Ex. nr. 1

SERVICIUL DE INFORMAȚII ȘI SECURITATE
AL REPUBLICII MOLDOVA

MD 2004, mun.Chișinău, bd. Ștefan cel Mare și Sfînt 166, tel. 022-239-625, fax. 022-234-068 e-mail: sis@sis.md

„30" martie 2023 nr. 3/640

Domnului Igor GROSU
Președinte al Parlamentului
Republicii Moldova

Stimate Domnule Președinte,

În conformitate cu prevederile articolului 3 din Hotărârea Parlamentului Republicii Moldova nr. 257 din 22.11.2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia, Serviciul de Informații și Securitate prezintă Raportul de monitorizare și evaluare a implementării acestora pentru anul 2022.

Anexă: Raport de monitorizare și evaluare a implementării Strategiei securității informaționale a RM pentru anii 2019-2024 (perioada de raportare – 2022), pe 69 (șaizeci și nouă) file, nesecret.

Cu respect,

Alexandru MUSTEAȚA
Director

SECRETARIATUL PARLAMENTULUI
REPUBLICII MOLDOVA
D.D.P. Nr. 1226
„22" 05 2023
Ora

R A P O R T

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

Perioada de raportare: 2022

SERVICIUL DE INFORMAȚII ȘI SECURITATE

Elaborat – martie 2023

CUPRINS:

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
- CA – Consiliul Audiovizualului
- CERT – Centru de reacție la incidentele de securitate cibernetică
- 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
- MDED – Ministerul Dezvoltării Economice și Digitalizării
- MEC – Ministerul Educaţiei şi Cercetării
- MF – Ministerul Finanţelor
- MJ – Ministerul Justiţiei
- 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 procesului de implementare a Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024 *(în continuare SSI/Strategie)* constituie o evaluare complexă a acţiunilor realizate şi rezultatelor înregistrate pe parcursul anului 2022 la executarea Planului de acţiuni al SSI, adoptat prin Hotărârea Parlamentului nr. 257 din 22.11.2018.

Serviciul de Informații și Securitate al Republicii Moldova, conform prevederilor art. art. 2 şi 3 al HP nr. 257 din 22.11.2018 şi a pct. 115 din Strategie, este autoritatea responsabilă de monitorizarea şi coordonarea implementării Planului de acţiuni al Strategiei.

În context, scopul primordial al SSI a Republicii Moldova pentru anii 2019 – 2024 constă în integrarea juridică și sistemică a domeniilor prioritare cu responsabilităţi şi competenţe în asigurarea securităţii informaţionale a țării noastre, pilonii de bază fiind rezilienţa cibernetică și informațională pe dimensiunea de securitate, menite să protejeze suveranitatea, independenţa, integritatea teritorială și interese naționale ale Republicii Moldova.

Planul de acţiuni pentru implementarea Strategia securității informaționale *(în continuare Plan)* prevede un set complex de acţiuni, ce au scopul realizării obiectivelor Strategiei, după cum urmează:

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

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

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

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

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

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

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

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

Pe parcursul anului 2022 – al patrulea an de implementare a Hotărârii Parlamentlui nr. 257, Serviciul de Informații și Securitate, de comun cu instituțiile responsabile și partenere, au realizat acțiuni întru executarea Planului, inclusiv organizatorice, fiind organizate interacționări și discuții între reprezentanții

Secretariatului Grupului de monitorizare și persoanele responsabile, desemnate de instituțiile vizate în Plan.

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

- ❖ Evaluare și analiză a acţiunilor realizate de către autorităţi prin prisma prevederilor Planului SSI şi a Planurilor instituționale elaborate;
- ❖ Măsurarea progresului cantitativ şi calitativ al executării acțiunilor de competență conform Planului SSI 2019-2024;
- ❖ Reflectarea indicatorilor de impact în al patrulea an de implementare, conform aprecierilor insitituţiilor responsabile şi a indicatorilor prezentaţi în rapoartele anuale;
- ❖ Identificarea riscurilor pentru implementarea Planului.

Raportul cuprinde:

1. Analiza acţiunilor şi a progreselor raportate de instituţiile responsabile, în corespundere cu informațiile remise în adresa Secretariatului Grupului de monitorizare din cadrul Serviciului de Informaţii şi Securitate;
2. Evaluarea calitativă şi cantitativă a realizării acţiunilor în baza indicatorilor de progres şi a rezultatelor scontate, raportate la obiectivul Strategiei;
3. Descrierea 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 desfăşurate la nivelul instituţiilor responsabile şi partenere;
5. Reflectarea evoluţiilor în grila indicatorilor de impact ai Strategiei, cât și în conformitate cu aprecierile şi recomandările ce vor fi oferite de deputaţii din Comisia securitate naţională, apărare şi ordine publică a Parlamentului Republicii Moldova, de organizaţiile neguvernamentale, experţii naţionali şi internaţionali din domeniul de securitate.

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

DESCRIEREA PROGRESELOR ACȚIUNILOR REALIZATE ÎN PERIOADA ANULUI 2022

Capitolul relevă progresul executării acţiunilor scadente în anul 2022 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	Parțial realizat

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

Pe parcursul anului 2022, experții SIS au participat la activitățile Grupului de lucru interinstituțional, în vederea elaborării Proiectului de lege privind securitatea cibernetică, ce prevede crearea şi edificarea Centrului Naţional de Reacţie la Incidentele de Securitate Cibernetică (CERT Naţional), înregistrat de Cancelaria de Stat (nr. 41/ME/2023). Proiectul de lege a fost elaborat de către Ministerul Economiei în comun cu Echipa proiectului Moldova Cybersecurity Rapid Assistance, în coordonarea viceprim-ministrului pentru digitalizare. Obiectivul proiectului de lege, este reglementarea cadrului juridic, organizațional și de cooperare în domeniul securității cibernetice, care stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și gestionarea incidentelor cibernetice.

Legea privind securitatea cibernetică, nr. 48 din 16.03.2023 a fost aprobată de Parlamentul RM în două lecrturi, la momentul elaborării prezentului Raport, este examniată pentru a fi votată şi în a treia lectură. Actul normativ stabilește principiile de organizare şi funcţionare a CERT Naţional, care va fi lansat în anul 2025.

Procuratura Generală a participat la avizarea proiectului de Hotărâre a Guvernului privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental. Pe parcursul anului 2022 procurorii din Procuratura Generală au participat la 3 ședințe de lucru naționale (18.08.2022; 28.09.2022 și 17.11.2022), de comun cu alți reprezentanți ai instituțiilor de stat în cadrul proiectului „Moldova Cybersecurity Rapid Assistance” cu subiectul „Administrarea securității cibernetice și rolul echipei de intervenție în caz de

urgență informatică (CERT)". La fel, reprezentanții PG în perioada 24-28.10.2022 au participat la vizite de studiu cu aceeași tematică în Estonia, Finlanda, Letonia în cadrul aceluiași proiect implementat de Fundația Estoniană Academia e-Guvernare și Consiliul Europei.

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.*

Prin Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raționalizare a administrării sistemelor informaționale de stat, a fost desemnată Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică" în calitate de Centru guvernamental de reacție la incidente de securitate cibernetică.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
1/3	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 contextul aprobării Legii privind securitatea cibernetică, nr. 48 din 16.03.2023, care stabileşte principiile de creare şi funcţionare a CERT Naţional, insitituţiile responsabile vor elabora indicatorii de securitate cibernetică.

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.*

Prin scrisoarea nr. 1.4/357/22 din 21.02.2022 I.P. „Serviciul Tehnologia informației și Securitate Cibernetică" (STISC) a solicitat autorităților publice desemnarea persoanei (subdiviziunii) responsabile de punere în aplicare a

măsurilor necesare pentru asigurarea securității cibernetice. Autoritățile publice au desemnat persoanele responsabile pentru colaborarea cu Centrul guvernamental de reacție la incidente de securitate cibernetică pe aspecte ce țin de securitate cibernetică.

În scopul consolidării capacităților instituționale de reacție la incidentele de securitate cibernetică au fost ajustate/ elaborate și aprobate 2 acte normative interne ale SIS. Complementar, în scopul optimizării managementului incidentelor de securitate cibernetică, în cadrul SIS a fost implementată o platformă de răspuns la incidente de securitate cibernetică. În scopul dezvoltării capacităților profesionale, ofițerii SIS au participat la evenimente internaționale și instruiri.

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.*

În temeiul art. 23 din Legea nr. 100/2017 cu privire la actele normative, pe parcursul anului 2022, a fost elaborat proiectul de lege privind securitatea cibernetică și Analiza de Impact, cu suportul experților proiectului UE „Moldova Cybersecurity Rapid Assistance”, iar ulterior, după avizare și consultare publică, proiectul de lege a fost aprobat prin Hotărârea Guvernului nr. 111/2023.

Legea nr. 48/16.03.2023 reglementează cadrul juridic, organizațional și de cooperare în domeniul securității cibernetice, stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, determină cadrul național de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme pentru asigurarea securității rețelelor și sistemelor informatice, precum și gestionarea incidentelor cibernetice.

Prevederile Legii nr. 48/16.03.2023 includ următoarele aspecte:

- Reglementarea instituirii unei autorități competente în domeniul securității cibernetice cu funcții de identificare, monitorizare și supraveghere, coordonare operațională a situațiilor de criză, de cooperare și interacțiune la nivel național și internațional.
- Instituirea în cadrul autorității competente a unei echipe de răspuns la incidente de securitate cibernetică (CSIRT) cu competențe la nivel național, asigurarea recunoașterii internaționale a acesteia.
- Definirea cadrului general strategic și operațional de coordonare și cooperare dintre sectorul public și privat în domeniul securității cibernetice (Planul național de răspuns la incidente cibernetice, Strategia națională privind securitatea cibernetică, Consiliul coordonator în domeniul securității cibernetice).
- Reglementarea măsurilor de securitate cibernetică care obligatoriu urmează a fi implementate de către entitățile ale căror servicii sunt critice pentru funcționarea economiei și a societății.

- Instituirea unui mecanism obligatoriu de raportare a incidentelor cibernetice semnificative de către furnizorii de servicii și a posibilității de notificare voluntară a incidentelor cibernetice.

- Crearea și asigurarea funcționării adecvate a mecanismelor de cooperare eficiente la nivel național și internațional în domeniul securității cibernetice.

Prin Legea nr. 48/16.03.2023 se transpune cadrul normativ și bunele practici europene în contextul obținerii statutului de țară – candidat pentru aderare la Uniunea Europeană. În acest sens, cel mai recent act european în domeniu este Directiva (UE) 2335 din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2).

Implementarea prevederilor Legii nr. 48/16.03.2023 va asigura o creștere a nivelului de reziliență cibernetică a entităților cheie din Republica Moldova, astfel, vor fi gestionate mult mai eficient și transparent, dar și evitate incidentele cibernetice, precum și eventuale prejudicii materiale și reputaționale asociate acestora.

Pentru a oferi suficient timp de conformare cu prevederile legii atât pentru sectorul privat, cât și pentru cel public, se propune intrarea în vigoare a legii la data de 01.01.2025.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
1/6	Determinarea politicii privind modalitatea de raportare, de stocare şi de prelucrare a informaţiilor aferente incidentelor şi ameninţărilor la adresa securităţii informaţionale	Perioada 2021-2022, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituţia resonsabilă: *Serviciul Tehnologia Informaţiei şi Securitate Cibernetică.*

A fost aprobată Hotărârea Guvernului nr. 388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” care reprezintă totalitatea sistematizată de date privind incidentele cibernetice raportate prin punctul unic de contact CERT Gov, deţinătorii resurselor informaţionale afectate, precum şi privind documentele şi mijloacele de identificare a incidentelor de securitate cibernetică raportate. În context, SIS, în semestrul I al a. 2022, a emis avizul la Proiectul Hotărârii Guvernului menționate supra *(nr. 161/ CSI/ STISC/ 2021)*.

Totodată, la etapa promovării a fost Proiectul de Lege privind securitatea cibernetică prin care se stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și gestionarea incidentelor cibernetice.

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.*

Cu referință la implementarea rezultatelor auditului de securitate cibernetică, AGE a solicitat de la entitățile auditate în anii precedenți, să informeze referitor la realizarea recomandărilor misiunilor de audit de securitate cibernetică, cu prezentarea dovezilor concludente (raport detaliat privind remedierea neconformităților). Astfel, aferent entităților publice auditate în 2019, se constată următoarele:

- Serviciul Tehnologia Informației și Securitate Cibernetică, Centrul de Tehnologii Informaționale în Finanțe, Ministerul Afacerilor Externe și Integrării Europene, Ministerul Finanțelor și Ministerul Apărării – au prezentat dovezi concludente privind implementarea recomandărilor de audit, indicatorii de realizare fiind peste 75%, iar acțiunile parțial realizate sau aflate în derulare sunt ținute la controlul managementului entității, prin transpunerea în planurile de activitate anuale sau tematice, aprobate de conducere.
- Agenția Servicii Publice, Ministerul Infrastructurii şi Dezvoltării Regionale, Cancelaria de Stat – au confirmat realizarea recomandărilor în proporție de peste 50%, iar acțiunile parțial realizate sau aflate în derulare nu prezintă risc de nivel sporit și sunt ținute la controlul managementului entității.
- Ministerul Afacerilor Interne – a raportat despre realizarea măsurilor de securitate cibernetică la nivel de minister și instituțiile subordonate, precum și au luat în considerare recomandările auditului în procesul de implementare și dezvoltare a SMSI, conform Ordinului MAI nr. 244/2017.
- Ministerul Dezvoltării Economice și Digitalizării – a comunicat ca este vacanta funcția de șef al Serviciului TIC, iar în ce privește asigurarea și controlul implementării cerințelor minime de securitate cibernetică, a propus ca aceste servicii sa fie asumate și livrate ministerelor centralizat în baza de contract de către STISC, care dispune de resurse umane si tehnologice necesare.
- Ministerul Agriculturii și Industriei Alimentare – a raportat despre lipsa specialiștilor în domeniu, invocând și alte motive precum schimbarea sediului și reorganizarea instituției.
- Ministerul Mediului – a informat despre realizarea unor măsuri de securitate cibernetică și unele acțiuni au fost planificate și urmează a fi implementate în anul următor.
- Ministerul Justiției, Ministerul Educației și Cercetării, Ministerul Culturii, Ministerul Sănătății – nu au răspuns nici la una din solicitările scrise ale AGE, iar la adresările

prin telefon au argumentat că nu dispun de resurse, în special umane, pentru realizarea recomandărilor.

Astfel, se constată că entitățile cu profil aferent prestării serviciilor bazate pe TIC au realizat o parte considerabilă din recomandările misiunilor de audit, dar totuși, în majoritatea autorităților administrației publice, se constată un nivel scăzut de implementare a Cerințelor minime de securitate cibernetică, în special a măsurilor organizaționale și administrative. Se denotă o problemă majoră în conștientizarea managementului de a aloca/asigura resursele necesare implementării cerințelor minime de securitate cibernetică.

Pentru anul 2022, AGE a planificat efectuarea misiunilor de audit de securitate cibernetică în cadrul a 4 entități publice (în limita bugetului alocat). Astfel, în luna iunie 2022, a fost inițiată procedura de achiziție a serviciilor de audit securitate cibernetică, care ulterior a fost anulată din motivul depășiri mijloacelor financiare bugetate. Ulterior, la organizarea repetată a procedurii de achiziție, a participat doar un ofertant care nu a întrunit cerințele de calificare, respectiv procedura de achiziție fiind anulată.

În cadrul STISC a fost desfășurată misiunea de audit de securitate cibernetică privind implementarea Hotărârii de Guvern Nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică, realizată de I.P. „Agenția de Guvernare Electronică”. Urmare a Raportului prezentat în acest sens, STISC a aprobat Planul privind înlăturarea neconformităților evidențiate în rezultatul misiunii de audit de securitate cibernetică, care este în proces de implementare.

În contextul reorganizării structurale și funcționale a ASP și inactualității listei de persoane responsabile de executarea măsurilor prevăzute în anexa planului nr.1 la Ordinul ASP nr. 300 din 01.07.2022 „Cu privire la aprobarea Planului de măsuri în vederea realizării recomandărilor auditului de securitate cibernetică, este necesară realizarea următoarelor măsuri organizatorice prioritare pentru finalizarea implementării acțiuni:

a) revizuirea Anexei nr. 2 la Ordinul ASP nr. 300 din 01.07.2022, Lista persoanelor din subdiviziunile ASP, responsabile în limitele competențîlor pentru executarea măsurilor prevăzute în Planul de măsuri;

b) revizuirea Anexei nr.1 la Ordinul ASP nr. 300 din 01.07.2022, potrivint rezultatelor implementării Planului de măsuri prezentate în Raport privind remedierea neconformităților în vederea realizării recomandărilor auditului de securitate cibernetică efectuat în ASP de către Agenția de Guvernare Electronică cu privire la implementarea prevederilor Hotărârii de Guvern nr.201/2017 privind aprobarea Cerinţelor minime obligatorii de securitate cibernetică.

Pentru realizarea recomandărilor auditului privind continuității funcționării subdiviziunilor Agenției a fost emis Ordinul ASP nr. 1014 din 29.11.2022 „Cu privire la implementarea Planului de asigurarea a continuității activității în cadrul centrelor multifuncționale ale Departamentului management servicii publice”.

În anul 2022 în cadrul PG s-au întreprins măsuri în vederea implementării recomandărilor auditului de securitate cibernetică din anul 2021.

În cadrul MA în 2022 au fost efectuate două audite interne ale securității informaționale și apărării cibernetice.

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	Parțial realizat

Instituția responsabilă: *Agenţia de Guvernare Electronică.*

În procesul de prestare a serviciilor electronice publice 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 201/2017 și furnizarea soluțiilor, recomandărilor de remediere a neconformităților identificate în rapoartele de audit pentru fiecare entitate auditată.

În ce privește serviciile electronice publice prestate de către AGE, acestea sunt testate de către o companie de consultanță, contractată în acest sens, pentru evaluarea sistemelor informaționale, aflate în gestiunea AGE, în conformitate cu standardele și practicile internaționale, care acoperă cerințele de securitate cibernetică stipulate în HG 201/2017. Astfel, în anul 2022 au fost efectuate teste de securitate, inclusiv de penetrare și evaluare a codului sursă, pentru sistemele dezvoltate pe parcursul anului. Rezultatele testelor, cu recomandările de rigoare, au fost preluate în lucru pentru înlăturarea neconformităților identificate, în termenii și modul stabilit.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii 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 opinia experților Serviciului de Informații și Securitate, actualmente, nu există temei legal de a obliga prestatorii de servicii informaționale *(persoane fizice și juridice),* care gestionează *(pagini web, platforme, bloguri)* să respecte cerințele obligatorii de securitate cibernetică.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
2/4	Identificarea unui mecanism legal de 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.*

În perioada de referință Serviciul Tehnologii Informaţionale a MAI nu a inițiat discuții cu alte instituții naționale și sectorul privat privind aspectele juridice și practice ale cooperării publice private în vederea acordării de către acestea a accesului la codul-sursă al aplicațiilor elaborate, comercializate și distribuite pentru autoritățile publice.

Conform prevederilor OMAI nr. 195/2016 „Cu privire la implementarea practicilor de management centralizat al serviciilor de Tehnologia Informației și Comunicațiilor în cadrul MAI", STI avizează/coordonează caietele de sarcini și specificațiile tehnice parvenite de la autoritățile administrative și instituțiilor din subordinea MAI, și anume a clauzelor ce vizează obligațiunea prestatorului/furnizorului de a prezenta/furniza codul sursa pentru aplicațiile și softurile care fac obiectul contractului de achiziții.

Actualmente mai multe autorități naționale sunt parte, în calitate de beneficiari, al proiectului „Moldova Cyber Security Rapid Assistance", inițiat în august 2022, gestionat de STISC cu perioada de implementare 18 luni, partener de implementare din partea externă fiind Academia de Guvernare Electronică din Estonia. Proiectul este inițiat în scopul pentru fortificarea rezilienței cibernetice și asigurarea securității informaționale a țării și va contribui la consolidarea eforturilor instituțiilor specializate, dar și implementarea unui model sustenabil de gestiune a domeniului, bazat pe experiența națională și internațională. Ariile de interes/intervenție ale proiectului:

1. Liderismul și Guvernanța;
2. Incidentele și managementul riscurilor;
3. Infrastructuri critică publică și private;
4. Educația, trening și bunele practici.

Acțiunile principale ale proiectului se grupează în 2 obiective: Consolidarea rezilienței cibernetice a structurilor guvernamentale și Managementul riscurilor și incidentelor de securitate cibernetică.

Cadrul normativ care urmează a fi promovat/ajustat în contextul proiectului în cauză va viza inclusiv metodologia ciclului de viață a softurilor, inclusiv ce ține de obligațiile de a obține codul-sursă al aplicațiilor implementare la nivel instituțional și testarea acestora din punct de vedere a securității cibernetice. De asemenea, pe parcursul anului 2022 au fost verificate și modificate parolele de acces a utilizatorilor sistemelor informaționale, a efectivului din subordinea MAI. În parte ce ține de interacțiunea cu autoritățile publice, persoane juridice sau fizice, ce ține de identificarea unui mecanism legal în vederea acordării de către acestea a accesului la codul-sursă nu au avut loc. De menționat, că în 2022, au fost organizate și petrecute mai multe ședințe de lucru cu partenerii străini, care la rândul lor au venit în ajutor cu diferite programe de asistență tehnică și propuneri de acordarea suportului pe domeniu, care ulterior urmează să fie discutate la nivel ministerial prin încheierea acordurilor de colaborare.

Cadrul normativ instituțional al SIS – Regulamentul cu privire la avizarea dispozitivelor și produselor asociate semnăturii electronice (Ordinul Directorului SIS nr. 25/2017), stabilește expres procedura privind accesul la codul-sursă al aplicațiilor și produselor informaționale utilizate în procesul prestării serviciilor de certificare a cheii publice și nu necesită a fi revizuit, ajustat și modificat.

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

Instituția responsabilă: *Autorităţile administraţiei publice.*

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 partea ce ține de realizarea acțiunilor de coordonare cu CNPDCP 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 ce 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 2022, CNPDCP a avizat un șir de proiecte de acte normative, prezentate spre examinare de către autoritățile administrației publice, prin care a venit 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 securităţii statului și sistemului naţional de apărare	Perioada 2019-2020, cu verificarea anuală a indicatorilor de progres	Parțial realizat

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

Potrivit obiectivului acțiunii, pe parcursul anului 2022 Ministerul Apărării a realizat următoarele acțiuni:

- s-a propus includerea în proiectul „legii securității cibernetice” prevederile apărării cibernetice;
- pe data de 14.11.2022 s-a desfășurat ședința de lucrul asupra definitivării specificațiilor tehnice a tehnicii și echipamentelor procurate prin intermediul programului de asistență externă European Peace Facility (EPF).

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

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

În anul 2022, de către SIS au fost identificate unele vulnerabilități în sistemele interne de comunicații și informatică ale Armatei Naționale, pe aspectele menționate fiind informat Ministerul Apărării și înaintate propuneri de remediere a situației și soluții pentru anticiparea vulnerabilităților sesizate.

În 2022, prin HG nr. 737/2022, au fost aprobate prin set unic proiectele elaborate și promovate de către SIS privind Programul și Planul național de consolidare și realizare a măsurilor de protecție antiteroristă a obiectivelor infrastructurii critice pentru anii 2022-2026. În semestrul I al a. 2022 a fost revizuit și actualizat Capitolul IV. Securitatea Cibernetică/ Pașaportul antiterorist pentru infrastructura critică – anexă la Ordinul directorului SIS nr. 50/2018, care extinde și exemplifică cerințele de securitate cibernetică pentru infrastructurile critice naționale.

Complementar, în anul 2022 SIS a emis avizul la Proiectul Hotărârii Guvernului privind aprobarea Proiectului de lege privind securitatea cibernetică (nr. 41/ME/2023), care prevede măsuri la nivel național pentru consolidarea capacităților de apărare cibernetică, inclusiv și a infrastructurii critice.

Pe parcursul anului 2022, în cadrul MA s-au întreprins următoarele acțiuni:

- elaborarea cerințelor de securitate specifică pentru sistemele informaționale atribuite la secretul de stat;
- managementul programelor de asistență externă pentru procurarea echipamentelor de criptare a traficului.

PG este parte a proiectului „Moldova Cybersecurity Rapid Assistance” cu subiectul „Administrarea securităţii cibernetice şi rolul echipei de intervenţia în caz de urgenţă informatică (CERT)” și a participat la elaborarea propunerilor privind măsurile de apărare cibernetică pentru protecţia infrastructurii critice naţionale, precum şi a altor sectoare prioritare pentru stat. PG a întreprins acţiuni pe interior îndreptate spre evaluarea situaţiei curente.

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	Realizat

Instituția responsabilă: *Serviciul de Informații și Securitate*

În anul 2022, Serviciul a elaborat 31 de avize consultative prin care a acordat suport structurilor de securitate TIC din cadrul autorităților publice la implementarea măsurilor de protecție a sistemelor informaționale ce prelucrează informații atribuite la secret de stat.

Concomitent, SIS a emis avizul consultativ la Proiectul cerințelor de securitate specifice (CSS) elaborat de către o societate comercială pentru elaborarea documentației necesare certificării sistemelor informaționale din posesie. Potrivit datelor, agentul economic are ca domeniu de activitate: realizarea de programe și consultanță în domeniul IT *(activități de realizarea softurilor la comandă)*, prelucrarea datelor activități legate de băncile de date.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În anul 2022, SIS a procurat o serie de echipamente ce urmează să consolideze securitatea sistemelor speciale de comunicații electronice.

De asemenea, SIS 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 anul 2022, a fost efectuată o procedură de audit a rețelei interne din cadrul SIS. La fel, ofițerii SIS au beneficiat de un curs de instruire pentru 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.*

În perioada de referință, în adresa SIS nu au parvenit solicitări de revizuire și modificare a cadrului normativ, dat fiind faptul că ultimele actualizări au avut loc

în anul 2020, prin Hotărârea Guvernului nr. 965/2020 pentru modificarea Regulamentului cu privire la sistemele speciale de telecomunicații ale Republicii Moldova, aprobat prin Hotărârea Guvernului nr.735/2002.

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.*

Conform prevederilor Legii nr. 175/2021 pentru modificarea unor acte normative, în vigoare din 10.01.2022, au fost introduse modificări la Legea nr. 133/2011 privind protecția datelor cu caracter personal, fiind 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.

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, înregistrat în Parlamentul RM cu nr. 422 din 22.11.2018.

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

Instituția responsabilă: *Serviciul de Informaţii şi Securitate.*

În perioada vizată, de către experții SIS a fost verificată conformitatea condițiilor de licențiere a 8 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 protecţie a informaţiei	Perioada 2020-2023, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituția responsabilă: *Serviciul Vamal, Serviciul de Informații și Securitate.*

Serviciul Vamal deține certificate de securitate de tip SSL Wild Card pentru securitatea informațiilor din cadrul domeniul „md”.

Securitatea în sistemele informaționale și serverele locale ale SV este asigurată prin Firewall, antivirus licențiat și Chei de securitate VPN Check point.

Serviciul Vamal de comun cu Serviciul de Informaţii şi Securitate examinează sistemele actuale de monitorizare a importului mijloacelor de protecţie a informaţiei şi sunt în proces de perfecţionare a acestuia conform rigorilor de securitate şi riscruilor identificate.

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 protecţiei criptografice a informaţiei la cadrul normativ european	Anul 2021, cu verificarea anuală a indicatorilor de progres în cazul realizării înainte de termen	Realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

Cadrul normativ de bază la acțiunea respectivă nu necesită modificări și se asigură prin Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere, care transpune parțial Regulamentul (UE) nr. 910/2014 al Parlamentului și al Consiliului European 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, publicat în Jurnalul Oficial al Uniunii Europene L 257 din 28 august 2014.

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	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În anul 2022, SIS a recepționat Raportul de activitate al prestatorului de servicii de certificare în domeniul aplicării tuturor tipurilor de semnături electronice pentru perioada anului 2021, elaborat de I.P. „STISC”.

În anul 2022, SIS a realizat un control al prestatorului de servicii de certificare din cadrul I.P. STISC. Totodată, în perioada de referință a fost stabilită o încălcare

a cadrului normativ ce stabilește procedura de prelucrare a cererii de certificare a cheii publice (01.04.2022).

De menționat că controlul planificat pentru trimestrul IV a. 2022, nu a fost efectuat în contextul necesității de reacreditare a prestatorilor conform Legii 124/2022.

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

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

În 2022, au avut loc 42 de instruiri la care au participat 87 de angajați ai Ministerului Afacerilor Interne. Aceste instruiri au inclus: produsele software utilizate la investigarea exploatării sexuale online a copiilor, investigațiile online pe dimensiunea Criptomonedelor și Dark Web-Ecdwi, , Digital Intelligence, Methods to Obtain Data from WhatsApp, Viber, and Telegram on an Android Device, IC Applied and Pragmatic Services for Policing (Law Enforcement only), Locked iPhones investigation, Penetration Testing Practitioner (PTP) - Training Course and Assessment, INTERPOL Young Global Police Leaders Programme, produsul „SOLIS”, destinat investigării abuzului sexual online asupra copiilor , AcțiunepentruJustiție!Pentru tinerii din ediția a V-a Acțiune pentru Justiție, în cadrul instruirii dedicate „Criminalității Informatice", Stop Cyber Attacks: Stopping Ransomware with Autonomous Response”, în cadrul căreia s-a prezentat detaliat Tehnologia Darktrace, precum și serviciile profesionale de SOC 24x7, instruire pentru aplicarea legii privind investigarea atacurilor ransomware, TOPCOP-Dark web. Online investigation, Tech Against Traffiking Acceletor, vizită de studiu la Europol în cadrul Proiectului privind combaterea criminalității organizate, Pirateria digitală și criptomoneda, cursul de formare „Investigarea crimelor informatice”, cursul intermediar de formare a investigatorilor și a forțelor de ordine în domeniul criminalității cibernetice și al probelor electronice, Intermediate Training Course for investigators and law enforcement on cybercrime and e-evidence, instruire în domeniul combaterii traficului de ființe umane, exploatării sexuale, abuzului și hărțuirii, sub egida OIPC Interpol, Internațional Task Force-2022 Pittsburgh, cursul de instruire în domeniul combaterii infracțiunilor comise prin intermediul platformelor de Streaming, cursul de instruire în domeniul utilizării bazei de date internaționale a INTERPOL privind exploatarea sexuală a copiilor (ISCE), vizita de lucru în cadrul proiectului „ Consolidarea capacității Republicii Moldova de contracarare a abuzului și exploatării sexuale online”, „Atacurile cibernetice-Criptomonedele, frauda de plăți online, sistemul malware”, „Investigarea infracțiunilor cibernetice”, „Investigarea crimelor informatice”, „Ultimele amenințări cibernetice, tendințe și strategii de combatere a criminalității cibernetice”.

Aceste instruiri au avut un impact pozitiv asupra capacității de investigație a angajaților din MAI Republica Moldova în domeniul infracțiunilor informatice, mai ales în ceea ce privește investigarea exploatării sexuale online a copiilor și a infracțiunilor cu criptomonede. În plus, instruirile au oferit oportunitatea angajaților de a învăța despre cele mai noi tehnologii și metode de investigație utilizate la nivel internațional în domeniul combaterii criminalității informatice.

Totodată, în perioada anului 2022, angajații IGP au participat și acordat suport în cadrul a 2 acțiuni comune de investigații cu caracter internațional, după cum urmează:

- investigații la nivel internațional desfășurate în comun cu autoritățile din cadrul Biroului Federal de Investigații din SUA și omologii din Franța, în privința unui grup de persoane, care administrau un șir de bulletproof hosting-uri, comercializate prin rețelele „Darknet", care oferă servicii de protecție în privința autorităților de drept, folosite în vederea accesării ilegale a sistemelor informatice, plasare de pagini pshishing, spălare de bani și alte acțiuni ilegale, prin intermediul cărora unui șir de companii fiind cauzate prejudicii în proporții deosebit de mari;
-investigații la nivel internațional cu suportul subdiviziunii specializate a Biroului Federal de Investigații din SUA în privința unui grup de persoane care se ocupă cu producerea, importul, comercializarea sau punerea la dispoziție, sub orice altă formă, în mod ilegal, a mijloacelor tehnice sau produse program, concepute sau adaptate în scopul accesării ilegale a sistemelor informatice la nivel național și internațional.

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

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

Pe parcursul anului 2022, angajații Inspectoratului General al Poliției a MAI au participat în calitate de formatori în cadrul a 3 sesiuni de instruire, după cum urmează:

- la 13.04.2022, 1 angajat al poliției a participat în calitate de formator în cadrul modulului de instruire organizat de Academia „Ștefan cel Mare" a MAI, privind investigarea abuzului sexual online asupra copiilor, pentru studenții anului III a Facultății de Drept a Academiei „Stefan cel Mare";
- la 02.06.2022, a fost realizată instruirea de bază privind investigarea crimelor informatice, destinată ofițerilor angajați fără experiență din cadrul Poliției;
- la 22.09.2022, 1 angajat al poliției a participat în calitate de formator la atelierul de instruire: "Utilizarea în siguranță a cardului de plată, aplicarea tuturor măsurilor necesare pentru minimizarea fraudelor şi descurajarea tentativelor de fraudă cu cardurile de plată", fiind instruiți 100 de ofițeri de investigații din toată țara. Evenimentul organizat de către BNM a RM și DIIII a IGP, în incinta ASEM.

Totodată de către INI al IGP se examinează posibilitate organizării sesiunilor de instruire pentru subdiviziunile teritoriale.

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 Poliţiei), Procuratura Generală.*

Pe parcursul anului 2022, Direcția investigații infracțiuni informatice a INI al IGP al MAI a fost dotată cu echipament și soft-uri specializate pentru investigarea infracțiunilor informatice în sumă totală 69.368 dolari SUA. Donația a parvenit din partea Ambasadei SUA în Republica Moldova.

În perioada de referință, 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	Parțial realizat

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

Legislația în domeniul salarizării are un caracter unitar, transparent, echitabil, nediscriminatoriu, capabilă să reflecte și să remunereze performanța profesională din domeniul de activitate. Conform prevederilor legale, Ministerul Finanțelor evaluează sistemic cel puțin o dată la 5 ani funcțiile în sectorul bugetar pentru a elimina eventualele discrepanțe atestate, 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 Poliţiei), Procuratura Generală.*

În anul 2022, angajații poliției au participat la un total de 10 activități de instruire în calitate de formatori la instruirile organizate pentru judecători și procurori. Aceste instruiri au acoperit o varietate de subiecte importante, cum ar fi

investigarea infracțiunilor cu caracter sexual săvârșite de minori și împotriva minorilor, abuzul online al minorilor, particularitățile investigării și judecării infracțiunilor în domeniul informaticii și telecomunicațiilor și măsurile speciale de investigații aplicate în vederea descoperirii criminalității informatice.

Instruirile au avut ca scop dezvoltarea abilităților și cunoștințelor judecătorilor și procurorilor în domeniul investigării și prevenirii infracțiunilor de pornografie infantilă pe Internet, astfel încât aceștia să poată îndeplini cu mai multă eficiență și profesionalism atribuțiile specifice acestor domenii.

Totodată, în perioada anului 2022 de către INI a IGP au fost înregistrate și investigate 36 cazuri de abuz sexual în mediul online asupra copiilor, dintre care:
- conform prevederilor art.208/1 CP (pornografia infantilă) – 29 cazuri;
- conform prevederilor art. 175 CP (Acțiuni perverse) – 7 cazuri.

În perioada de raport de către angajații Poliției a fost acordată asistență pentru 3 minori și audierea cu participarea psihologului din cadrul CI „La Strada" a 8 minori.

Pentru comiterea infracţiunilor prevăzute la art. 208[1] din Codul penal al Republicii Moldova, în cadrul PG a fost înregistrat un număr de 39 de cauze penale. Cauze transmise în judecată – 33, sentinţe de condamnare în număr de 21.

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

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

În perioada anului 2022 de către INI al IGP au fost înregistrate 7 cazuri de ademenirea copiilor în mediul online – art. 175 (Acțiuni perverse).

Procuratura Generală – Pentru comiterea infracțiunilor prevăzute la art. 175[1] din Codul penal al Republicii Moldova, în anul 2022, au fost pornite 7 cauze, care sunt la faza de urmărire penală.

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

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

Întru realizarea acțiunii în perioada de raport de către IGP al MAI a fost întreprinse următoarele acțiuni:
- la 08.02.2022, un angajatal al IGP a participat în calitate de mentor și membru al juriului în cadrul evenimentului Online Safety Ideathon „Think before you share" (Gîndește înainte de a distribui), organizat de Yep!Moldova, în contextul Zilei

Internaționale a Siguranței pe Internet, la care au participat 54 de tineri care au format 7 echipe, au făcut un brainstorming de idei și au venit cu soluții pentru problemele găsite. Problemele-cheie abordate au fost: Sexting, Șantajul online, Confidențialitatea și informațiile personale, Cyberbullying-ul, Știri false și Escrocheria online;
- la 13.04.2022, a fost realizată o lecție privind investigarea abuzului sexual online asupra copiilor, pentru studenții anului III a Facultății de drept a Academiei „Stefan cel Mare";
- la 14.02.2022, a fost realizată o ședință de lucru în comun cu Poliția din Regatul Țărilor de Jos, Ofițerul de legătură al Regatului Țărilor de Jos, Șeful CCTP al INI al IGP al MAI, Directorul STI și Rectorul UTM, cu scopul înființării la nivel de UTM a RM a unui centru de cercetare a fenomenului de exploatare sexuală a copiilor și traficului de persoane, în special sub aspectul tehnologic;
- la 23.06.2022, a fost realizat o activitate de informare a pedagogilor și psihologilor din cadrul Asociației Obștești „SOS Autism", fiind abordat fenomenul abuzului copiilor în spațiu internet;
- la 27.07.2022, a fost desfășurată prezentarea pe tematica „Siguranța copiilor în spațiu online" în cadrul proiectului Școlii de Vară „Police Explorer". La eveniment au participat 50 de elevi ai claselor 11-a din 15 raioane ale Republicii Moldova.

Totodată, în perioada anului 2022, Poliția în comun cu CI „La Strada", în cooperare cu organizația „INHOPE", cu suportul Ambasadei SUA la Chișinău a inițiat realizarea activităților de creare a unui Mecanism de raportare a materialelor de abuz sexual asupra copiilor. În acest sens, Poliția în comun cu CI „La Strada" a elaborat Proiectul Conceptului privind crearea mecanismului de raportare a materialelor de abuz sexual asupra copiilor și proiectul Regulamentul de funcționare şi organizare a Serviciului de raportare a materialelor de abuz sexual asupra copiilor, fiind aprobat prin Ordinul IGP nr. 480 din 29.12.2022.

Pe pagina oficială a Poliției au fost publicate 2 comunicate privind siguranța copiilor în internet, după cum urmează:
- la 08.02.2022 pe siteul oficial al Poliției Republicii Moldova, a fost mediatizat un comunicat în contextul marcării „Zilei siguranței pe Internet" link: https://politia.md/ro/content/ziua-sigurantei-peinternet-politia-vine-cu-ecomandari-privind-securitatea-mediulonline;
-la 01.07.2022, a fost mediatizat pe pagina oficială a Poliției, comunicatul: Protecția copiilor împotriva exploatării sexuale și abuzurilor sexuale - obiectivul principal al poliției;
https://politia.md/ro/content/protectia-copiilor-impotriva-exploatariisexuale-si-abuzurilor-sexuale-obiectivul-principal.

Totodată ăn perioada de raport angajații poliției au participat la 6 emisiuni/interviuri, după cum urmează:
- la 09.02.2022, un angajat al IGP a oferit un interviu la TVR Moldova, cu tema: "Siguranța în mediul online a copiilor la data de 08.02.2022, a fost mediatizat pe siteul oficial al Poliției Republicii Moldova un comunicat privind „Ziua Siguranței pe Internet: Poliția vine cu recomandări privind securitatea în mediul online";

https://politia.md/ro/content/ziua-sigurantei-pe-internet-politia-vinecu-recomandari-privind-securitatea-mediul-online;
- la 22.02.2022, 1 angajat al IGP a acordat un interviu canalului de televiziune Jurnal TV despre canalele telegram, unde sunt minori implicați în pariuri, jocuri de noroc;
- la 10.06.2022 1 angajat al IGP a acordat un interviu la TV8, pe subiectul: „Fenomenul abuzului sexual față de copii este în creștere".
https://tv8.md/ru/2022/10/06/specialistii-atentioneaza-fenomenulabuzului-sexual-fata-de-copii-este-in-crestere/202666;
- la 29.06.2022 un angajat al IGP a participat la emisiunea „Acasă", difuzată pe canalul youtube cu tema: „Abuzul sexual online. Cum sunt atraşi copiii şi ce trebuie să cunoască părinţii"; https://www.youtube.com/watch?v=IhtSLzLQFAk
- la 21.07.2022, 1 angajat al IGP, a participat la emisiunea „Telematinal" de la TVR Moldova, cu tema lansarea de către Meta a unui sistem de alertă pentru a ajuta la localizarea copiilor dispăruți din RM.
https://www.facebook.com/TVRMoldova/videos/405224721586902/
- la 26.10.2022, 1 angajt al IGP a oferit un interviu la Ziarul de Gardă, privind „Protecția și siguranța copiilor".

În anul 2022, în cadrul Institutului Național al Justiției, PG în calitate de formator, semestrial desfășoară cursuri de insturire cu tematicile „Metodici și tactici de identificare, investigare și judecare a infracțiunilor săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale" și „Particularitățile urmării 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, IGP al MAI efectuează permanent schimb de informații cu Departamentele de securitate ale instituțiilor financiare. Totodată, la 10.05.2022, trei angajați IGP au participat la o ședință cu reprezentanții BNM, unde au fost abordate mai multe subiecte referitor la desfășurarea campaniei de prevenire și combatere a infracțiunilor legate de cardurile bancare și de educație financiară a cetățenilor.

În vederea asigurării continuității acțiunilor îndreptate spre prevenirea și combaterea fraudelor prin utilizarea mijloacelor de plată electronice în perioada 02-22 noiembrie 2022, subdiviziunea specializată a Poliției, în bază Ordinul IGP nr. 392 din 01.11.2022, a desfășurat Campania „Fii precaut! Utilizează în siguranță cardurile de plată!". Scopul campaniei a constituit creșterea nivelului de

culturalizare financiară a populației. Activitățile de sensibilizare și informare a populație au fost desfășurate în mai multe zone ale Republicii Moldova.

În baza Acordului cu privire la schimbul de informații (în continuare – Acord) între Centrul pentru combaterea crimelor informatice din cadrul MAI și Banca Națională a Moldovei, a fost examinată oportunitatea de extindere a spectrului de informații ce constituie obiect al Acordului, părțile au concluzionat, reieșind din complexitatea informației, că furnizarea unor informații suplimentare decât cele prevăzute în formatul actual al schimbului de date, va fi efectuată la necesitatea și cererea expresă a părților, conform prevederilor capitolului II al Acordului, fără modificări suplimentare ale acestuia.

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

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

În perioada anului 2022, în urma mai multor atacuri asupra ATM-urilor pe teritoriul țării, de către INI al IGP au fost întreprinse măsuri de investigații în scopul identificării persoanelor culpabile, totodată au fost înaintate sesizări către instituțiile bancare privind implementarea unor noi măsuri de securitate.

Cu referire la promovare a unor măsuri de securitate sporită în privința bancomatelor (ATM-urilor) la nivel de hardware și software, băncile licențiate în Republica Moldova au asigurat migrarea tuturor bancomatelor la sisteme de operare ce dispun de suport din partea furnizorilor.

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.*

Cu privire la identificarea mecansimelor comune de combatere a fraudelor în tranzacțiile cu card și fără card (card-present și card not-present), BNM a publicat pe pagina web oficială și pe rețelele de socializare un comunicat prin care a îndemnat cetățenii să asigure confidențialitatea informațiilor despre cardurile de plată deținute, cu referire la recomandările pentru îmbunătățirea siguranței utilizării cardului de plată plasate pe pagina web a BNM.

Totodată, la data de 23.09.2022, BNM a organizat un atelier de lucru pentru reprezentanții MAI la tema „Utilizarea în siguranță a cardului de plată, aplicarea tuturor măsurilor necesare pentru minimizarea fraudelor și descurajarea

tentativelor de fraudă cu cardurile de plată", având scopul de a îmbunătăți cultura financiară în societate și de a preveni fraudele aferente.

PG, de comun cu BNM, a prevăzut în Acordul cu privire la schimbul de informații mecansimele comune de combatere a fraudelor cu card și fără card. La fel, PG 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 atelefoanelor mobil, 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	Parțial realizat

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

În scopul realizării acțiunii, pe parcursul anului, 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. Rețeaua a fost creată în baza ord. IGP 429 din 07.11.2019.

Totodată, pe parcursul perioadei de raport în cadrul Direcției de poliție a mun. Chișinău a fost creat Serviciu specializat, responsabil de investigare infracțiunilor informatice, la fel a fost mărit numărul ofițerilor responsabili de investigarea crimelor informatice din cadrul Direcției investigarea crimelor informatice a INI a IGP de la 30 la 35 de angajați.

La 28 decembrie 2022, Guvernul RM a aprobat Programul de prevenire și combaterea a criminalității pentru anii 2022-2025, care prevede crearea unităților regionale de investigare a infracțiunilor informatice.

Prin Ordinul Procurorului General nr. 33/3 din 03.05.2022 a fost aprobat un nou Regulament al Procuraturii, prin care Secția Tehnologii Informaționale și Combaterea Crimelor Cibernetice a fost reorganizată, fiind formate în cadrul PG două subdiviziuni distincte: Secția Combatere Crime Cibernetice și Secția Tehnologii Informaționale din cadrul Aparatului Procurorului General. În consecință, au fost divizate funcțiile de asigurare tehnică a securității a instituției și funcția de combatere a criminalității cibernetice.

La fel, a fost creată subdiviziunea specializată Biroul anti-trafic și de imvestigare a crimelor cibernetice din cadrul PCCOCS. A fost creată Secția exercitare a urmării penale din cadrul Procuraturii mun. Chișinău Oficiul Principal și a fost elaborată Dispoziția cu privire la crearea birourilor specializate din cadrul PCCOCS.

Capacitățile SIS în combaterea criminalității informatice sunt funcționale și în proces de modernizare, îmbunătățire și dezvoltare continuă. Astfel, în anul 2022, în

scopul preluării bunelor practici și schimbului de experiențe în domeniul combaterii și investigării criminalității informatice, ofițerii SIS au participat la evenimente publice și instruiri.

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

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

La 26.12.2022 a avut loc în sediul MAI – Serviciul Tehnologii Informaționale, o ședință la care au participat reprezentații din cadrul mai multor instituții de stat – PG, SIS, STI a MAI, unde a fost discutat subiectul creării bazei de date naționale privind evoluția fenomenului criminalității informatice. În rezultat s-a stabilit că crearea unei baze de date separată cu privire la dezagregarea datelor pe anumite categorii de infracțiuni, la moment ar contravine Legii 216/2003. Soluția optimă, ar fi dezvoltarea modulelor suplimentare în Sistemul gestionat de MAI, însă acestea urmează a fi definite reieșind din posibilitățile instituționale (modernizarea la zi a bazei de date existente). Baza de date actuală, rulează pe o platformă învechită și la moment MAI este în procesul de identificare a posibilităților tehnice și resurselor financiare în vederea migrării informației existente pe o platformă modernă, cu o securitate informațională sporită, în care va fi posibilă și dezvoltarea și actualizarea modulelor noi conform necesităților. Acțiunea a fost transpusă pentru a fi implementată în anul 2023.

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 informaţiilor criminalistice și criminologice”	Permanent, cu verificarea anuală a indicatorilor de progres	În proces de realizare

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

Actualmente, în cadrul Sistemului informațional automatizat *„Registru informației criminalistice și criminologice*” sunt supuse evidenței centralizate toate tipurile de infracțiuni, prevăzute de Codul Penal, inclusiv infracțiunile în domeniul criminalității informatice.

Statistica PG cu privire la activități desfășurate în domeniul criminalității informatice, poate fi generată în Sistemul Informațional Automatizat „Urmărire penală E-Dosar”. Banca centrală de date a Sistemului informațional automatizat „Registrul informațiilor criminalistice și criminologice” este gestionată de MAI, la subiect Procuratura Generală a participat la discuții cu MAI, în contextul modificării ordinului comun de evidența unică a infracțiunilor, iar în anul 2022 a

fost pusă în discuție o nouă variantă a proiectului de Ordin comun privind evidența sesizărilor (inclusiv electronică), la care Procuratura a venit cu obiecțiile sale. Până la moment varianta finală nu a fost prezentată de către STI al MAI, fiind instituit un grup de lucru interinstituțional din care fac parte și reprezentanți ai PG.

Pe parcursul anului 2022 „Registrul informațiilor criminalistice și criminologice" a fost completat de către CNA în conformitate cu prevederile Ordinului comun nr.121/254/286-O/95 din 18.07.2008 cu privire la evidenţa unică a infracţiunilor, a cauzelor penale şi a persoanelor care au săvârşit infracţiuni.

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

Instituția responsabilă: *Procuratura Generală.*

PG 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 contextul inițierii procesului de abrogare a Ordinului interdepartamental al Procurorului General, Ministrului Afacerilor Interne, Directorului general al Serviciului Vamal, Directorului Centrului pentru Combaterea Crimelor Economice şi Corupţiei nr. 121/254/286-O/95 din 18.07.2008 şi a Ordinului interdepartamental nr. 198/84/11/166/10/2-30/44 din 04.05.2007, cu promovarea unor reglementări noi în domeniu, inclusiv implementarea SI „E-Dosar", la 28.02.2023, în cadrul STI al MAI a avut loc prima şedinţă a grupului de lucru, pentru elaborarea cadrului normativ care reglementează instituirea Sistemului informațional automatizat E-Dosar, precum și implementarea, dezvoltarea și interconectarea acestuia.

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

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

Potrivit prevederilor Programului 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 în conformitate cu prioritatea strategică „COMPETITIVITATE ECONOMICĂ ȘI TEHNOLOGII INOVATIVE", în cadrul căreia este în derulare proiectul realizat

de către Institutul de Matematică și Informatică „Vladimir Andrunachievici” (USM) – „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	Parțial realizat

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

Pe parcursul anului 2022, au fost realizate 6 campanii de informare și sensibilizare a societății pe rețelele de socializare și pagina oficială a IP STISC, de asemenea au fost plasate 3 ghiduri de informare pe pagina web oficială https://stisc.gov.md și 54 anunțuri/publicații pe rețelele de socializare și pagina oficială a STISC privind amenințările, vulnerabilitățile şi riscurile la adresa securității cibernetice cu scopul de a spori conștientizarea utilizatorilor de Internet privind potențialele atacuri cibernetice, impactul acestora și importanța Siguranței Online, inclusiv de a promova igiena cibernetică. Perioada desfășurării campaniilor au fost de la o săptămână până la o lună, timp în care STISC a publicat informații, postări scurte cu recomandări, date statistice, acțiuni prioritare, cu referire la provocările din mediul on-line, cerințele minime pentru a face din internet un loc mai sigur și mai bun pentru fiecare, în special pentru tânăra generație. Desfășurarea campaniilor de informare a avut impact pentru cca 128 865 mii de utilizatori în mediul online și a generat un rezultat maxim de conștientizare și dezvoltare a capacităților, dar și extindere a conceptului securității cibernetice la nivel național.

Agenția de Guvernare Electronică a continuat în anul 2022 acțiunile de sensibilizare şi informare a societății privind amenințările, vulnerabilitățile şi riscurile la adresa securității cibernetice. În context, AGE a oferit instruiri în acest domeniu pentru grupuri de persoane interesate, copii, tineri etc, sub formă de ateliere, webinare, inclusiv la solicitare, și adaptate la nivelul de înțelegere și pregătire al beneficiarului. Totodată, AGE, în comun STISC, UTM și Proiectul Tehnologiile Viitorului, au semnat la 22 decembrie 2022, un Acord de parteneriat pentru crearea Academiei de Securitate Cibernetică, ce are drept obiectiv consolidarea securității informaționale a statului și dezvoltarea industriei pe segmentul securității cibernetice în Republica Moldova.

În anul 2022, SIS a lansat prin intermediul rețelei de socializare „Facebook” *7 campanii de informare* a societății civile, reprezentanților mass-media privind pericolele din spațiul informațional.

În contextul monitorizării amenințărilor la adresa spațiului cibernetic național, au fost identificate unele vulnerabilități de securitate și respectiv au fost anunțate următoarele autorități publice: Ministerul Justiției, CNAM, I.P. „STISC”.

Totodată, au fost pregătite materiale pentru ședința CSS pe domeniul amenințărilor, vulnerabilităților și riscurilor la adresa securității cibernetice.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
11/2	Realizarea de către Centrul național de reacție la incidente de securitate cibernetică a analizei strategice privind incidentele de securitate cibernetică și coordonarea acțiunilor de răspuns la astfel de incidente, inclusiv prin organizarea unor cursuri specializate de către experți calificați	Perioada 2021-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

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

Urmare aprobării Legii nr. 48/16.03.2023, autorităţile ce au competenţe în domeniu vor evalua sectoarele vulnerabile şi vor înainta propuneri de consolidare a nivelului de securitate cibernetică, care vor sta la baza politicilor de securitate promovate de pe platforma CERT Naţional.

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	Parțial realizat

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

În perioada de referință, reprezentanții I. P. STISC au particpat la următoarele exerciții de antrenamente de competență:

1. În data de 17 februarie 2022, a fost desfășurată cea de-a doua ediție a forumului economic EBA BUSINESS OUTLOOK 2022, la Chișinău. Evenimentul a fost organizat de EBA Moldova în parteneriat cu Delegația Uniunii Europene;
2. În perioada 22-25 februarie 2022, I.P. „STISC” în parteneriat cu „EU4Digital: Îmbunătățirea rezilienței cibernetice în țările Parteneriatului Estic” a organizat atelierul de lucru internațional privind amenințările cibernetice;
3. La data de 06 aprilie 2022 I.P. „STISC” a participat la un master-class online cu genericul „Cybersecurity Strategy Design and Implementation”. Evenimentul a fost organizat de Uniunea Internațională a Telecomunicațiilor și Banca Mondială;
4. În perioada 02-06 mai 2022, Autoritățile publice din Republica Moldova au participat la un program internațional de instruire în securitate cibernetică. Organizarea programului de instruire a fost facilitată de I.P. „STISC” în colaborare internațională cu Centrul European pentru Studii de Securitate George C. Marshall;
5. În perioada 01-31 august 2022 I.P. „STISC” a participat la un program de instruire internațională, cu tematica: „Capacity Building in International Law and Policy Formation for Enhancement of Measures to Ensure Cybersecurity”, lansat de Agenția Japoneză pentru Cooperare Internațională (JICA);

6. La data de 01 septembrie 2022 I.P. „STISC” a participat la un atelier de instruire internațională cu scopul de a cunoaște noi instrumente de îmbunătățire și dezvoltare a capacităților operaționale ale echipelor CERT naționale și guvernamentale. Eveniment organizat în cadrul proiectului Uniunii Europene Cybersecurity East;
7. În perioada 12-16 septembrie 2022 specialiști din cadrul I.P. „STISC” au participat la un exercițiu regional de cooperare în domeniul combaterii criminalității cibernetice, la Istanbul, Turcia. Eveniment organizat de proiectele: CyberEast și CyberSecurity EAST, finanțate de Uniunea Europeană;
8. În perioada 19-23 septembrie 2022 specialiști din cadrul I.P. „STISC” au participat la o sesiune de instruire cu exerciții practice de testare și dezvoltare a capacităților de reacție în cazul fraudelor de plată online și a programelor malware. Eveniment organizat de Agenția de aplicare a legii a Uniunii Europene (EUROPOL) și Agenția Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL);
9. În perioada 17-18 octombrie 2022, I.P. „STISC” în parteneriat cu CRDF Global și Academia Militară „General Mihailo Apostolski” a organizat Atelierul de instruire și conștientizare în securitate cibernetică cu tematica TTX (Table Top Exercise) - Evaluare, organizare, comunicare și reacție, unde au participat 23 persoane din cadrul a 12 instituții.

În contextul consolidării capacității de reacție la atacurile cibernetice, ofițerii SIS au participat la peste *10 evenimente* pe domeniul securității cibernetice.

Reprezentanții PG în anul 2022 a participat la următoarele evenimente:
- 15-16.11.2022 - exercițiul practic privind procedurile standard/protocol de acces la date între instituțiile de aplicare a legii și furnizorii de servicii/sector privat, (Proiectul CyberEast);
- 17-18.10.2022 - instruirea TTX - Assess, Organize, Communicate and React (I.P. ”STISC” în parteneriat cu CRDF Global a sesiunii de instruire-TTX-Assess, Organize, Communicate and React);
- Conferința națională anuală „XONTECH-CYBER SECURITY DAY 2022” cu genericul „Dezvoltarea unei infrastructuri puternice de securitate cibernetică în noile condiții de normalitate” 09.11.2022.

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	Parțial realizat

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

Pe parcursul anului 2022, I.P. STISC a organizat și desfășurat 5 ateliere de instruire în domeniul securității cibernetice destinat funcționarilor din sectorul public şi privat deţinători de elemente de infrastructură critică, cu scopul de a spori capacitățile în domeniul securității cibernetice și de a consolida mecanismul de

aplicare a cerințelor minime obligatorii de securitate cibernetică pentru a preveni cazurile de atacuri phishing, Dos și DDoS, incidente de tip ransomware. Totodată, prin organizarea și desfășurarea cursurilor de instruire I.P. STISC a avut ca obiectiv instruirea participanților în elaborarea și optimizarea metodologiilor și practicilor aplicate pentru combaterea riscurilor și atacurilor cibernetice, precum și de a familiariza personalul din sectorul public şi privat cu cele mai actuale instrumente și practici utilizate de actorii malițioși în penetrarea unei rețele supuse atacului cibernetic. De asemenea, participanții au avut oportunitatea să își îmbunătățească abilitățile în căutarea/verificarea contactelor sigure sau suspecte, utilizarea roboților, analizarea imaginilor și fotografiilor, identificarea fraudelor, profilurilor și informațiilor false precum să afle mecanismele de lucru cu registrul de date, inclusiv discuții despre cazuri reale și exemple de investigații complexe și să exerseze cazuri reale de investigații în domeniul securității cibernetice. În acest sens, au fost instruiți cca 900 de reprezentanți ai instituțiilor din sectorul public și cca 20 persoane de reprezentanți ai instituțiilor din sectorul privat.

În perioada de referință, ofițerii SIS au participat la 10 ateliere de lucru în domeniul asigurării securității cibernetice.

În anul 2022, zece procurori ai PG au participat la 3 ateliere de lucru, fiind analizate modalitățile de acumulare a informațiilor din surse deschise, precum și activitățile necesare pentru buna cooperare dintre sectorul public cu cel privat în domeniul identificării și contracarării amenințărilor cibernetice.

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*.

AGE, în comun cu STISC, a organizat instruiri tematice în domeniul securității cibernetice pentru specialiștii instituțiilor publice, după caz, cu certificarea cunoștințelor și abilităților obținute (Incident Response (25 persoane), CompTIA Security (10 persoane). De menționat că, entitățile publice acordă atenție acestor aspecte dependent de necesitățile organizaționale interne, în special, în contextul insuficienței personalului specializat în domeniul securității cibernetice și menținerii infrastructurilor TIC.

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	Parțial realizat

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

În anul 2022, I.P. STISC a desfășurata 6 campanii de informare și sensibilizare a societății pe rețelele de socializare și pagina oficială a STISC, de asemenea au fost plasate 3 ghiduri de informare pe pagina web oficială https://stisc.gov.md și 54 anunțuri/publicații pe rețelele de socializare și pagina oficială a STISC privind pericolele din spaţiul cibernetic şi măsurile de protecţie ce pot fi luate de către persoanele fizice şi juridic, cu scopul de a spori conștientizarea utilizatorilor de Internet privind potențialele atacuri cibernetice, impactul acestora și importanța Siguranței Online, inclusiv de a promova igiena cibernetică. Perioada desfășurării campaniilor a fost de la o săptămână până la o lună, timp în care STISC a publicat informații, postări scurte cu recomandări, date statistice, acțiuni prioritare, cu referire la provocările din mediul on-line, cerințele minime pentru a face din internet un loc mai sigur și mai bun pentru fiecare, în special pentru tânăra generație. Desfășurarea campaniilor de informare a avut impact pentru cca 128 865 mii de utilizatori în mediul online și a generat un rezultat maxim de conștientizare și dezvoltare a capacităților, dar și extindere a conceptului securității cibernetice la nivel național.

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.*

La etapa actuală, pregătirea specialiștilor în domeniul TIC se realizează în 8 instituții de învățământ superior, inclusiv: Universitatea de Stat din Moldova, Universitatea Tehnică a Moldovei, Academia de Studii Economice din Moldova, Universitatea Pedagogică de Stat ”Ion Creangă”, Universitatea ”Alecu Russo” din Bălți, Universitatea de Stat ”B.P.Hasdeu” din Cahul, Universitatea Liberă Internațională din Moldova, Universitatea de Studii Politice și Economice Europene.

În Nomenclatorul domeniilor de formare profesională și al specialităților în învățământul superior, domeniul 06 Tehnologii ale informației și comunicațiilor este un nou Domeniu fundamental al științei, culturii și tehnicii, care include 7 specialități: 0612.1 Calculatoare și rețele, 0612.2 Managementul informației, 0613.1 Tehnologia informației, 0613.2 Securitate informațională, 0613.3 Ingineria software, 0613.4 Informatică, 0613.5 Informatică aplicată. Totodată, formarea inițială a cadrelor în TIC se realizează și în cadrul domeniilor: 071 Inginerie și activități inginerești la specialitățile: 0714.2 Rețele și software de telecomunicații, 0714.6 Automatică şi informatică, 0714.7 Robotică și mecatronică, 0714.8 Securitatea sistemelor electronice și de telecomunicații etc.; 041 Științe economice la specialitatea 0410.4 Cibernetică și informatică economică; 011 Științe ale educației la specialitatea Informatică. În conformitate cu Planul de Activitate a

Guvernului, cu cerințele pieței muncii, Comanda de stat 2022 la ciclul I, licență, și la ciclul II, master, susține prioritar anumite domenii, unul dintre acestea fiind Tehnologii ale informației și comunicațiilor – 816, ceea ce reprezintă 10% din totalul Comenzii de Stat. În context, Comanda de stat în anul de studii 2022-2023, la Ciclul I, pentru domeniul separat Tehnologii ale informației și comunicațiilor a fost de 690 (2021 – 633) de locuri bugetare (665 zi + 25 fr.).

Totodată, MEC a planificat locuri bugetare la alte specialități conexe, inclusiv: 70 de locuri la Informatică (profil pedagogic); 10 locuri bugetare la Cibernetică și informatică economică; 20 locuri la Rețele și software de telecomunicații, 30 de locuri la Automatică şi informatică, 20 de locuri la Robotică și mecatronică, 10 de locuri la Securitatea sistemelor electronice și de telecomunicații, 10 de locuri la Electronică aplicată, 55 de locuri la Tehnologii și sisteme de telecomunicații – acestea fiind specialități din domeniul ingineresc. În anul de studii 2022-2023 la specialitatea 6132 Securitatea informațională își fac studiile 159 studenți iar la specialitatea 0714.8 Securitatea sistemelor electronice și de telecomunicații învață 8 studenți.

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*

AGE, în comun cu STISC și CRDF Global, a organizat cursul de instruire „Cyber Hygiene Workshop for Governance”, care a prevăzut dezvoltarea competențelor în domeniul cerințelor obligatorii de securitate cibernetică, cu formarea bunelor deprinderi de activitate în mediul online. De asemenea, cursul a presupus o testare finală nominală, în vederea evaluării nivelului de însușire a materialului propus, cu o informare ulterioară referitor la rezultatele obținute. La instruire au participat circa 500 de angajați din instituțiile publice.

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

Instituții responsabile: *Autoritățile administrației publice.*

În anul 2022, în temeiul *Raportului de evaluare a sectoarelor vulnerabile sub aspectul Comunicării strategice,* SIS a elaborat *nota informativă* privind aspectele problematice în sectorul de securitate națională sub expresia *Comunicării strategice la nivel interinstituțional*, fiind formulată/ înaintată propunerea de implementare a unui STRATCOM - național *(07.04.2022).*

În rezultat, propunerile SIS privind implementarea unui STRATCOM-național a fost remise conducerii statului și altor beneficiari legali. De menționat că

în cadrul informației remise a fost solicitată poziția instituțiilor privind completarea/ definitivarea *„Cadrului interinstituțional de referință privind amenințarea hibridă în RM”* și evaluării *„Modele de influență hibridă în contextul vulnerabilităților interne”*, având în vedere viziunile autorităților naționale care fac parte din *Grupul de lucru interinstituțional pe domeniul Amenințărilor Hibride (AH)*.

La nivel instituțional, în baza priorităților formulate de către Directorul SIS, de către specialiștii în domeniul comunicării și relațiilor publice a fost elaborat și diseminat conducerii SIS *produsul informativ-analitic cu privire la transparentizarea activității Serviciului și managementului brandului instituțional (nr. 26/101 din 12.06.2022)*, care conține anexa sub denumirea: *Strategia de comunicare instituțională.* În acest sens, toate acțiunile planificate pentru implementare în anul 2022, au fost realizate integral.

Totodată, în anul 2022, SIS a realizat un set de activități în contextul dezvoltării comunicării strategice cu sectorul mass-media societatea civilă, după cum urmează:

- au fost elaborate propuneri în contextul Legii pentru modificarea unor acte legislative privind „securitatea informațională”;
- au fost înaintate propuneri pentru Dispoziția Comisiei Situații Excepționale (CSE) din luna februarie 2022, care prevăd atribuțiile SIS pe palierul combaterii știrilor false și distribuirea informațiilor ce promovează ura și războiul;
- a fost elaborat studiul analitic „Semiotica militară în contextul invaziei în Ucraina” (studiul a inclus caracteristica propagandei pe teritoriul RM. Specificul propagandei simbolurilor pro-război, concluzii și evaluări destinate beneficiarilor legali în eventualitatea examinării oportunității interzicerii acestora pe teritoriul RM);
- experții SIS au participat la dezbaterea publică organizată de TRM- Radio Moldova Tineret la subiectul combaterea știrilor false;
- a fost elaborat Ordinul directorului SIS în vederea executării prevederilor Dispoziției CSE, în scopul eficientizării procesului identificare și publicare a surselor cu conținut online care promovează informații false în domeniul energetic, ce afectează securitatea națională în perioada stării de urgență;
- au fost elaborate propuneri privind necesitatea modificării Hotărârii Guvernului nr. 359/1995 cu privire la acreditarea jurnaliștilor străini în Republica Moldova;
- a fost elaborat și remis în adresa beneficiarilor studiul cu tematica: „Protecția spațiului informațional, inclusiv în contextul stării de urgență. Lupta cu propaganda și dezinformarea. Atribuțiile SIS”.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul II **Asigurarea securității spațiului informațional-mediatic**			
12/2	Dezvoltarea unor politici de comunicare strategică pe plan intern și racordarea la platformele de comunicare strategică externe ale structurilor sistemului de securitate, apărare și ordine publică pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Consiliul Audiovizualului*.

Consiliul Audiovizualului are atribuții de monitorizare a spațiului audiovizual național, conform art. 17 din Codul serviciilor media audiovizuale nr. 174/2018 și nu deține sferă de competență extrainstituțională. Astfel, Consiliul Audiovizualului urmează a fi exclus ca instituție responsabilă de respectiva acțiune.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
12/3	Crearea, în RM, a resursei/ platformei informaționale de comunicare strategică care va conține informații privind: a) incidentele de securitate informațională; b) ghidurile de comunicare strategică pe subiecte de interes național; c) tentativele și acțiunile de dezinformare și/ sau de informare manipulatorii ce afectează securitatea informațională și starea generală de securitate	Perioada 2021-2024, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituții responsabile*:* *Serviciul de Informaţii şi Securitate.*

În conformitate cu Hotărîrea Guvernului nr. 467/2022, a fost creat Consiliul coordonator pentru asigurarea securității informaționale (CCASI) (Monitorul Oficial nr.201-207/531 din 08.07.2022). Funcția de bază a CCASI este promovarea și coordonarea măsurilor de punere în aplicare a politicilor de securitate informațională și cibernetică într-o societate democratică în funcție de dezvoltarea tehnologiei, raporturilor juridice și de altă natură din sectorul informațional, atât la nivel național, cât și internațional. SIS în cadrul CCASI este reprezentat de către Directorul adjunct și este desemnat/ implicat în activități pe palierul operațional. De menționat că platforma informațională de comunicare strategică privind incidentele de securitate informațională, tentativele și acțiunile de dezinformare și/ sau de informare manipulatorii ce afectează securitatea informațională și starea generală de securitate, nu a fost creată, dat fiind faptul constituirii cu depășirea termenului a CCASI. Concomitent, pe parcursul anul 2022, membrii delegați ai CCASI s-au întrunit doar într-o singură ședință de lucru (18 noiembrie 2022), în cadrul căreia au abordat impedimentele implementării Strategiei Securității Informaționale a RM pentru anii 2019-2024.

Subsidiar, menționăm că tentativele și acțiunile de dezinformare și/ sau de informare manipulatorii ce afectează securitatea informațională și starea generală de securitate, urmează a fi abordate prin prisma unor consultări publice de către CCASI, pe palierul mediatic sau operațional.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
14/1	Evaluarea spațiului 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	Parțial realizat

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

În anul 2022, SIS a continuat monitorizarea resurselor mediatice online, în special în contextul declanșării războiului din Ucraina. Informațiile obținute au fost utilizate pentru elaborarea produselor informativ-analitice.

În general, în vizorul SIS s-au aflat resurse media din exteriorul și interiorul țării, care distribuiau pe teritoriul RM elemente de propagare a agresiunii militare asupra Ucrainei, având ca scop justificarea sau propagarea războiului. În perioada enunțată, de către SIS au fost remise 79 de sesizări către administrația rețelelor de divertisment și de socializare. SIS a sesizat de repetate ori factorii decidenți cu referire la sursele web, care au distribuit date tendențioase pentru examinarea oportunității de blocare/ redresare a situației. În final, au fost blocate 13 surse media online. Serviciul a sesizat instituțiile statului de resort în vederea necesității dezmințirii informațiilor în contextul apariției informațiilor false în spațiul public, pasibile de a provoca panică în societate.

Pe faptul răspândirii mesajelor ce incită la ură și propagă războiul, a fost informată Procuratura generală, care a pornit cauze penale în temeiul *art. art. 140 „Propaganda războiului”* și 346 *„Acțiunile intenționate îndreptate spre aţâţarea vrajbei, diferențierii sau dezbinării naționale, etnice, rasiale sau religioase”* din Codul penal.

În anul de referință, SIS a întocmit lista entităților cu conținut on-line, care promovau informații ce incitau la ură și război. Ulterior, lista enunțată a fost remisă Registratorului național al domeniului de nivel superior „.md” și furnizorilor de rețea și/ sau servicii de comunicații electronice, pentru blocarea accesului utilizatorilor din Republica Moldova la sursele cu conținutul on-line compromis.

În opinia SIS, este necesară ajustarea sancțiunilor administrative, contravenționale, dar și stabilirea altor norme legale, în vederea prevenirii și contracarării răspândirii și/sau utilizării în public a informației, care nu corespunde adevărului și aduce atingere drepturilor și intereselor persoanei și societății în general. La subiect, SIS a identificat o serie de articole/ materiale jurnalistice, ale unor entități on-line, care diseminau materiale sub formă de opinii ale unor „pseudo-experți” de proveniență externă, la baza fiind materialele difuzate de agenții de presă străine, care prin declarațiile oficialilor de stat justificau războiul și agresiunea militară. La solicitarea SIS, articole/materiale jurnalistice au fost eliminate de pe paginile electronice ale resurselor on-line din jurisdicția RM.

STISC a executat deciziile/ordinile Serviciului de Informații și Securitate cu privire la blocarea numelor de subdomenii din domeniul de nivel superior .md care promovează știri false, instigă la ură, război, la încălcarea ordinii publice sau la violență.

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	Parțial realizat

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

În anul 2022, SIS a participat la elaborarea unui set de propuneri legislative pe domeniul combaterii știrilor false și a materialelor extremiste. Proiectul cu propuneri a fost remis în adresa Aparatului Președintelui Republicii Moldova.

La fel, SIS a perfectat avizul la proiectul de Lege nr. 123/2022, care s-a finalizat cu adoptarea Legii nr. 143/2022 pentru modificarea Codului serviciilor media audiovizuale al Republicii Moldova nr.174/2018, ce ține de contracararea propagandei și dezinformării. De menționat că, după aprobarea de către Parlamentul RM în primă lectură a Proiectului de lege nr. 123, Comisia cultură, educație, cercetare tineret, sport și mass-media, în baza unor consultări publice desfășurate, a propus atribuirea unor competențe doar Consiliului audiovizualului, iar Serviciul de Informații și Securitate nu a primit competențe necesare pentru a combate știrile false și materialele extremiste. Astfel, legiuitorul practic a ignorat cerințele Strategiei securității informaționale și Planului de acțiuni, necesare pentru reglementare unei dimensiuni a spațiului mediatic. În aceste circumstanțe, SIS a înaintat propunerea de a dezbate subiectele în cauză în cadrul CCASI pe palierul operativ și mediatic în anul 2023.

Luând în considerare faptul că Consiliul Audiovizualului reglementează doar domeniul audiovizual – TV și Radio, și nu deține dreptul la inițiativă legislativă, acțiunea rămâne în sarcina Serviciului de Informații și Securitate și Ministerului Justiției. Totodată, Consiliul Audiovizualului urmează a fi exclus din lista instituțiilor responsabile de respectiva acțiune.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
14/3	Implementarea cadrului normativ care prevede acțiuni comune de intervenție și de gestionare a spațiului media on-line și off-line informațională și starea generală de securitate	Perioada 2021-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituții responsabile: *Autorităţile administraţiei publice; Societatea civilă.*

Potrivit experților ai SIS, actualmente este necesară inițierea elaborării unor acte legislative pentru înlăturarea lacunelor depistate și reglementarea spațiului mediatic on-line. În acest scop, este necesar ca rapoartele de evaluare pe palierul mediatic și extremist, întocmite de către SIS în perioada anilor 2019-2021, cu privire la implementarea Strategiei Securității Informaționale a RM pentru anii 2019-2024, să fie remise în adresa CCASI *(către membrii ce activează pe palierul mediatic).*

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
15/1	Elaborarea, sub egida Consiliului coordonator pentru asigurarea securității informaționale, a criteriilor de calificare a informației ca produs de dezinformare, de manipulare sau de propagandă, orientat spre subminarea securității informaționale, în scopul identificării comanditarilor, a surselor de finanțare și a executorilor	Perioada 2021-2024, 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.*

Măsura urmează a fi implementată după realizarea unor discuții/ dezbateri la subiect de către membrii CCASI.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
15/2	Ajustarea cadrului legal în vederea eficientizării colectării de date pentru identificarea provenienţei mijloacelor financiare şi a proprietăţii ale subiecţilor implicaţi în activităţi de dezinformare, manipulare şi propagandă ce subminează securitatea informaţională	Perioada 2019-2024, cu verificarea anuală a indicatorilor de progres	Parțial realizat

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

În anul 2022, SIS a elaborat propuneri pentru Proiectul de lege privind contracararea fenomenului de răspândire a dezinformării, în contextul războiului din Ucraina.

Continuarea măsurilor de implementare a Strategiei securității informaționale a Republicii Moldova pentru anii 2022–2024, urmează a fi realizată prin prisma întrunirii în cadrul ședințelor de lucru a CCASI și demararea consultărilor publice privind modificarea unor acte normative tangențiale securității informaționale, precum și de atenuare a riscurilor de competența SIS.

Pe data de 18 noiembrie 2022 au intrat în vigoare noile modificări la Codul serviciilor media audiovizuale nr. 174/2018, aprobate de Parlamentul Republicii Moldova prin Legea nr. 303 din 03 noiembrie 2022 (Monitorul Oficial nr. 363-373 din 18 noiembrie 2022). Amendamentele pot fi accesate și consultate pe următorul link: https://www.legis.md/cautare/getResults?doc_id=134139&lang=ro#.

Astfel, au fost introduse prevederi noi privind raportarea anuală de furnizorii și distribuitorii de servicii media către CA legat de beneficiarii finali și acționari, sursele de finanțare, dar și asigurarea transparenței acestor informații față de public. Astfel, a fost realizat un punct prevăzut în Planul de acțiuni pentru implementarea măsurilor propuse de Comisia Europeană în Avizul său privind cererea de aderare a Republicii Moldova la Uniunea Europeană, aprobat de Comisia Națională pentru Integrare Europeană pe 04 august 2022. În acest sens, CA a elaborat și aprobat formulare noi ale rapoartelor anuale ale furnizorilor și

distribuitorilor, menite să sporească gradul de transparență a proprietății și a surselor de finanțare.

Totodată, în contextul eforturilor de apropiere de standardele europene vizând transparența proprietății media, Republica Moldova, prin intermediul Consiliului Audiovizualului, a devenit parte a Mecanismului european de raportare a informațiilor privind acționarii și proprietarii beneficiari ai furnizorilor de servicii media de televiziune. Astfel lunar, CA oferă informații necesare pentru completarea și actualizarea bazei de date MAVISE, gestionată de Observatorul european al audiovizualului.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
15/3	Interacţiunea cu instituţiile de drept în ceea ce priveşte analiza riscurilor şi a ameninţărilor din domeniul mass-mediei, cu scopul de a monitoriza evoluţia ameninţărilor depistate, de a investiga activitatea subversivă sau penală în spaţiul informaţional şi de a stabili sursele de finanţare a factorilor de risc	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	În proces de realizare

Instituția responsabilă: *Serviciul de Informaţii şi Securitate.*

În perioada de referință nu a fost implementat mecanismul de interacțiune cu instituțiile de drept, în ceea ce privește analiza riscurilor și a amenințărilor din domeniul mass-media. Acțiunea nu a fost executată dat fiind faptul neexecutări acțiunilor 15.1 și 15.2.

Conform atribuțiilor prevăzute în regulamentul PG aprobat prin Ordinul Procurorului General nr.33/3 din 03.05.2022, cu modificările ulterioare, Procuratura Generală monitorizează spațiul informațional în scopul identificării, reacționării prompte la semnale, eventualei intervenții instituționale și prevenirii unor abateri de la lege.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
16/1	Crearea, la nivel naţional, a entităţii cu competenţe de promovare şi coordonare a politicilor de securitate informaţională într-o societate democratică în funcţie de dezvoltarea tehnologiei, raporturile juridice şi de altă natură din sectorul societăţii informaţionale la nivel naţional şi internaţional (Consiliul coordonator pentru asigurarea securităţii informaţionale): a) identificarea şi integrarea componentelor existente cu funcţii şi atribuţii în domeniul cibernetic şi mediatic, a autorităţilor administraţiei publice locale, precum şi a componentelor care vor fi create pe parcurs; b) determinarea liniei de activitate pentru fiecare componentă inclusă în cadrul Consiliului coordonator pentru asigurarea securităţii informaţionale, în funcţie de atribuţiile şi funcţiile deţinute din perspectiva asigurării securităţii informaţionale; c) elaborarea şi adoptarea cadrului normativ de interacţiune pentru realizarea sarcinilor de depistare, prevenire şi contracarare a riscurilor şi ameninţărilor la adresa securităţii informaţionale	Anul 2019	Realizat

Instituţia responsabilă: *Serviciul de Informaţii şi Securitate*.

Pe data de 06 iulie 2022 Guvernul Republicii Moldova a aprobat Hotărârea de Guvern nr. 467 „Cu privire la crearea Consiliului coordonator pentru asigurarea

securităţii informaţionale”, care a fost publicată în Monitorul Oficial nr. 201-207 din 08.07.2022.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

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 informații clasificate, precum și să participe la discuțiile de lansare a pregătirilor pentru trecerea la schimbul de informații clasificate în format digital.

De asemenea a fost lansat dialogul cu Centrul satelitar al UE (SatCen). Astfel, începând cu sfârșitul lunii mai 2022, au fost stabilite împreună cu SEAE aranjamentele de lucru în baza acordului SIA pentru partajarea produselor SatCen UE pe suport de hârtie, iar începând cu luna decembrie, MAEIE a început să recepționeze și rapoarte în format digital, în special ce țin de infrastructura critică civilă.

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	Parţial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

SIS a informat și atenționat autoritățile publice prin intermediul site-ului oficial „sis.md” și paginii de „Facebook” a instituției privind intensificarea atacurilor de tip phishing, fiind menționate metodele de identificare a acestora și soluții de protecție.

Totodată, SIS a publicat pe pagina web și Facebook ale instituției ghiduri de identificare a știrilor false în vederea promovării consumului calitativ de către societate a informațiilor publice.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

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

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de referință nu au fost înregistrate progrese la acțiunea respectivă.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
17/3	Elaborarea unor protocoale operaţionale de interacţiune între autorităţile responsabile şi factorii de decizie în cazul unor ameninţări 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 2022 nu au fost înregistrate progrese la acțiunea respectivă.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În anul 2022 SIS a întreprins măsuri pentru dezvoltarea capacităților de reacție în cazul unor amenințări hibride, după cum urmează:

- la 14.01.2022 a fost elaborată scrisoarea adresată MAEIE, AGE, MA, MIDR, prin care au fost solicitate viziunile instituționale privind proiectele/ inițiativele: „Cadrul interinstituțional de referință privind amenințarea hibridă în Republica Moldova” și „Modele de influență hibridă în contextul vulnerabilităților interne”;
- la 20.04.2022 a fost elaborată scrisoarea adresată MAEIE privind organizarea unei ședințe a grupului de lucru în domeniul Amenințărilor Hibride (la nivel de experți) pentru punerea în discuție a propunerilor și obiecțiilor autorităților naționale pe marginea proiectelor documentelor menționate; aprobarea unei versiuni finale agreate a proiectelor: „Cadrul interinstituțional de referință privind amenințarea hibridă în Republica Moldova” și „Modele de influență hibridă în contextul vulnerabilităților interne”; aspecte ce țin de elaborarea „Protocolului operațional de interacțiune între autoritățile responsabile și factorii de decizie în cazul unor amenințări hibride” (structura, instituția responsabilă de coordonarea rețelei naționale în combaterea amenințărilor hibride, mecanismul nemijlocit de interacțiune și sarcinile fiecărui component);

- la 29.06.2022 a fost elaborată scrisoarea adresată MAEIE prin care anexat a fost remisă versiunea în limba engleză a proiectului „Cadrul interinstituțional de referință privind amenințarea hibridă în RM”, în scopul expertizării de către specialiștii European Union Intelligence and Situation Centre (EU INTCEN).

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.*

În perioada de referință nu au fost înregistrate progrese la acțiunea respectivă.

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.*

În perioada de referință, un obiectiv important promovat de MAEIE a constituit dezvoltarea cooperării cu NATO în domeniul comunicării strategice cu scopul consolidării capacităților de comunicare strategică la nivel național. Acest obiectiv este inclus în Planul Individual de Acțiuni al Parteneriatului Republica Moldova-NATO (IPAP) pentru anii 2022-2023 (aprobat prin HG nr. 26/2022 în ianuarie 2022), precum și în noul pachet de asistență reflectat în documentul „Tailored support to the Republic of Moldova”, aprobat de statele NATO la Summit-ul din iunie 2022, de la Madrid.

Astfel, autoritățile naționale își propun să dezvolte cooperarea cu NATO și să exploreze mecanismele existente în vederea îmbunătățirii capacităților de comunicare strategică la nivel național. Parte a acestui proces, va fi avansarea în continuare a interacțiunii cu Centrul de excelență NATO pentru comunicare strategică de la Riga.

În octombrie 2022, a fost organizată o reuniune a experților RM și NATO în domeniul comunicării strategice, unde au fost discutate situația actuală și dezvoltarea cooperării în acest domeniu. NATO urmează să elaboreze un raport cu posibilități de dezvoltare a colaborării.

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 2022 MA a întreprins următoarele acțiuni:
- s-a lucrat asupra dezvoltării capabilităților de apărare cibernetică și identificării potențialelor cooperări pe domeniu atât din țară cât și peste hotare;
- s-a elaborat Planul de acțiuni privind ameliorarea situației în domeniul apărării cibernetice a Sistemului de comunicații și informatică al AN (SCIAN);
- s-a coordonat cu președinția Republicii Moldova inițierea procesului de aderare la platforma „Federated Mission Networking".

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	Parțial realizat

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

În anul 2022, MA a desfășurat următoarele activități de competență:
- în perioada 31.01-11.02.2022 a fost desfășurat cursul de specializare în domeniul comunicații și informatică Managementul securității cibernetice cu implicarea a 8 militari;
- în perioada 30.05 – 03.06.2022, în orașul Tallinn, Estonia s-a desfășurat a 14-a conferință internațională destinată discuțiilor asupra conflictului cyber – CyCon 2022;
- participarea la workshop-ul cu tema: Abordarea problemelor diminuare și combatere a amenințărilor de natură cibernetică organizat on-line de IP STISC și compania FORTINET în perioadele:
a) 18-19.05.2022 - 2 militari;
b) 24-25.05.2022 - 2 militari;
c) 31.05-01.06.2022 - 2 militari;
- participarea la curs pentru lideri de conștientizare a securității cibernetice desfășurat on-line de Centru european Gh. C. Marshall în perioada 02-06.05.2022 cu implicarea a 1 militar;
- participarea la Atelierul de lucru pe domeniul securității cibernetice cu genericul: „Sporirea securității cibernetice a instituțiilor Republicii Moldova" pe data de 22.06.2022 cu implicarea a 5 militari;
- pe data de 30.06.2022 a fost desfășurată întrevederea cu echipa de experți britanici și reprezentanții CRIC (BCAC) pe domeniul securității informaționale cu implicarea a 6 militari;
- participarea contingentului Armatei Naționale la exercițiul multinațional CISEX „Cetatea – 2022" în perioada 05-23.09.2022, România cu implicarea a 12 militari;
- întâlnirea de lucru privind cooperarea sistemelor de comunicații și informatică statice organizată în perioada 26 – 30 septembrie 2022, în or. București, România;
- conferința inițială de planificare a exercițiului "CWIX23 - Coalition Warrior Interoperability Exercise";
- participarea la atelierul de securitate cibernetică desfășurat în perioada 06-10.11 în or. București, România cu implicarea a 3 militari;

- Cyber Security workshop în perioada 07 – 11.11.2022, în București, România cu prezentarea și simularea tehnicilor și tacticilor pe timpul unui incident cibernetic;
- în perioada 14-18.11.2022 a fost desfășurat atelierul de lucru cu experții proiectului Uniunii Europene - Echipele de răspuns rapid și asistența reciprocă în securitate cibernetică (Cyber Rapid Response Teams) CRRT cu implicarea a 12 militari;
- participarea la atelierul de lucru cu experții în securitate cibernetică ai gărzii naționale din Carolina de Nord „Cyber Security Roadmap" în perioada 05-09.12.2022 cu implicare a 11 militari.

În anul 2022, 3 ofițeri ai SIS au participat la 2 evenimente internaționale pe domeniul apărării cibernetice.

Totodată, 3 ofițeri ai SIS au participat la ședința de lucru cu partenerii externi pe dimensiunea implementarea Inițiativei DCBI (Defence Capacity Building Initiative). În cadrul consultărilor, au fost discutate aspecte ce țin de consolidarea potențialului de apărare cibernetică a instituțiilor statului, acordarea asistenței prin dispunerea de expertize și dotarea cu echipamente, lansarea Programului de dezvoltare profesională în cadrul centrelor acreditate ale partenerilor externi.

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	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

SIS și MA au stabilit mecanismul de cooperare/ înștiințare comună pe dimensiunea de apărare cibernetică privind anticiparea și contracararea atacurilor cibernetice asupra infrastructurilor Forțelor Armate. Actualmente, se implementează un instrument de schimb de informații privind amenințările cibernetice.

În anul 2022, de către SIS au fost identificate riscuri de securitate privind intențiile unor companii private și persoane neautorizate de a obține acces la sistemele informaționale ale Ministerului Afacerilor Externe și Integrării Europene.

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.*

Ministerul Justiției a propus amendarea cadrului normativ în scopul de contracarare a dezinformării, inclusiv definirea și uniformizarea unor noțiuni. În acest sens, pentru a asigura o contracarare promptă a acestui fenomen mediatic, pe platforma parlamentară au fost demarate mai multe modificări ale cadrului normativ. Astfel, prin Legea nr. 143/2022 a fost modificat Codul serviciilor media audiovizuale al RM nr. 174/2018. În scopul protejării spațiului audiovizual național și a asigurării securității informaționale au fost introduse noțiuni și prevederi noi ce țin de „dezinformare, propagandă a agresiunii militare, conținut extremist" ș.a. Astfel, articolul 1 a fost completat cu o nouă noțiune juridică – „dezinformare", iar alin. (3) și (4) ale art. 17, care se referă la protejarea spațiului audiovizual național, au fost completate/reformulate. În virtutea faptului că a fost introdusă o nouă definiție a dezinformării, s-a impus necesitatea completării unor articole cu sancțiuni ce vizează acțiuni de dezinformare. Un șir de sancțiuni sunt prevăzute pentru nerespectarea art. 17: amenzi de la 40000 de lei la 70000 de lei Pentru încălcarea repetată, amenda constituie de la 70000 de lei la 100000 de lei, precum și retragerea licenței de emisie.

La fel, prin Legea nr. 102/2022 pentru modificarea unor acte normative a fost modificat Codul contravențional al Republicii Moldova nr.2018/2008. Respectiv, cadrul normativ prenotat a fost completat cu art. 365^5 care prevede sancțiuni care se aplică în cazul încălcării drepturilor cetățenilor prin răspândirea atributelor și simbolurilor general cunoscute ce sunt utilizate în contextul unor acțiuni de agresiune militară, crime de război sau crime împotriva umanității, precum și al propagandei sau glorificării acestor acțiuni.

Respectiv, odată cu instituirea stării de urgență pe teritoriul Republicii Moldova de către Parlamentul Republicii Moldova (24 februarie 2022), în legătură cu escaladarea războiului din Ucraina și întru securizarea spațiului audiovizual național și protejarea consumatorilor de programe de știrile false și propagandistice, CA a desfășurat o serie de controale tematice a programelor audiovizuale de știri și de dezbateri, de informare în probleme de interes public, inclusiv cele achiziționate/retransmise. Astfel, un grup de posturi de televiziune nu au asigurat informarea corectă, încălcând principiile bunei-credințe, imparțialității, echilibrului de opinii, separării faptelor de opinii. În mod particular, acestea au prezentat într-o lumină extrem de negativă statul ucrainean, respectiv – în lumină pozitivă conducerea rusă, iar o parte din ele au omis din buletine de știri despre mersul războiului. Drept urmare, în legătură cu reflectarea agresiunii armate a Federației Ruse împotriva Ucrainei, CA a aplicat 55 de sancțiuni, suma totală a amenzilor fiind de 213000 de lei.

Consiliul Audiovizualului a mai inițiat, din oficiu, controlul privind corectitudinea cu care au fost reflectate tema refugiaților, decizia de interzicere a simbolurilor ce ilustrează și justifică agresiunea militară, precum și o serie de alte evenimente de însemnătate social-politică.

În anul 2022, SIS a mediatizat mai multe măsuri executorii efectuate pentru înlăturarea cauzelor și condițiilor ce contribuie la realizarea amenințărilor securității de stat, capabile să afecteze securitatea informațională a Republicii

Moldova. Printre acestea se includ măsurile de identificare și blocare a 13 surse cu conținut online compromis, care promovează știri false cu privire la războiul din Ucraina.

În acest context, SIS a îndemnat publicul să raporteze știrile false prin intermediul unui formular online, cu scopul de a sensibiliza și implica societatea în procesul de prevenire și combatere a dezinformării. De asemenea, SIS a atenționat publicul prin intermediul site-ului oficial despre instituirea nivelului moderat de alertă teroristă și pericolul proliferării simbolurilor tendențioase.

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 Informaţii şi Securitate.*

Conform specialiștilor SIS, este necesară elaborarea unor acte legislative pentru eliminarea disfuncțiilor stabilite și reglementarea spațiului mediatic on-line. În acest sens, se consideră judicioasă expedierea în adresa Consiliului coordonator pentru asigurarea securității informaționale (CCASI) a rapoartelor de evaluare pe palierul mediatic și extremist, întocmite de către SIS în perioada anilor 2019-2021.

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 Informaţii şi Securitate.*

În perioada de referință, SIS a elaborat Proiectul de lege pentru combaterea știrilor false și materialelor extremiste, în cadrul căruia au fost stipulate reglementări și filtre de depistare și/ sau de blocare a unor produse informaționale și/ sau resurse informaționale ce conțin elemente de risc la adresa securității naționale.

Odată cu instituirea la 24.02.2022 a Stării de Urgență prin punctele 26-28 din Dispoziția nr. 1 a CSE, propuse de către SIS, s-au stabilit filtre de depistare și/ sau de blocare a unor produse informaționale și/ sau resurse informaționale ce conțin elemente de risc la adresa securității naționale.

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 Informaţii şi Securitate*

În anul de referință, Centrul Antiterorist al SIS a elaborat și înaintat propunerea de completare a Codului Contravențional, inițiativa legislativă fiind votată de Parlament (Legea 102/2022, MO nr.115-117 din 20.04.2022) – proiectul de completare cu art. 3654 „Încălcarea legislației în domeniul protecției antiteroriste", care prevede sancțiuni cu amendă pentru încălcarea prevederilor Regulamentului privind protecția antiteroristă a infrastructurii critice, aprobat prin HG nr. 701/2018, precum și pentru neexecutarea prescripțiilor obligatorii emise în conformitate cu Regulamentul privind organizarea și desfășurarea testelor antiteroriste, aprobat prin HG nr. 996/2018. La fel, în anul de referință, a fost revizuit și actualizat Capitolul IV Securitatea Cibernetică din Pașaportul antiterorist pentru infrastructura critică – anexă la OD SIS al RM nr. 50/2018.

La 26 octombrie 2022, prin HG nr. 737 a fost aprobat proiectul cu numărul unic 130/SIS/2022 Cu privire la aprobarea Programului național de consolidare și realizare a măsurilor de protecție antiteroristă a obiectivelor infrastructurii critice naționale pentru anii 2022-2026 și a Planului de acțiuni privind implementarea acestuia (Publicat în Monitorul Oficial nr.363-373 din 18.11.2022). Proiectele enunțate, au drept scop eficientizarea măsurilor de siguranță și securitate pe palierul de infrastructură critică.

Complementar, a fost asigurată participarea și reprezentarea SIS la 9 ședințe ale Grupului de lucru pentru implementarea Sistemului de Informații prealabile despre pasageri în RM. Actualmente, proiectul este în desfășurare și va fi implementat cu suportul ONU, fiind inițiate instruiri pentru certificarea specialiștilor și adaptarea cadrului normativ național. Totodată, experții SIS au participat în cadrul grupurilor de lucru și ședințelor comune cu autoritățile competente la elaborarea și definitivarea proiectului Legii privind securitatea cibernetică, care specifică inclusiv desemnarea și funcționarea CERT-ului național și cerințe de securitate pentru infrastructurile critice.

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	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În contextul înrăutățirii situației de securitate la nivel regional, a fost aprobat și publicat Ordinul Directorului SIS cu privire la stabilirea nivelului moderat de alertă teroristă (cod galben) – nr. 11 din 24.02.2022.

Prin intermediul paginii oficiale a Centrului Antiterorist, pe data de 22.04.2022 au fost informați operatorii infrastructurilor critice despre Notificarea în legătură cu unele riscuri de securitate cibernetică.

Pe parcursul anului 2022, Centrul Antiterorist al SIS a desfășurat 2 teste antiteroriste pe subiecte de securitate cibernetică în infrastructura critică națională cu informarea beneficiarilor legali. La fel, în anul 2022, SIS a participat la verificarea

nivelului de realizare a protecției antiteroriste pe domeniul TIC a infrastructurii critice din cadrul Î.S. Moldelectrica „TermoElectrica”.

La mijlocul lunii septembrie 2022, MAEIE a recepționat Chestionarul privind Amenințările Hibride (EU Hybrid Risk Survey), un document cuprinzător, care abordează riscurile și vulnerabilitățile ce țin de domeniul hibrid, conținând inclusiv întrebări privind securitatea energetică și pașii pentru protejarea infrastructurii critice, dar și încercările actorilor terți de a diminua coeziunea socială și a disemina dezinformare în rândul populației. Completarea acestui document permite crearea unui tablou cuprinzător, în baza căruia se vor identifica lacunele existente, precum și pașii necesari pentru eliminarea/reducerea riscurilor existente.

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

Instituția responsabilă: *Serviciul de Informaţii şi Securitate.*

Prin Ordinul Directorului SIS nr. 9/2022 a fost aprobat Planul național de reglementare a situațiilor excepționale legate de actele de intervenție ilicită. Documentul a fost înregistrat la Ministerul Justiției cu nr. 1704 din 23 martie 2022 și publicat în MO nr. 106-114, art. 437.

Prin redactarea Capitolului IV Securitatea Cibernetică din Ordinul Directorului SIS nr. 27/2022 a fost revizuit, modificat și publicat în Monitorul Oficial modelul Pașaportului Antiterorist.

În scopul eficientizării mecanismelor de reacție și răspuns în cazul alertelor false cu bombă, Centrul Antiterorist al SIS de comun cu MAI a elaborat și aprobat Ordinul comun (MAI nr.526, PG nr.81, SIS nr.60, SPPS nr.180, SNUPAU 112 nr. 01/10-193) Cu privire la aprobarea acțiunilor comune de reacție și răspuns în cazul amenințării sau pericolului de producere a unei explozii, depistării unor obiecte suspecte ca exploziv, muniții, care a intrat în vigoare la data de 31.10.2022.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
22/1	Evaluarea nivelului actual de pregătire a resurselor umane în domeniul securităţii informaţionale, pe fiecare compartiment în parte: mass-media, tehnologia informaţională, apărare, ordine publică şi contrainformaţii	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	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 anul 2022, cadrul didactic al SIS a elaborat Modulul de formare profesională (structurat în volum de 8 ore academice), destinat pregătirii

profesionale pe dimensiunea securității informaționale, cum ar fi: igiena cibernetică, amenințările cibernetice, utilizarea surselor deschise de informații, protecția sistemelor informaționale departamentale. În baza modulului enunțat au fost instruiți 60 de ofițeri ai SIS. Subsidiar, a fost elaborat și un Chestionar pe dimensiunea igienei cibernetice, structurat în 20 de teste.

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*

La data de 14 mai 2022 de către Institutul Național de Informații și Securitate al SIS a fost organizată Conferința științifică cu tematica: Securitatea națională a Republicii Moldova: provocări și tendințe. În cadrul conferinței formatorii INIS a prezentat 3 materiale analitice pe dimensiunea 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 anul 2022, Academia Militară a Forțelor Armate „Alexandu cel Bun”, a elaborat programul Servicii ale securității (Probleme actuale ale securității naționale) 600 ore/ 20 credite, aprobat prin Ordinul nr. 770 din 73.07.2022 – 5 ani acreditare.

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	Parțial realizat

Instituția responsabilă: *Autorităţile administraţiei publice*

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 2022, Institutul Național de Informații și Securitate a organizat două cursuri de instruire, destinate funcționarilor publici, inclusiv cu statut special.

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 și organizaţiile internaţionale ce își desfășoară activitatea în domeniul asigurării securităţii informaţionale și elaborarea unor acţiuni privind intensificarea cooperării respective	Perioada 2020-2021, cu verificarea anuală a indicatorilor de progres	Realizat

Instituția responsabilă: *Autorităţile administraţiei publice*

În perioada de referință nu au fost înregistrate progrese la acțiunea respectivă.

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*

Dezvoltarea cooperării RM-NATO în domeniul securității informaționale și cibernetice a fost inclusă ca obiectiv al Planului Individual de Acțiuni al Parteneriatului (IPAP) RM-NATO pentru anii 2022-2023, aprobat prin HG nr. 26/2022 în ianuarie 2022. MAEIE a insistat asupra promovării acestui obiectiv în parteneriatul bilateral, subiectul fiind abordat în cadrul întrevederilor la cel mai înalt nivel a conducerii RM cu conducerea NATO și reuniunilor în formatul 30 aliați + RM. În perioada 6-7 iunie 2022, a fost organizată vizita în RM a Secretarului General adjunct NATO pentru informații și securitate David Cattler, au avut loc întrevederi cu conducerea SIS, MAp, MAEIE în cadrul cărora a fost discutată cooperarea bilaterală.

Urmare a demersurilor efectuate, obiectivul dezvoltării cooperării RM-NATO în domeniul securității informaționale și cibernetice a fost inclus în noul pachet de asistență reflectat în documentul „Tailored support to the Republic of Moldova", aprobat de statele NATO la summit-ul din iunie 2022, de la Madrid.

De asemenea, MAEIE a insistat asupra obținerii asistenței NATO pentru sporirea rezilienței și nivelului de pregătire pentru situații de urgență civilă. În iulie 2022, NATO a creat o echipă de experți Resilience Advisory Support Team (RAST), care să dezvolte cooperarea cu țara noastră. Au avut loc reuniuni la nivel de experți pentru dezvoltarea cooperării în domeniul securității cibernetice și securizării rețelelor civile de comunicații și informatice.

În octombrie 2022, la Chișinău a fost organizată o reuniune a experților RM și NATO în domeniul apărării cibernetice unde a fost discutată cooperarea de mai departe.

În perioada de referință, instituțiile naționale au beneficiat de instruiri în cadrul centrelor specializate acreditate de NATO, precum și prin programe bilaterale, în cadrul Meniului de Cooperare cu Partenerii (PCM).

Contracararea amenințărilor hibride, precum și asigurarea securității cibernetice au constituit subiecte discutate cu UE în cadrul primei reuniuni a Dialogului la nivel înalt în domeniul politic și de securitate (18.03.2022), vizitei interinstituționale din RM la Centrul de Situații și de Analiză a informațiilor al UE (INTCEN) și stabilirea contactelor instituționale cu reprezentanții Hybrid Fusion Cell (31.05.2022), precum și în cadrul celei de-a 6-a reuniune a consultărilor în domeniul securității și apărării dintre RM și UE (22.11.2022).

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*

În perioada de referință nu au fost înregistrate progrese la acțiunea respectivă.

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.*

MA lucrează actualmente asupra dezvoltării capabilităților de apărare cibernetică şi identificării potențialelor cooperări pe domeniu atât din ţară cât şi peste hotare, fiind în proces de elaborare a planului de implementare a capabilităților de apărare cibernetică ale MA. La fel, 3 militari ai MA au participat pe data de 23.03.2022 la webinarul Stop incidente cibernetice desfășurat on-line de compania „Orange” în calitate de Top Integrator de soluții și servicii de securitate avansate.

În anul 2022, reprezentanții SIS au participat la ședințele de lucru organizate de către Ministerul Apărării, la care au fost abordate aspecte de cooperare în domeniul apărării cibernetice, schimbului de informații privind indicatorii de compromitere, etc.

În contextul implementării acțiunilor din cadrul proiectului „Moldova Cyber Security Rapid Assistance” în perioada 22.10.2022-29.10.2022 – reprezentanții STISC au efectuat vizite de studiu în Tallinn, Helsinki și Riga. Scopul acestora a fost realizarea schimbului de experiență, prin studierea modelelor estonian, leton și finlandez de transformare digitală a societății, cadrul normativ-legislativ aferent domeniului, particularitățile parteneriatului public-privat, dar și definirea rolurilor și atribuțiilor corespunzătoare entităților implicate în proces.

De asemenea, STISC în comun cu AGE, UTM și Proiectul Tehnologiile Viitorului finanțat de Agenția Statelor Unite pentru Dezvoltare Internațională și Guvernul Suediei, au semnat un acord de parteneriat pentru crearea Academiei de Securitate Cibernetică, ce are drept obiectiv consolidarea securității informaționale a statului. Totodată, la data de 23 noiembrie 2022 STISC și Directoratul Național de Securitate Cibernetică (DNSC) din România au semnat, un acord de cooperare în domeniul securității cibernetice pentru a facilita schimbul de informații referitoare la incidente sau evenimente de securitate cibernetică, dar și să realizeze schimb de bune practici în acest sens.

Reprezentanții PG au participat la următoarele evenimente:

- Cea de-a doua sesiune a Comitetului Ad-Hoc al ONU pentru crimă cibernetică, creat prin Rezoluția Adunării Generale a ONU nr. 74/247, Viena, 30.05-10.06.2022;
- Cea de-a 3-a Sesiune al Comitetului ONU Ad-hoc cu privire la criminalitatea cibernetică, 29.08.-09.09.2022;
- Cel de-al doilea Forum Regional de Cooperare a experților în domeniul criminalității și securității cibernetice, organizat în contextul proiectului comun UE/ Consiliul Europei CyberEast și CyberCecurity EAST, 23-24.06.2022;
- Reuniunea regională a grupului de experți pe tema: ”Abordarea traficului de persoane în vederea exploatării sexuale facilitate de tehnologie și cibernetică, inclusiv a copiilor din Europa de Sud-Est”, 05-06.07.2022;

Exercițiul de Cooperare Regională în domeniul criminalității cibernetice, Istanbul, Turcia, 13-16.09.2022;

De către Uniunea Europeană și Proiectul Consiliului Europei CyberEast, a fost organizată ședința celui de-al 6-lea Comitet Director al Proiectului și Întâlnirea Regională cu privire la Raportarea Cibernetică și Partajarea Datelor, ambele evenimente având ca scop concluzionarea asupra activităților desfășurate de statele membre ale Parteneriatului Estic, orientate spre asigurarea securității cibernetice, 12-14.12.2022.

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	Parțial realizat

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

Trei militari ai MA au participat la întrevederea cu atașatul militar din Olanda privind discuții despre securitate cibernetică și posibilitățile perspectivelor de cooperare pe data de 01.06.2022. La fel, cinci militari au participat pe data de 22.12.2022 la întrevederea cu Ambasadorul Estoniei, expertul estonian pe apărare cibernetică cu Secretarul de stat privind cooperarea în cadrul EPF pentru suportul Moldovei în domeniul securității cibernetice și prezentarea soluțiilor digitale.

În anul 2022, ofițerii SIS au participat la cinci ședințe de lucru în domeniul securității și apărării cibernetice. Totodată, ofițerii SIS au beneficiat de cursuri de instruire din partea partenerilor externi pe dimensiunea securității cibernetice.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
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 anul 2022 nu au fost înregistrate progrese la acțiunea respectivă.

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

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

Pe parcursul anului 2022 de către IGP nu au fost realizate activități cu EMAS (Europol Malware Analysis Solution) al EUROPOL, mecanismele de cooperare internațională cu structura menționată urmând a fi instituite în perioada următoare.

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	Parțial realizat

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

Pe parcursul anului 2022 de către IGP al MAI au fost examinate în Sistemul Informațional „Protecția Copiilor” pe c/p pornite peste 155 dispozitive de stocare a datelor, fiind depistate și excluse din circuit în rețeaua Internet peste 216 mii de imagini foto și 8 mii fișiere video cu conținut de pornografie infantilă. La fel, au fost examinate 1.007 fișiere cu imagini și video în baza de date ICSE a Interpol, pentru stabilirea apartenenței la categoria pornografiei infantile.

Reprezentanții PG participă 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 perioada de referință au fost dezvoltate instrumente și metode de identificare a victimelor, inclusiv prin utilizarea Sistemului informațional automatizat. În anul 2022 capacitățile dezvoltate au fost aplicate activ în practică. Astfel, au fost introduse și analizate în baza de date ICSE a OIPC Interpol – 1007 fișiere foto/video depistate în dispozitivele ridicate de la persoane (suspecți, martori etc), precum și analizate serii de imagini în scop de identificare a victimelor.

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

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, IGP al MAI asigură și recepționează solicitările privind asistențe imediate pentru investigațiile referitoare la infracțiunile informatice.

Pe parcursul anului 2022 au fost recepționate prin puncte de contact 24/7 pe Convenția privind criminalitatea informatică:

- cereri de conservarea datelor parvenite: 6 (3 US Departament , 1 Franța, 2 Cehia);
- solicitări recepționate: 2 (Ucraina);
- transmise răspunsuri: 2 (Ucraina);
- transmise solicitări: 2(Rusia, Ucraina);
- primite răspunsuri: 2(Rusia-1/1caracter de informare)-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:

• remise solicitări: 15 (3 Facebook, 4 webmoney, 3 Google, 1 Robinhood, 4 Binance)

• primite răspunsuri: 2 (2 Facebook, 3 Binance).

În anul 2022, Procuratura Generală, a examinat mai multe comisii rogatorii inclusiv 29 privind infracțiunile informatice sau legate de utilizarea de sisteme informaționale, care au parvenit de la autoritățile competente din: Austria, Belarus, Cehia, Coreea, Finlanda, Franța, Germania, Letonia, Marea Britanie, SUA, Polonia, România, Federația Rusă. În aceiași perioadă de către Procuratura Generală au fost inițiate 10 cereri de asistență juridică internațională în materie de criminalitate cibernetică, prin care a fost solicitată asistența autorităților din străinătate.

Prin intermediul punctului de contact 24/7 au fost examinate 31 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	Parțial realizat

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

În perioada de raportare, angajații IGP al MAI au participat în cadrul următoarelor evenimente:

- la data de 30.05.2022, un angajat al IGP a participat la ședința online realizată în cadrul unui proiect care prevede dezvoltarea soft-ului „Aviator” utilizat la prelucrarea rapoartelor NCMEC al SUA;
- la data de 07.07.2022, un angajat al IGP a participat la întâlnirea online privind utilizarea soft-ului „Aviator” pentru analiza rapoartelor NCMEC;

De asemenea, la solicitarea PG din 17.02.2022, IGP a furnizat informația privind cooperarea cu NCMEC, utilizarea bazei de date ICSE a OIPC Interpol și realizarea activităților de informare.

Ca rezultat a Generalizării anuale a infracțiunilor în domeniul informatic și de telecomunicații, prin care s-a stabilit 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 2022, au fost înaintate două cereri către ARBI pentru aplicarea sechestrelor a bunurilor provenite din infracțiuni transfrontaliere.

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

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

MAEIE – Reprezentanții instituțiilor naționale vizate (STISC, MAEIE, SIS) au participat în cadrul consultărilor în domeniul securității cibernetice cu UE "EU Cyber Consultations with the Eastern Partnership countries", care s-au desfășurat la Tbilisi (Georgia).

În perioada 5-7.10.2022, reprezentanții MAEIE, STISC, AGE, SIS au participat în cadrul Conferinței „Parteneriatul digital pentru securitatea cibernetică și reziliența în regiune", organizată la Telč (Republica Cehă).

Experții IT din MAEIE au participat în cadrul vizitei de studiu în Estonia, Finlanda și Letonia pentru preluarea bunelor practici în domeniul securității cibernetice, care a fost organizată în perioada 24-28.10.2022 sub umbrela proiectului UE - *Moldova Cybersecurity Rapid Assistance project.*

De asemenea, pe parcursul anului 2022, pe linia MAEIE, reprezentanții RM au participat următoarele la evenimente în domeniul securității cibernetice:

- Instruirea Cyber Diplomacy Training and Open Ended Working Group, 7- 9 noiembrie 2022, Viena, Austria: 1 participant din cadrul MAEIE;
- Conferința „Building societal resilience by raising public awareness of cyber threats and enhancing the role of cyber education", 20-21 octombrie 2022, Łódź, Polonia și format hibrid: 2 participanți din cadrul MAEIE;
- Seminarul National Cyber Incidents Classification, Banja Luka, Bosnia și Herțegovina, 22-23 septembrie 2022: 1 participant din cadrul Agenției de Guvernare Electronică și 1 participant din cadrul Serviciului de Informații și Securitate;

- Instruirea Sub-regional Trainings on the role of information and communication technologies (ICTs) in the context of regional and international security, 25 – 26 august 2022, Tirana, Albania: 1 participant din cadrul Agenției de Guvernare Electronică.

La fel, 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 Programe de combatere a criminalității informatice al CoE din București (C-PROC). Astfel, în decursul anului 2022 a fost facilitată participarea experților naționali la următoarele activități:

- International law enforcement training course on investigating ransomware attacks (online), 3-4 mai 2022: 1 pers MAI, 1 pers PG;
- Second Regional Cooperation Forum of cybercrime and cybersecurity experts – Cooperation Networks, București, 23-24 iunie 2022: 1 pers PG;
- Conferința „Underground Economy Conference", Strasbourg, 5-8 septembrie 2022: 1 MAI, 1 PG;
- International workshop on conducting criminal investigations in ransomware attacks, Haga, 3-4 noiembrie 2022: 1 MAI, 1 PG;
- Conferința Globală privind rolul femeilor în combaterea crimelor cibernetice, Costa Rica, 10-11 noiembrie 2022: 1 MAI, 1 PG;
- Cea de-a 2-a sesiune a Comitetului ad-hoc pentru elaborarea unei convenții internaționale cuprinzătoare privind combaterea utilizării tehnologiilor informaționale și comunicațiilor în scopuri penale, Viena, 30 mai-10 iunie 2022: 1 PG, 1 MAEIE;
- Cea de-a 3-a sesiune a Comitetului ad-hoc pentru elaborarea unei convenții internaționale cuprinzătoare privind combaterea utilizării tehnologiilor informaționale și comunicațiilor în scopuri penale, New York, 29 august-9 septembrie 2022: 1 PG, 1 MAEIE.

În perioada de referință angajații IGP al MAI au participat în cadrul a 20 de evenimente internaționale, după cum urmează:

- la 07.03.2022, 1 angajat al poliției a participat la cea de-a 9-a Reuniune a grupului de lucru Interpol privind criminalitatea financiară transnațională, care va servi concomitent drept ședința preoperațională a Operațiunii „First Light", organizată sub egida OIPC Interpol, în vederea combaterii fraudelor în domeniul telecomunicațiilor și ingineriei sociale;
- la 10.03.2022, 2 angajați ai poliției au participat la conferința online cu genericul „Europol Dark Web Conference", organizat sub auspiciul OEP Europol/SOC-AP Dark Web;
- în perioada 26-29.04.2022, 1 angajat al poliției a participat la Conferința internațională „The International;
- în perioada 04-09.09.2022, 1 angajat al poliției a participat la conferința „ Underground Economy Conference 2022", în Strasbourg, Franța;

- în perioada 09-14.05.2022, 1 angajat al poliției a participat la Cea de-a 26-a Reuniune plenară T-CY, deschiderea spre semnare a celui de-al doilea protocol adițional la Convenția privind criminalitatea cibernetică și Conferința internațională privind cooperarea și divulgarea probelor electronice în Franța, Strasbourg;
- la 31.05.2022, un angajat al poliției a participat la cea de-a 10-a Reuniune a Grupului de lucru INTERPOL privind criminalitatea financiară transnațională, și concomitent ședința de închidere a Operațiunii First Light 2022;
- în perioada 30.05-03.06.2022, 1 angajat al poliției a participat la cursul de formare „Investigarea crimelor informatice", organizat de către Academia Internațională a Organelor de drept (ILEA) din Budapesta, Ungaria;
- în perioada 13-16.06.2022, un angajat al poliției a participat la cursul de instruire în domeniul combaterii infracțiunilor comise prin intermediul platformelor de Streaming în or.Sofia, Bulgaria;
- în perioada 29.06-01.07.2022, un angajat al poliției a partipat la cursul de instruire în domeniul utilizării bazei de date internaționale a INTERPOL privind exploatarea sexuală a copiilor (ISCE), desfășurat la sediul OIPC Interpol or. Lyon, Franța;
- în perioada 28.06-02.07.2022, un angajat al poliției a participat la cursul de instruire în domeniul utilizării bazei de date internaționale a INTERPOL privind exploatarea sexuală a copiilor (ISCE), la sediul Organizației INTERPOL, Lyon, Franța;
- în perioada 04-07.07.2022, un angajat al poliției a participat la reuniunea regională a grupului de experți privind combaterea traficului de persoane inclusiv copii din Europa de Sud-Est în vederea exploatării sexuale, facilitat de tehnologii și cibernetică în Herceg Novi, Muntenegru;
- în perioada 08-11.08.2022, un angajat al poliției a participat la vizita de lucru în cadrul proiectului „ Consolidarea capacității Republicii Moldova de contracarare a abuzului și exploatării sexuale online", organizat de către CI „La Strada" în Dallas, Statele Unite ale Americii;
- în perioada 21-27.08.2022, 4 angajați ai poliției au participat la Cursul de formare cu genericul Investigarea crimelor informatice organizat de către Academia Internațională a Organelor de drept (ILEA) din Budapesta, Ungaria;
- în perioada 19-23.09.2022, 1 angajat al poliției a participat la cursul regional cu tema: „Atacurile cibernetice-Criptomonedele, frauda de plăți online, sistemul malware", care s-a desfășurat în Ungaria, Budapesta;
- în perioada 28-30.09.2022, un angajat al poliției a participat la evenimentul de reuniune a utilizatorilor soft-ului „Aviator", organizat în or. Amsterdam, Regatul Țărilor de Jos, sub egida organizației INHOPE;
- în perioada 03-07.10.2022, un angajat al poliției a efectuat o vizită de studiu „Ultimele amenințări cibernetice, tendințe și strategii de combatere a criminalității cibernetice" în Atena, Grecia;
- în perioada 18-22.10.2022, un angajat al poliției a participat la Conferința Europol privind criminalitatea cibernetică și Reuniunea anuală a punctelor de

contact 24/7, care a avut loc în orașul Haga (Olanda), eveniment organizata de către Consiliul Europei;
- în perioada 15-19.11.2022, 3 angajați ai poliției au efectuat o vizită de studiu la Lisabona, Republica Portugheză organizată cu suportul Asociației internaționale a liniilor telefonice de urgență referitoare la internet(INHOPE);
- în perioada 28.11-01.12.2022, un angajat al poliției a participat la Reuniunea plenară a Comitetului Convenției privind criminalitatea informatică în Strasbourg, Franța;
- în perioada 11-15.12.2022, un angajat al poliției a participat la reuniunea regională privind raportarea cibernetică și partajarea datelor, organizată în cadrul proiectului „CyberEast" sub egida Consiliului Europei în Tbilisi, Georgia.

Pe parcursul anului 2022, procurorii din Procuratura Generală, procuraturile specializate și teritoriale *(în total 20 de procurori)* au participat în scop de formare la următoarele evenimente internaționale:
- Forumul Regional de Cooperare a experților în domeniul criminalității și securității cibernetice – „Cazuri practice de utilizare pentru SOP-uri", organizat în contextul proiectului comun UE/CoE CyberEast și Cyber Security EAST, finanțat de Uniunea Europeană. 24 – 25 februarie 2022;
- Cea de-a 32-a Conferință a Grupului Consultativ al Procurorilor din Sud-Estul Europei (SEEPAG) cu tematicele „Aplicații criptate, ca instrumente pentru comiterea infracțiunilor" și „Criptomonede, dificultăți în investigarea și efectuarea urmăririi penale", organizată de Centrul Sud-Est European de Aplicare a Legii (SELEC) în contextul Președinției Bosniei și Herțegovinei la SEEPAG. 28 aprilie 2022;
- Cea de-a 26-a sesiune plenară a Comitetului Convenției privind criminalitatea informatică (T-CY), Deschiderea pentru semnare a celui de-al II-lea Protocol adițional la Convenția privind criminalitatea informatică și Conferința internațională privind fortificarea cooperării și divulgarea probelor electronice, organizate de Consiliul Europei. 10 – 13 mai 2022;
- Cursul de formare „Investigarea crimelor informatice", organizat de Academia Internațională a Organelor de Drept (ILEA) cu susținerea Departamentului de Justiție al SUA. 30 mai – 03 iunie 2022;
- Cea de-a doua sesiune a Comitetului Ad-Hoc al ONU pentru crimă cibernetică, creat prin Rezoluția Adunării Generale a ONU nr. 74/247. Viena, Austria 30 mai - 10 iunie 2022;
- Al doilea Forum Regional de Cooperare a experților în domeniul criminalității și securității cibernetice, organizat în contextul proiectului comun UE/ Consiliul Europei CyberEast și CyberCecurity EAST. 23-24 iunie 2022;
- Reuniunea regională a grupului de experți pe tema: „Abordarea traficului de persoane în vederea exploatării sexuale facilitate de tehnologie și cibernetică, inclusiv a copiilor din Europa de Sud-Est". 05-06 iulie 2022;
- Vizita de studiu a instituțiilor competente în cadrul proiectului „Consolidarea capacității Republicii Moldova de contracarare a abuzului și exploatării sexuale on-line" implementat de Centrul Internațional „La Strada" și finanțat de

Departamentul de Stat al SUA. 08-11 august 2022;
- Conferința „Economia Tenebră 2022”, co-organizată de către Oficiul Consiliului Europei de Programe Cibernetice (C-PROC) și Compania Team Cymru (SUA). 03-08.09.2022;
- Exercițiul de Cooperare Regională în domeniul criminalității cibernetice. Istanbul, Turcia, 13-16 septembrie 2022;
- Cursul regional „Atacuri cibernetice – Criptomonedele, frauda de plăți online și sistemul malware”. 19-23 septembrie 2022;
- Vizita de studiu în Estonia, Finlanda, Letonia cu subiectul „Administrarea securității cibernetice și rolul echipei de intervenția în caz de urgență informatică (CERT)”, organizată în cadrul Proiectului „Moldova Cybersecurity Rapid Assistance” implementat de Fundația Estoniană Academia e-Guvernare. 24-28.10.2022;
- Conferința internațională privind promovarea rolului femeilor în prevenirea și investigarea crimelor cibernetice, organizată de Consiliul Europei în cooperare cu Ministerul Public din Costa Rica. 10-11.11.2022;
- Atelierul internațional cu tema „Desfășurarea urmăririi penale în cazul atacurilor de tip ransomeware”, organizat în cadrul proiectului CyberEast în cooperare cu Eurojust. 03-04.11.2022;
- Cea de-a 27-a sesiune plenară a Comitetului Convenției privind criminalitatea informatică (T-CY), organizată de Consiliul Europei. 29-30.11. 2022
- „Artificial intelligence and law”, Scuola Superiore della Magistratura, Justice Programme of the European Union, 26-28.09.2022;
- SIRIUS Conference 2022: Cross-Border Access to Electronic Evidence - SIRIUS Team – Europol, 29-30.11.2022.

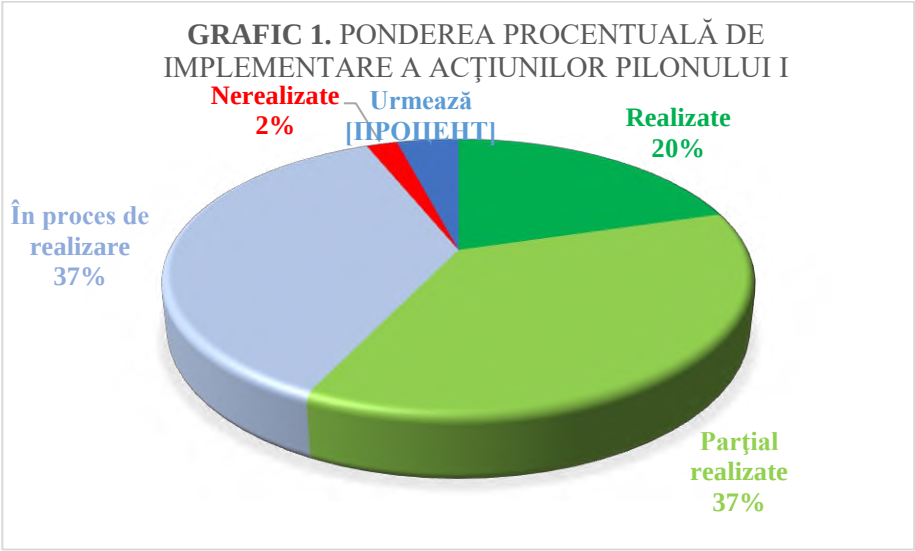
Participarea la evenimentele internaționale din domeniul prevenirii și combaterii criminalității informatice s-au dovedit a fi utile sub mai multe aspecte, în special pentru obiectivul de formare a personalului de specialitate, familiarizării acestuia cu mecanismele de cooperare internațională între autoritățile statului cu atribuții în combaterea criminalității informatice și asigurarea nivelului înalt de cooperare întru identificarea și combaterea în comun a noilor riscuri și provocări.

REFLECTAREA INDICATORILOR DE PROGRES CONFORM PRIORITĂŢILOR ŞI ACȚIUNILOR PLANIFICATE

Urmare evaluării rezultatelor de implementare a Planului SSI, a fost elaborată şi o prezentare grafică conform calificativelor indicatorilor de progres pe acţiunile executate de către instituţiile responsabile şi partenere în anul 2022.

Totodată, ponderea procentuală a realizării acţiunilor este prezentată în graficile 1, 2, 3, 4 și 5, care au fost elaborate în corespudere cu indicii de rezultat ale acestora.

Pilonul I. Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice	
Prioritățile 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



Cu referință la acțiunile Pilonului I, au fost realizate – 20%, parțial realizate – 37%, în proces de realizare – 37%, nerealizate – 2% și cele scadente în următoarea etapă – 4%.

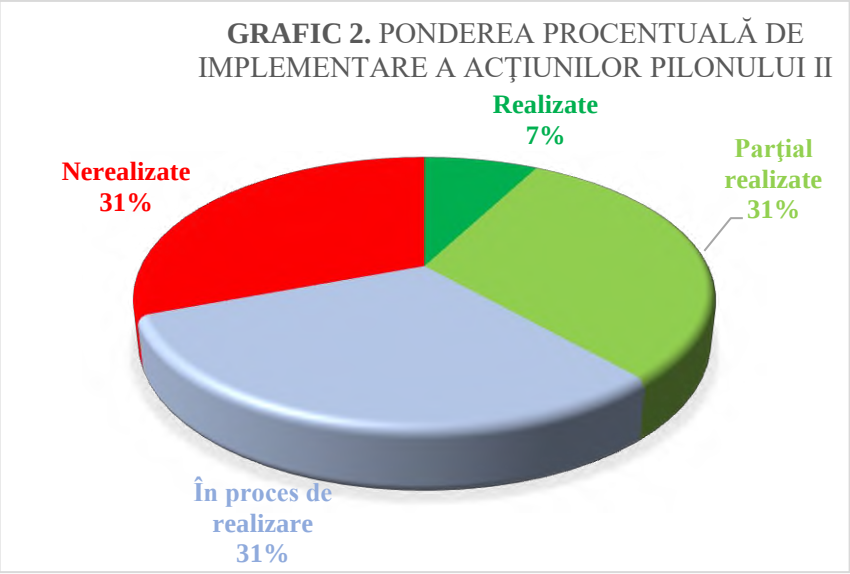
De menționat că în anul 2022, SIS al RM a elaborat 31 de avize consultative prin care a acordat suport structurilor de securitate TIC din cadrul autorităților publice la implementarea măsurilor de protecție a sistemelor informaționale ce prelucrează informațiile atribuite la secret de stat.

Concomitent, SIS a emis avizul consultativ la Proiectul cerințelor de securitate specifice (CSS) înaintat de către o societate comercială pentru elaborarea documentației necesare certificării sistemelor informaționale din posesie. Potrivit datelor, agentul economic are ca domeniu de activitate: realizarea de programe și consultanță în domeniul IT *(activități de realizarea softurilor la comandă)*, prelucrarea datelor activități legate de băncile de date.

Pe parcursul anului 2022 autorităţile responsabile de crearea CERT Naţional au elaborat proiectul de Lege privind securitatea cibernetică, care are scopul central crerea entităţii CERT Naţional, derivă din obiectivul 1/1 şi este prioritatea de bază a Pilonului I. La 16.03.2023 Parlamentul RM a votat în a doua lectură Legea privind securitatea cibernetică, nr. 48, care prevede crearea Centrului naţional de reacţie la incidente de securitate cibernetică *(perioada de raportare)* care intră în vigoare la data de 01.01.2025.

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



În privința acțiunilor Pilonului II, au fost realizate – 7%, parțial realizate – 31%, în proces de realizare – 31%, nerealizate – 31%.

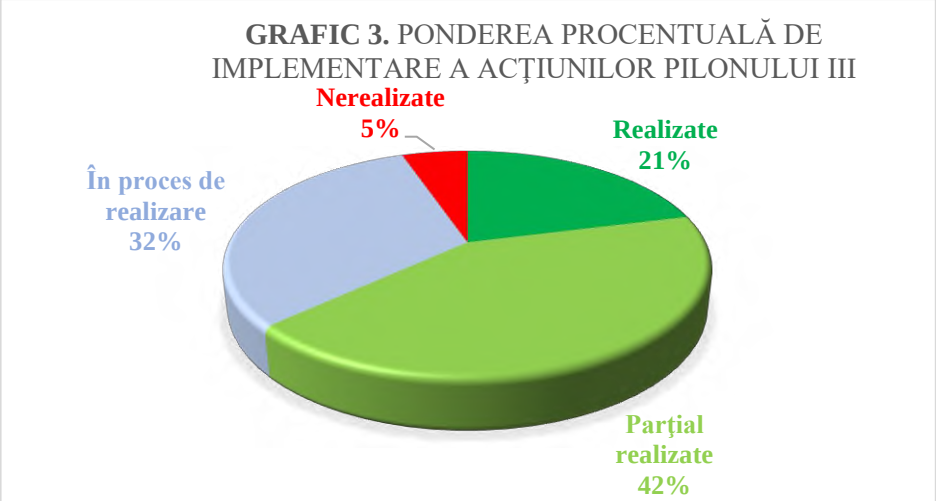
Pe parcursul anului 2022, în temeiul Raportului de evaluare a sectoarelor vulnerabile sub aspectul Comunicării strategice, SIS a elaborat nota informativă privind aspectele problematice în sectorul de securitate națională sub expresia

Comunicării strategice la nivel interinstituțional, fiind înaintată propunerea de implementare a unui STRATCOM – național.

Procesul de implementare a acțiunilor la Pilonul II urmează să se amplifice în anii 2023 – 2024, în special urmare a creării la nivel naţional a Consiliului coordonator pentru asigurarea securităţii informaţionale, care include în componența sa palierele mediatic și civic-privat, formate inclusiv din reprezentanți ai societății civile și mass-media, precum sunt Platforma Națională a Forumului Societății Civile a Parteneriatului Estic, Asociația Presei Independe și Asociația Națională a Companiilor din Domeniul TIC, etc.

Pilonul III. Consolidarea capacităţilor operaţionale

Pilonul III. Consolidarea capacităţilor operaţionale	
Prioritățile 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



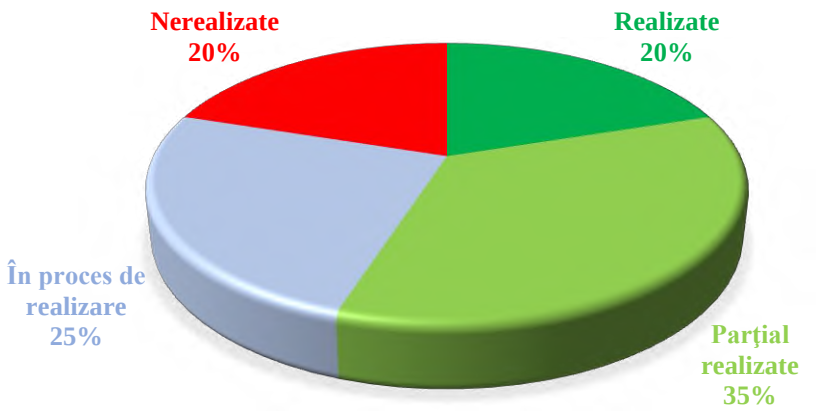
Referitor la acțiunile Pilonului III, au fost realizate – 21%, parțial realizate – 42%, în proces de realizare – 32%, nerealizate – 5%.

În cadrul Pilonului III, în conformitate cu Hotărîrea Guvernului nr. 467/2022, a fost creat Consiliul coordonator pentru asigurarea securității informaționale

(CCASI). Obiectivul central al CCASI este promovarea și coordonarea măsurilor de punere în aplicare a politicilor de securitate informațională și cibernetică într-o societate democratică în funcție de dezvoltarea tehnologiei, raporturilor juridice și de altă natură din sectorul informațional la nivel național, cât și internațional.

Pilonul IV. Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale	
Prioritățile 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 IMPLEMENTARE A ACŢIUNILOR PILONULUI IV



Cu privire la acțiunile Pilonului IV, au fost realizate – 20%, parțial realizate – 35%, în proces de realizare – 25%, nerealizate – 20%.

În context, prioritățile și obiectivele Pilonului IV au o importanță majoră prin prisma proceselor vizate, în special dezvoltarea sistemului de pregătire a specialiștilor în domeniul securității informaționale, sincronizarea coordonării activității tuturor autorităților de drept public și privat în asigurarea securității informaționale, cât și amplificarea cooperării internaționale pe dimensiunile expuse.

DESCRIEREA RISCURILOR DE IMPLEMENTARE

Implementarea obiectivelor Strategiei securității informaționale necesită impulsionarea mobilizării și implicarea plenară a tuturor componentelor societății informaționale în scopul transpunerii în practică a acțiunilor planificate, în special din considerentul că acestea au o configurare transectorială și solicită contribuția instituțiilor și organizațiilor din domeniul civil, media, telecomunicații, cât și celor de securitate, apărare și de drept.

Având în vedere caracterul complex și multidimensional al acțiunilor prevăzute de Planul Strategiei 2019-2024, au fost stabilite riscuri ale procesului de implementare a SSI, unele necesitând o atenție sporită și identificate soluții urgente pentru înlăturarea sau diminuarea acestora. Întru accentuarea și soluționarea acestora, riscurile menționate au fost divizate în trei categorii:

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

- În anul 2022, similar anilor precedenți, a fost remarcată poziția superficială în realizarea acțiunilor planificate, elaborarea și adoptarea documentelor de politici la nivel instituțional sau sectorial ce derivă din Strategia SSI 2019-2024 din partea managementului strategic al unor instituții responsabile sau partenere conform prevederilor Planului;
- Persistă în continuare o cooperare și interacțiune redusă între echipele de specialiști în materie de securitate cibernetică și informațională din cadrul instituțiilor de drept public și privat, vizate în Planul SSI 2019-2024 și managementul decizional al acestora, care în astfel de circumstanțe pot decide unilateral modificarea sau excluderea anumitor acțiuni și obiective din Strategie, reprofilându-le sub alte documente de politici instituționale sau acțiuni, diminuând din caracterul unitar în implementarea Planului de acțiuni.

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

- Insuficiența sau chiar lipsa specialiștilor calificați în domeniul tehnologiilor informaționale în subdiviziunile cu competențe de asigurare a securității cibernetice în cadrul autorităților publice, în special la funcționarea și dezvoltarea Centrelor de reacție la incidentele de securitate cibernetică – CERT departamental;
- Dotarea insuficientă a CERT-urilor instituționale cu sisteme și tehnică specializată pentru asigurarea securității cibernetice la nivelul 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:

- Generarea și dezvoltarea unor noi tipuri de riscuri și amenințări la adresa securităţii informaționale, derivate din amplificarea evoluției tehnologiilor informaționale și, în special, războiul hibrid, care nu sunt prevăzute de SSI și Planul de acțiuni pentru implementarea acesteia;

- Caracterul complex și imprevizibil al dinamicii situației de securitate la nivel regional și internațional urmare a războiului din Ucraina, 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 Serviciului de Informații și Securitate va dezbate cu reprezentanții autorităților responsabile de implementarea Planului de acțiuni al SSI 2019-2024 riscurile menționate cu identificarea soluțiilor pentru remedierea acestora, în funcție de atribuțiile și competențele instituționale.

CONCLUZII ŞI RECOMANDĂRI

Monitorizarea și coordonarea procesului de implementare a Strategiei și Planului acesteia pe parcursul anului 2022, cu elaborarea Raportului de progres pentru al patrulea an, relevă în continuare că prioritățile de securitate informaţională ale SSI rămân conforme tendințelor actuale ale evoluției societăţii informaţionale la nivel național și regional.

Evaluarea punctuală a realizărilor și indicatorilor de rezultat prezentați de instituţiile responsabile și partenere pentru anul 2022, în corespundere cu scopul, obiectivele şi acțiunile Strategiei, **denotă un progres insuficient** în realizarea acestora.

În context, **riscurile de securitate** şi **criminalitate cibernetică**, dar și evoluţia **noilor forme de ameninţări hibride** la adresa **securităţii informaţionale a Republicii Moldova – războiul informaţional, ameninţările hibride, dezinformarea, propaganda, manipularea,** care **sunt în vizorul Strategiei**, sunt actuale și încă **nu au fost eliminate** sau **diminuate**.

Totodată, **unele realizări raportate** de autorităţile vizate de Plan, **se suprapun pe cadrul de competență instituțională** și **activitatea ordinară** a acestora. Astfel, **este primordial** să **percepem** și **conștientizăm obiectivele** și **acțiunile Planului Strategiei** vizavi de activitatea autorităţilor pe atribuţii şi competenţe.

Subsidiar, **rapoartele de progres** prezentate pe activități **nu atestă o cooperare eficientă între instituțiile responsabile și cele partenere**, or pentru rezolvarea problemelor de securitate informațională sunt **necesare soluții complexe** și **coerență interinstituțională**, cu aplicabilitate în toate domeniile de drept public și privat, părți ale societății informaționale în general.

Totuși, **parțial se atestă o conștientizare a problemelor de securitate informaţională din partea reprezentanţilor insitituţiilor de drept public şi privat**, una din **realizările majore pentru anul 2022** fiind **crearea Consiliului coordonator pentru asigurarea securității informaționale** (CCASI) prin Hotărârea Guvernului Republicii Moldova nr. 467 din 06 iulie 2022 (Monitorul Oficial nr. 201-207/531 din 08.07.2022) şi crearea legii cadru – Legea nr. 48/16.03.2023 privind securitatea cibernetică, ce stabileşte modul de instituire a CERT Naţional.

Prin urmare, evaluarea și analiza rezultatelor înregistrate în anul 2022 şi a celor cu termen permanent de implementare, prezentate de instituțiile responsabile și cele partenere, urmează a fi examinate punctual în cadrul următoarelor şedinţe ale Grupului de monitorizare a implementării SSI din cadrul SIS și persoanele responsabile din instituțiile vizate în Planul de acțiuni privind implementarea Strategiei securității informaționale a Republicii Moldova 2019-2024.