar, în perioada de referință, experții SIS au întocmit 6 informări în adresa beneficiarilor legali cu materiale probatorii privind vulnerabilități și riscuri de securitate cibernetică, inclusiv cu potențial informativ-subversiv, fiind înaintate recomandări pentru înlăturarea și minimizarea acestora.

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

Instituţii responsabile: *Ministerul Justiţiei, Consiliul Audiovizualului.*

Cadrul normativ cu privire la asigurarea securității informaționale în domeniul audiovizualului a fost asigurat odată cu completarea Codului audiovizualului al Republicii Moldova nr. 260-XVI din 27.07.2006.

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.*

Pe parcursul anului 2021, specialiștii SIS au analizat cadrul normativ cu identificarea actelor în vederea intervenirii cu modificări, inclusiv cu preluarea bunelor practici ale țărilor UE și din regiune.

În context, SIS a elaborat două proiecte de legi, transmise pentru promovare în adresa Președinției RM și Ministerului Justiției.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
19/3	Stabilirea unor filtre de depistare şi/sau de blocare a unor produse informaţionale şi/sau resurse informaţionale, ce conţin elemente de risc la adresa securităţii naţionale, precum şi elaborarea şi adoptarea cadrului normativ aferent	Perioada 2021-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de referință, SIS a elaborat două proiecte de legi, care prevăd modificarea Codului contravențional privind sancționarea diseminării informațiilor false privind prevenirea și/ sau combaterea bolilor epidemiologice.

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	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate*

În precedență, în anul 2019, SIS a elaborat și remis către Cancelaria de Stat proiectul 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)*, inclusiv a celor ce țin de sistemele informaționale de importanță vitală. În acest sens, pentru definitivarea proiectului legislativ, a fost desemnat MEI în calitate de instituție responsabilă.

Subsidiar, în anul curent, SIS a emis o scrisoare în adresa MIDR și ME prin care a solicitat întreprinderea măsurilor necesare cu referire la promovarea proiectului de lege enunțat supra.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Pe parcursul anului 2021, de către SIS au fost realizate 46 de măsuri practice de instruire pe profil antitero *(cursuri, exerciții, teste antiteroriste)* cu antrenarea autorităților competente și a sectorului privat, după cum urmează:

- în perioada 23 august - 02 septembrie 2021 a fost asigurată participarea RM la exercițiul comun „Caspii-Antiteror 2021”, realizat concomitent pe teritoriul al 8 state din cadrul CSI;
- au fost realizate 11 teste și 2 exerciții antiteroriste.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
21/1	Sincronizarea și repartizarea rațională a forțelor instituțiilor naționale spre depistarea preventivă a acțiunilor derulate din exteriorul și/sau interiorul țării, concepute ca diversiuni complexe la adresa securității informaționale	Perioada 2020-2022, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada vizată, de către SIS a fost evaluat cadrul normativ, care reglementează atribuțiile instituțiilor naționale cu competențe în domeniul prevenirii, depistării și contracarării acțiunilor extremiste, teroriste și de altă natură ce periclitează securitatea informațională.

În condițiile de extremă necesitate, Serviciul poate aplica indicații executorii privind înlăturarea cauzelor și condițiilor care contribuie la realizarea amenințărilor securității de stat (în condițiile art. 10 alin. (1) lit. h) din Legea nr. 753 din 23.12.1999 privind Serviciul de informații și Securitate al Republicii Moldova), prin care se vor obliga operatorii în telecomunicații să blocheze accesul la un sistem informațional. Însă, măsura dată, nu are acoperire legală, care ar putea obliga operatorii în telecomunicații să execute documentul SIS (excepție fiind atribuțiile delegate SIS în temeiul deciziilor Comisiilor situațiilor excepționale).

Ținând cont de faptul că criteriul de baza pentru depistarea și contracararea informației false ce afectează securitatea națională, pentru SIS este unul destul de important, de către specialiștii SIS a fost elaborat un proiect de lege, care a fost înaintat către factorul decident pentru promovare.

Concomitent, pe dimensiunea combaterii extremismului, rasismului și xenofobiei, Serviciul, a punctat necesitatea perfecționării cadrului legislativ național în domeniu, fiind completat Codul Penal al RM, după cum urmează:

- art. 134^{18} - Organizație și simboluri cu caracter fascist, rasist sau xenofob;
- art. 176^{1} - Încălcarea drepturilor cetățenilor prin propagarea fascismului, a rasismului și a xenofobiei și prin negarea Holocaustului.

În contextul ajustării cadrului normativ în conformitate cu prevederile Legii nr. 120/2017 cu privire la prevenirea si combaterea terorismului, au fost realizate următoarele măsuri:

- prin HG nr. 121 din 12.08.2021 a fost aprobat „Regulamentul Comandamentului operațional antiterorist";
- a fost elaborat și supus procedurii de avizare departamentală „Proiectul Regulamentului Consiliului teritorial antiterorist (CTA)";
- a fost definitivat și remis în adresa Guvernului proiectul „Programului național de consolidare și realizare a măsurilor de protecție antiteroristă a obiectivelor infrastructurii critice pentru anii 2021-2025" și „Proiectul Planului de implementare a Programului național de consolidare și realizare a măsurilor de protecție antiteroristă a obiectivelor de infrastructură critice pentru anii 2021-2025";
- în vederea realizării prevederilor Legii privind securitatea aeronautica nr. 192/2019 și HG nr. 124/2021 cu privire la aprobarea Programului național de securitate în domeniul aviației civile a fost elaborat, supus avizării departamentale și remis în adresa aviației civile proiectul „Planului național de reglementare a situațiilor excepționale legate de actele de intervenție ilicită".
- a fost avizat proiectul „Strategiei naționale privind prevenirea și combaterea spălării banilor și finanțării terorismului pentru anii 2020-2025" și a „Planului de acțiuni" pentru implementarea acesteia, ulterior aprobat prin HP nr. 239/2020.

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 securității informaționale, pe fiecare compartiment în parte: mass-media, tehnologia informațională, apărare, ordine publică și contrainformații	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Realizat

Instituții responsabile: *Autorităţile administraţiei publice, Consiliul Audiovizualului, Ministerul Economiei, Ministerul Apărării, Ministerul Afacerilor Interne, Procuratura Generală, Serviciul de Informaţii şi Securitate, organizaţiile neguvernamentale.*

În cadrul MAEIE, s-a luat decizia privind instruirea obligatorie a tuturor angajaților Ministerului și Misiunilor diplomatice și oficiilor consulare în domeniul

securității cibernetice. Instruirea, cu denumirea „Conștientizare generală în materie de securitate” a decurs pe parcursul lunilor iulie-august ale anului 2021 prin intermediul Agenției de Guvernare Electronică.

În perioada de referință, în cadrul Serviciului de Informații și Securitate și autorităților administrației publice vizate, au fost realizate studii și analize pe aspectele evaluării nivelului de pregătire a resurselor umane în domeniul securității informaționale, pe fiecare compartiment în parte: *mass-media, tehnologii informaționale, apărare, ordine publică și contrainformații*, cu scopul aprecierii specialiștilor pe dimensiunile de competență.

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	Realizat

Instituția responsabilă: *Autorităţile administraţiei publice*

MEC – În anul 2021, instituțiile de învățământ superior au revizuit sau au inițiat noi generații de programe de studii (USM-4, USARB-5, ASEM-8, UTM-2, US Slavonă-1, USPEE-2, US Comrat – l, UPS „I. Creangă” – 1) în domeniul general de formare profesională 061 Tehnologii ale informației și comunicațiilor la ciclul I – studii superioare de licență și ciclul II – studii superioare de master.

În același context, AMFA, ciclul I, desfășoară programul de studii superioare de licență în domeniul general de formare profesională 1031.3 Conducerea subunităților de comunicații și informatică, iar la ciclul II – programul de master de profesionalizare Securitate și apărare.

În perioada de referință, a fost elaborat Planul de formare profesională continuă pentru anul de studii 2021-2022, aprobat prin ordinul MAI nr. 301/2021, în care au fost incluse cursuri de perfecționare a angajaților cu atribuții în domeniul urmărire penală/investigații infracțiuni.

Pe parcursul anului 2021, în cadrul MAEIE a fost organizată instruirea în domeniul securității cibernetice cu denumirea „Conștientizare generală în materie de securitate”, care a avut loc pe parcursul lunilor iulie-august ale anului 2021 prin intermediul Agenției de Guvernare Electronică. Au beneficiat de instruiri toți funcționarii Ministerului și MDOC, în număr de 352 persoane.

În perioada anului 2021, 12 ofițeri ai SIS au participat la 23 evenimente multilaterale organizate în format online (cursuri, conferințe, grupuri de lucru) în cadrul diverselor platforme de interacțiune sub egida Uniunii Europene, NATO și EUBAM pe subiecte ce vizează securitatea cibernetică, amenințările hibride și managementul securității informaționale.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
22/3	Elaborarea unor programe noi de pregătire a resurselor umane în domeniul vizat	Anul 2021, cu verificarea anuală a indicatorilor de progres	Realizat

Instituția responsabilă: *Autorităţile administraţiei publice*

În perioada de referință, de către Institutul Național de Informații și Securitate al SIS și specialiștii din domeniul TIC ai Serviciului, a fost ajustat și îmbunătățit *Programul de studii în domeniul securităţii informaţionale*, destinat audienților SIS și partenerilor din alte autorități publice ale statului.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
22/4	Dezvoltarea şi implementarea unor programe de instruire adresate angajaţilor cu atribuţii de investigare şi urmărire penală, procurorilor, judecătorilor, specialiştilor şi experţilor judiciari în domeniu din cadrul structurilor de aplicare a legii, precum şi celor adresate personalului tehnic din cadrul instituţiilor publice	2021-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Autorităţile administraţiei publice*

În luna august 2021, Institutul Național de Informații și Securitate al SIS a organizat instruiri pentru ofițerii SIS și reprezentanții SV, MAI cu tematica: „Utilizarea softurilor analitice în procesul de investigații în domeniul asigurării securității informaționale”.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
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	Realizat

Instituția responsabilă: *Autorităţile administraţiei publice*

MAEIE – Un obiectiv prioritar al Planului Individual de Acțiuni al Parteneriatului (IPAP) RM-NATO 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. La 21.01.2021, a fost inaugurat Centrul de Reacție la Incidente Cibernetice (CRIC) al Armatei Naționale, urmare a implementării proiectului „Dezvoltarea capacităților de apărare cibernetică ale Forțelor Armate ale RM” din cadrul Programului Știință pentru Pace și Securitate al NATO.

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.

În perioada de referință, ofițerii SIS au participat la 4 întrevederi la nivel înalt de cooperare, în domeniul securității informaționale, organizate cu reprezentanți serviciilor de intelligence partenere.

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	Parțial realizat

Instituția responsabilă: *Autorităţile administraţiei publice*

MAEIE – Textul agreat al Agendei de Asociere 2021-2027, conține prevederi cu privire la cooperarea RM-UE în sfera contracarării amenințărilor hibride și dialogului RM-UE în sfera securității cibernetice și va reprezenta baza pentru dezvoltarea cooperării în domeniu.

De asemenea, MAEIE menține comunicarea instituțională cu ministerele de externe ale statelor străine partenere, Taskforce East StratCom al Serviciul european de acțiune externă.

În vederea realizării cooperării internaționale în domeniul securității informaționale, în 2021 ofițerii SIS au participat la 3 întâlniri bilaterale cu reprezentanții serviciilor speciale partenere, fiind stabilită continuarea schimbului de informații, dar și a întrevederilor la nivel de experți SIS.

Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
24/4	Alinierea la şi implementarea instrumentelor internaţionale existente ce ar asigura prevenirea, depistarea şi contracararea accesului neautorizat la informaţiile cu accesibilitate limitată din reţelele de comunicaţii electronice bancare şi din sistemele de comerţ electronic, precum şi la informaţiile organelor internaţionale de ocrotire a normelor de drept	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Autorităţile administraţiei publice*

MAEIE – Pe parcursul anului de referință a fost actualizată și aprobată Politica internă privind securitatea cibernetică a MAEIE, aspecte reglementate detaliat prin Ordinul MAEIE Nr. 184-b-169 din 23 iulie 2021.

În același sens, a fost organizată instruirea obligatorie a personalului instituțiilor serviciului diplomatic privind conștientizarea generală în materie de securitate cibernetică pe platforma guvernamentală elearning.gov.md.

Au fost profilate stațiile, periferiile și softul de lucru, aprobat prin Ordinul MAEIE Nr. 222-b-204 la data de 3 septembrie 2021.

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

Instituții responsabile: *Ministerul Apărării, Serviciul de Informaţii şi Securitate, Ministerul Economiei, Serviciul Tehnologia Informației și Securitate Cibernetică, Procuratura Generală, Ministerul Afacerilor Interne.*

Pe parcursul anului 2021, în cadrul Ministerului Apărării s-a lucrat asupra dezvoltării capabilităţilor de apărare cibernetică şi identificării potenţialelor cooperări pe domeniu atât din ţară cât şi peste hotare. La fel, s-a inițiat procesul de elaborare a Planului de implementare a capabilităţilor de apărare cibernetică ale Ministerului Apărării, cât și s-a elaborat și aprobat Planul de acţiuni al MA pentru implementarea strategiei securităţii informaţionale.

În perioada de referință, în incinta Centrului de Comunicații și Informatică al Armatei Naționale, a fost desfășurată o ședință comună de lucru – MA, I.P. STISC, SIS având ca subiect de discuții situația actuală pe segmentul asigurării apărării cibernetice și intensificarea colaborării interinstituționale.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
25/2	Intensificarea cooperării cu partenerii de dezvoltare externi privind schimbul de informaţii şi de experienţă în domeniul apărării cibernetice	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Ministerul Apărării, Serviciul de Informaţii şi Securitate, Ministerul Economiei, Serviciul Tehnologia Informației și Securitate Cibernetică, Procuratura Generală, Ministerul Afacerilor Interne.*

În cadrul cooperării cu parterii de dezvoltare, experții Ministerului Apărării lucrează asupra elaborării Acordului de colaborare pe domeniul comunicațiilor și tehnologiilor informaționale.

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

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

În perioada de referință nu au fost semnate Acorduri de cooperare cu partenerii externi de dezvoltare pe dimensiunea apărării 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 victimelor, inclusiv prin utilizarea Sistemului informațional automatizat „Protecția copiilor” și a bazei de date privind exploatarea sexuală a copiilor (ICSE) a OIPC INTERPOL	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei), Procuratura Generală.*

În perioada de referință au fost examinate în Sistemul Informațional „Protecția Copiilor” pe c/p pornite peste 116 dispozitive de stocare a datelor, fiind depistate și excluse din circuit în rețeaua Internet peste 181 mii de imagini foto și 7 mii fișiere video cu conținut de pornografie infantilă.

Au fost examinate 1.601 fișiere cu imagini și video în baza de date ICSE a Interpol, pentru stabilirea apartenenței la categoria pornografiei infantile.

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

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

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

Instituții responsabile: *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 al MAI asigură și recepționează solicitările privind asistențe imediate pentru investigațiile referitoare la infracțiunile informatice.

Astfel, pe parcursul perioadei de raport au fost recepționate prin puncte de contact 24/7 pe Convenția privind criminalitatea informatică:

- cereri de conservarea datelor parvenite: 20 (1-Spania, 11-US Departament, 1-Rusia, 2-Cehia, 2-Germania, 1-Franța, 1-Ungaria, 1-Austria);
- răspunsuri de conservarea datelor: 6 (1-Spania, 2-US Departament , 1-Rusia, 1-Cehia, 1-Germania);
- solicitări recepționate: 1 (Belarus)
- transmise răspunsuri: 1(Belarus).

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: 15 (3 Facebook, 4 webmoney, 3 Google, 1 Robinhood, 4 Binance);
- primite răspunsuri: 2 (2 Facebook, 3 Binance).

În anul 2021, Procuratura Generală, a examinat 80 comisii rogatorii parvenite de la autoritățile competente din: Austria, Belarus, Germania, Turcia, Cehia, Franța, Belarus, SUA, România, Regatul Țărilor de Jos, Japonia, Armenia, Estonia, Bulgaria, Elveția, Portugalia, Polonia, Belgia.

Prin intermediul punctului de contact 24/7 au fost examinate 33 cereri de conservare a datelor informatice.

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

Instituții responsabile: *Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei), Procuratura Generală.*

În perioada de referință, patru reprezentanți ai Direcției investigații infracțiuni informatice a INI a IGP au participat pe data de 23.02.2021 la trainingul online privind platforma organizației NCMEC din SUA.

Ca rezultat a generalizării anuale a infracțiunilor în domeniul informatic și de telecomunicații, prin care sa depistat o creștere a infracțiunilor de pornografie infantilă, Procuratura Generală urmează să intensifice dezvoltarea parteneriatelor existente cu NCMEC (Centrul Național al SUA privind Copiii Dispăruți și Exploatați) și aderarea la alte inițiative similare.

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

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

Pe parcursul anului 2021, Direcția investigații infracțiuni informatice a INI a înaintat o cerere către ARBI pentru aplicarea a 2 sechestre a bunurilor provenite din infracțiunile transfrontaliere.

În perioada de referință, ofițerii SIS au avut o serie de întrevederi cu reprezentanții serviciilor speciale partenere fiind abordate inclusiv și subiecte de combatere a criminalității informatice. Totodată, SIS a identificat grupări infracționale transfrontaliere în domeniul criminalității informatice. Pe marginea aspectelor infracționale elucidate, au fost informate organele abilitate ale RM (MAI, PG), în scopul elucidării situațiilor pe caz.

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 internaționale în domeniul prevenirii și combaterii criminalității informatice în scopul formării personalului de specialitate	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *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 2021 a fost facilitată participarea experților naționali la următoarele activități:

- Atelier privind reforma legislației în materie de procedură penală în domeniul crimelor informatice în Republica Moldova (29 ianuarie 2021);
- Instruire privind cooperarea internațională privind criminalitatea cibernetică și evidențele electronice (1-3 februarie 2021);
- Atelier privind protecția datelor cu caracter personal (15-16 februarie 2021);
- Webinar privind discursul de ură și măsurile restrictive - violența cibernetică (26 februarie 2021);
- Masa rotundă cu privire la politicile RM privind criminalitatea și securitatea cibernetică (19 martie 2021) ;
- Atelier privind elaborarea procedurilor de cooperare între CSIRTs (Computer Security Incident Response Team) și organele de aplicare a legii (11-12 mai 2021);
- Atelier comun cu Proiectul EndOCSEA privind instruirea de aplicare a legislației împotriva abuzului sexual online asupra copiilor (3-4 iunie 2021);
- Sesiunea pilot de instruire online în domeniul judiciar (23-25 iunie 2021);
- Training național pentru unitățile responsabile de combaterea criminalității cibernetice și procurori privind utilizarea șabloanelor pentru păstrarea datelor și informațiilor despre abonați (5-6 iulie 2021);

- Instruire privind cooperarea dintre interagenții și investigații financiare/ inteligență (25-27 octombrie 2021).

Totodată, un alt rezultat important al proiectului a fost selectarea a 2 experți din cadrul MAI pentru participarea la cursul intensiv privind Programarea Phyton organizat ECTEG Forensic Training (mai-iulie 2021).

În perioada de referință, angajații Poliției au participat în cadrul a 23 de evenimente internaționale, fiind instruiți 63 de experți. după cum urmează:

1. În perioada 26-27.01.2021, 1 ofițer a participat la 2 webinare privind impactul abuzului asupra copilului, eveniment organizat de către DCAC din SUA;
2. În perioada 01-03.02.2021, 5 ofițeri au participat la cursul de instruire privind cooperarea internațională în domeniul crimelor cibernetice și dovezilor electronice, eveniment organizat în cadrul proiectului CoE ”CyberEast;
3. În perioada 18.02-19.02.2021, 1 ofițer a participat la trainingul online „ETSI Quantum Safe Cryptography”, eveniment organizat de Institutul European de Standardizare în Telecomunicații (ETSI);
4. La 18.03.2021, 3 ofițeri au participat la evenimentul de prezentarea a noii descoperiri în industria securității – soluție de tip DLP de la Palo Alto Networks: și securitate IoT”, desfășurate online de către „RTSolutions;
5. În perioada 22-26.03.2021, 25 angajați au participat în cadrul vizitei de studiu în domeniul securității cibernetice în or. București, România, eveniment organizat în contextul implementării Acordului de parteneriat privind transferul know-how , dintre MAI RM și MAI al României;
6. La 15.04.2021, 4 ofițerii au participat la cursul de instruire privind Conștientizarea tehnologiilor financiare pentru autoritățile de aplicarea a legii în vederea identificării riscurilor unice de criminalitate financiară lansat de către FINTRAIL;
7. În perioada 24.05-04.06.2021, 1 reprezentant al DIII a participat la cursul de instruire online cu genericul "Combaterea corupției și crimelor economice", organizat de către Centrul național avansat pentru prevenirea crimei organizate din or. Caserta, Italia;
8. În perioada 25.05-10.06.2021, 1 angajat a participat la cursul online pentru ofițerii de investigații privind limbajul de programare Python, organizat de către ECTEG- European Cybercrime Trening and Educationa Group și Proiectul cu privire la combaterea criminalității cibernetice (CyberEast);
9. În perioada anului 2021, 1 ofițer a participat la 10 webinare privind produsele software utilizate la investigarea exploatării sexuale online a copiilor, organizate de Biroul Federal de Investigații al SUA;
10. La 15.06.2021, 1 ofițer a participat în cadrul evenimentului virtual pe subiectul abuzului sexual online asupra minorilor, organizat de UNICRI și Ministerul Afacerilor Interne al Emiratelor Arabe Unite;
11. La 18.06.2021, 1 reprezentat din cadrul Direcției a participat în cadrul conferinței online de finalizare a proiectului CoE „Stoparea exploatării și abuzului sexual online în rândul copiilor în Europa” (EndOCSEA@Europe);
12. În perioada 14-25.06.2021, 1 reprezentant al DIII a participat în cadrul evenimentului „Victim identification Task-Force 9”, organizat de Europol;

13. În perioada 24-25.06.2021, 1 ofițer a participat Conferința a 7-a a Criptomonedelor organizată de Europol EC3;

14. La 15.07.2021, 1 reprezentant al Poliției a participat în cadrul webinar-ului sub egida CoE, privind instrumentele noi de investigare a infracțiunilor informatice elaborate în cadrul proiectului „Freetool;

15. În perioada 24-26.08.2021, patru angajați au participat la cursul de instruire cu genericul "Investigarea Crimelor Informatice", organizat sub egida Academiei Internaționale a Organelor de Drept (ILEA) din Budapesta, Ungaria;

16. În perioada 13-17.09.2021, 4 ofițeri au participat la atelierul de instruire în cadrul proiectului Consolidarea capacităților ofițerilor de Poliție moldoveni în combaterea tuturor formelor de crimă organizată, organizat de către Poliția Regională din Cracovia, Polonia;

17. În perioada 14-16.09.2021, șase ofițeri au participat la cursul de instruire (online) cu genericul Sesiune de pregătire în domeniul investigării infracțiunilor informatice a ofițerilor de poliție și poliție de frontieră din România și Republica Moldova, organizat în cadrul proiectului Cooperare Regională pentru Prevenirea și Combaterea Criminalității Transfrontaliere România-Moldova (THOR);

18. În perioada 15-17.09.2021, un reprezentant al Direcției a participat la Cursul de instruire în domeniul utilizării bazei de date internaționale a INTERPOL privind exploatarea sexuală a copiilor (ICSE) în or. Lyon, Franța;

19. În perioada 13-17.09.2021, un ofițer a participat la cursul cu tematica "Consolidarea capacităților ofițerilor de Poliție în combaterea tuturor formelor de crimă organizată", organizat de Poliția din Polonia/Cracovia, care s-a desfășurat în incinta hotelului Aria, mun. Chișinău;

20. În perioada 20-24.09.2021, 1 angajat al Direcției a participat la Conferința în domeniul crimelor cibernetice, organizată în or. Budva, Muntenegru cu suportul SEPCA și OSCE;

21. În perioada 18-22.10.2021, un ofițer a participat la cursul de instruire online cu genericul „Open source intelligence in criminal investigation”, pentru ofițerii de poliție din statele membre ale organizației Cooperării Economice la Marea Neagră, organizat de Departamentul de poliție al Turciei;

22. În perioada 07-08.12.2021, 2 ofițeri au participat la cea de-a V-a ”Conferință globală în domeniul criminalității financiare și criptomonedei”, organizată sub egida OIPC Interpol și Europol;

23. În perioada 06-11.12.2021, 2 reprezentanți ai DIII au participat în cadrul vizitei de lucru în cadrul proiectului ”Consolidarea capacității Republicii Moldova de contracarare a abuzului și exploatării sexuale online”, implementat de CI „La Strada” cu suportul financiar al Ambasadei SUA la Chișinău, în or. Amsterdam, Olanda.

Pe parcursul anului 2021, Procuratura Generală, procurorii din procuraturile specializate și teritoriale au avut mai multe seminare de instruire în ceea ce ține de domeniul prevenirii și combaterea criminalității informatice:

- Atelierul de lucru „Privind reforma legislației privind procedura penală în conformitate cu Convenția de la Budapesta privind criminalitatea cibernetică”, mun. Chișinău, în perioada 29 ianuarie 2021;

- Instruire privind cooperarea internațională în domeniul criminalității cibernetice și probe electronice pentru anchetatori, procurori și judecători (online perioada 1-3 februarie 2021);

- Atelier de lucru cu autoritățile de protecție a datelor cu caracter personal și autoritățile naționale de reglementare în domeniul comunicațiilor despre încredere și cooperare în ceea ce privește criminalitatea cibernetică și acțiunile în materie de probe electronice (on-line perioada 15-16 februarie 2021);

- Participarea la cea de-a șaptea reuniune a Grupului de experți privind criminalitatea cibernetică, (ședința on-line) Comisiei ONU 1963-14 pentru Prevenirea Criminalității şi Justiție Penală, realizate în Cadrul de Cooperare programatică Consiliul Europei – Uniunea Europeană, găzduită de UNODC, 06-08 aprilie 2021.

- A 24 reuniune a Plenarei Comitetului Consiliului Europei (T-CY), pentru criminalitatea informatică, sesiune pentru elaborarea protocolului adițional a Convenției de la Budapesta pentru prevenirea criminalității cibernetice, online 28 mai 2021.

- A 25 reuniune a Plenarei Comitetului Consiliului Europei (T-CY), pentru criminalitatea informatică, sesiune pentru elaborarea protocolului adițional a Convenției de la Budapesta pentru prevenirea criminalității cibernetice, on-line 28 mai 2021.

În contextul consultărilor RM - UE în domeniul securității cibernetice și vizitei delegației SIS la Bruxelles (noiembrie 2021), a fost înaintată propunerea pentru încheierea unui Acord de cooperare între „*European Union Agency for Network and Information Security (ENISA)" și Republica Moldova.*

Concomitent, în perioada vizată, Serviciul a delegat un reprezentant în *Grupul de lucru inter-instituțional*, creat în contextul transpunerii prevederilor „*Directivei Network and Information Security (NIS) a UE"* în legislația națională.

În luna septembrie 2021, un reprezentat al SIS a participat la ședința grupului de lucru în cadrul *proiectului UE „Cyber Security EAST"*, la care s-a convenit elaborarea unui proiect de Hotărîre privind transpunerea în legislația națională a *Directivei NIS (versiunea 2.0).*

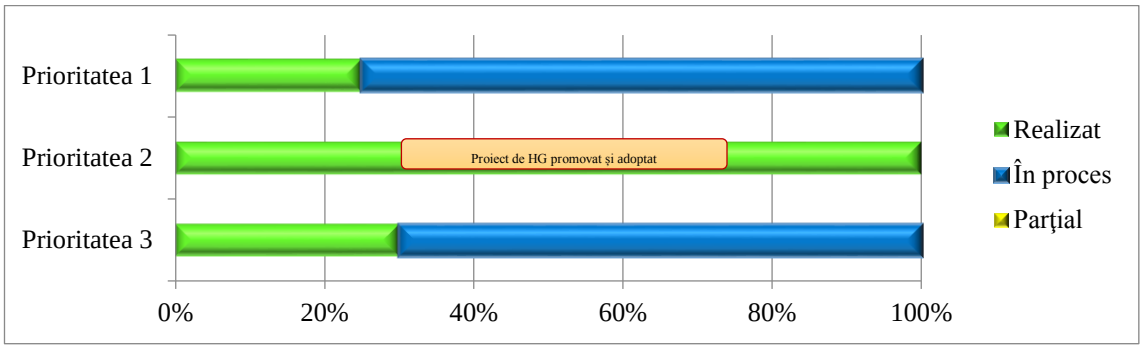
REFLECTAREA INDICATORILOR DE PROGRES CONFORM PRIORITĂŢILOR

În rezultatul evaluării rezultatelor înregistrate în implementarea Planului Strategiei, se atestă un randament redus al acţiunilor realizate de către instituţiile responsabile şi partenere în anul 2021 prin prisma priorităţilor SSI, cauzat primordial datorită situaţiei pandemice la nivel naţional.

Concomitent, ponderea procentuală a realizării priorităţilor pe parcursul anului 2021 sunt prezentate în graficile 1, 2 şi 3, care au fost elaborate prin prisma indicilor de rezultat ale acestora.

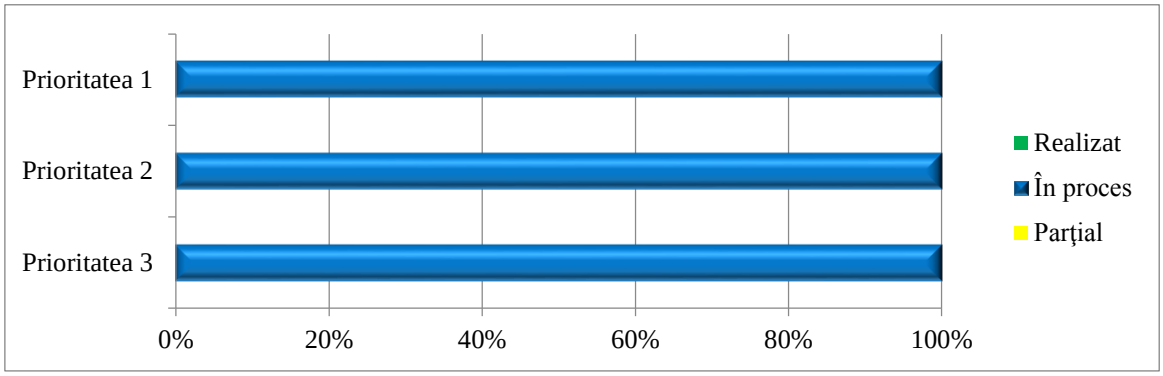
Pilonul I. Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice	
Priorităţile pilonului	Indicatori de rezultat
1. Crearea Centrului naţional de reacţie la incidente de securitate cibernetică (CERT naţional)	1. Centrul naţional creat, care elaborează documente 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

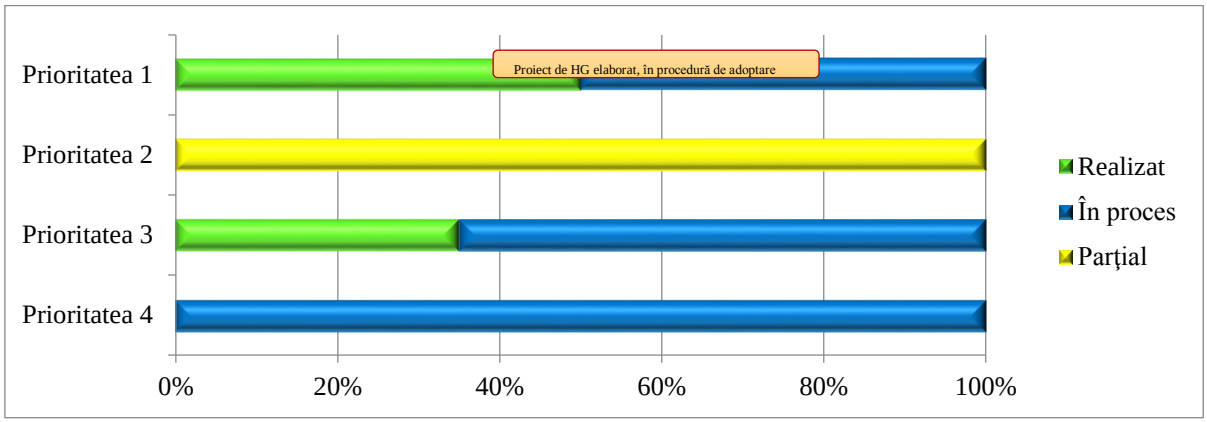
Grafic 2. Ponderea procentuală de realizare a priorităţilor Pilonului II



Pilonul III. Consolidarea capacităţilor operaţionale

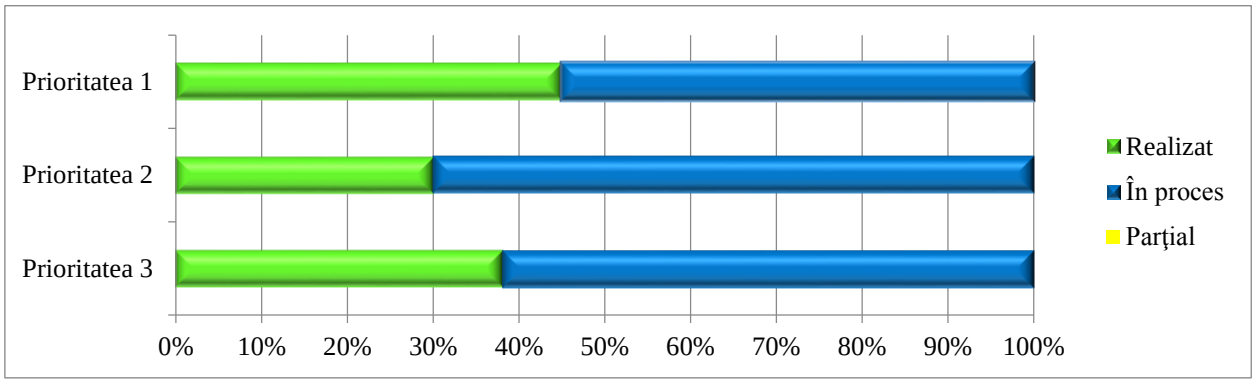
Pilonul III. Consolidarea capacităţilor operaţionale	
Priorităţile pilonului	Indicatori de rezultat
1. Crearea, la nivel naţional, a Consiliului coordonator pentru asigurarea securităţii informaţionale, în cadrul căruia vor fi identificate proceduri de comunicare strategică	1. Cadrul normativ privind 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 angajaţilor cu atribuţii de investigare şi urmărire penală în spaţiul informaţional	1. Specialişti instruiţi în baza practicilor UE
2. Dezvoltarea cooperării naţionale şi internaţionale în domeniul apărării cibernetice	2. Cadrul legal de cooperare negociat şi încheiat
3. Stabilirea mecanismelor de cooperare internaţională între autorităţile statului cu atribuţii în combaterea criminalităţii informatice şi organismele internaţionale pe segmentul asigurării securităţii informaţionale	3. Runde de consultări; acorduri bilaterale/ multilaterale semnate şi încheiate

Grafic 4. Ponderea procentuală de realizare a priorităţilor Pilonului IV



DESCRIEREA RISCURILOR DE IMPLEMENTARE

Realizarea obiectivelor Strategiei securității informaționale necesită amplificarea mobilizării tuturor componentelor societății informaționale în scopul implementării acțiunilor planificate, mai ales că ultimele au o dimensiune transectorială și implică instituții din domeniul civil, media, TIC, cât și celor de securitate, apărare și de drept.

Având în calcul caracterul complex și multidimensional al acțiunilor din Planul SSI 2019-2024, au fost constatate și riscuri ale implementării Strategiei, care necesită în continuare o atenție sporită în vederea înlăturării sau diminuării acestora. Printre acestea, sunt de accentuat următoarele categorii de riscuri:

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

- În perioada de referință – 2021, similar anilor precedenți, a fost sesizată poziția superficială în elaborarea și adoptarea documentelor de politici la nivel instituțional sau sectorial ce rezultă din Strategia SSI 2019-2024 din partea managementului strategic al unor instituții responsabile sau partenere în conformitate cu prevederile Planului;
- Cooperarea redusă între echipele de experți pe dimensiunea de securitate informațională din cadrul instituțiilor de drept public și privat, vizate în Planul SSI 2019-2024 și managementul decizional al acestora, fapt ce diminuează din caracterul unitar în implementarea Planului de acțiuni.

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

- Insuficiența specialiștilor în domeniul tehnologiilor informaționale în subunitățile cu atribuții de asigurare a securității informaționale în cadrul autorităților publice, în special la funcționarea și dezvoltarea Centrelor de reacție la incidentele de securitate cibernetică – CERT departamental;
- Echiparea redusă a CERT-urilor instituționale cu sisteme și tehnică specializată pentru asigurarea securității cibernetice conform standardelor internaționale de securitate informațională.

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

- Apariția și dezvoltarea unor noi generații de riscuri și amenințări la adresa securității informaționale, derivate din evoluția accelerată a tehnologiilor informaționale, care nu sunt prevăzute de SSI și Planul de acțiuni pentru implementarea acesteia;

➢ Caracterul imprevizibil al evoluției situației de securitate la nivel regional și internațional, cât și impactul acesteia asupra proceselor și activităților oamenilor, inclusiv din domeniile vizate în Planul de acțiuni: civic, media, public și privat.

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

CONCLUZII ŞI RECOMANDĂRI

Monitorizarea pe parcursul anului 2021 şi prezentarea Raportului pentru al treilea an de implementare denotă prioritățile de securitate informaţională ale Strategiei, care rămâne în continuare corespunzătoare procesului de evoluție a societăţii informaţionale la nivelul Republicii Moldova și internațional.

Analiza exhaustivă a indicatorilor de rezultat prezentaţi de instituţiile responsabile prin prisma atribuţiilor şi acţiunilor executate în anul 2021 de fiecare instituţie în parte sau prin cooperare cu alte autorităţi partenere, raportaţi la obiectivele şi scopul SSI, **reflectă un progres diminuat** în realizarea acestora, condiționat și de factori excepționali, cum este situația pandemică și impactul acesteia asupra activităților societății.

În context, **riscurile de securitate cibernetică** și **formele noi de amenințări hibride** la adresa **securităţii informaţionale** care sunt **vizate de SSI: dezinformarea, propaganda, manipularea, războiul informaţional,** rămân actuale și **necesită** a fi **înlăturate** și **minimalizate**.

Subsidiar, rapoartele de referință pe anumite activități din Plan, **denotă o conlucrare deficientă** între **instituțiile responsabile** și cele **partenere**, în pofida unei necesități stringente de coeziune a acestora întru depășirea problemelor de securitate informațională la nivel național.

Totodată, evaluarea **atestă** și o **abordare pragmatică** a **subiectelor de securitate informaţională** din partea responsabililor insitituţiilor de stat şi private, cu identificarea clară a vulnerabilităților şi riscurilor pe domeniile de competență, fapt ce **coroborează indicatorii de progres raportați**.

Astfel, analiza rezultatelor înregistrate în anul 2021 şi a celor cu termen permanent de implementare, prezentate de instituțiile responsabile și cele partenere, urmează a fi examinată detaliat în cadrul următoarelor şedinţe ale Grupului de lucru din cadrul SIS și persoanele desemnate de instituțiile vizate în Planul de acțiuni privind implementarea Strategiei securității informaționale a Republicii Moldova 2019-2024.