R A P O R T

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

Perioada de raportare: 2023

SERVICIUL DE INFORMAȚII ȘI SECURITATE

Elaborat – martie 2024

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”
- HG – Hotărârea Guvernului
- HP – Hotărârea Parlamentului
- IGP – Inspectoratul General de Poliție
- INI – Inspectoratul Național de Investigații
- MA – Ministerul Apărării
- MAE/MAEIE – Ministerul Afacerilor Externe
- MAI – Ministerul Afacerilor Interne
- MAIA – Ministerul Agriculturii și Industriei Alimentare
- MDED – Ministerul Dezvoltării Economice și Digitalizării
- MEC – Ministerul Educaţiei şi Cercetării
- MF – Ministerul Finanţelor
- MJ – Ministerul Justiţiei
- MS – Ministerul Sănătății
- 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
- 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)* reprezintă o evaluare complexă a acţiunilor realizate şi rezultatelor înregistrate pe parcursul anului 2023 în procesul de aplicare a 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. 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 pentru anii 2019 – 2024 constă în integrarea juridică și sistemică ale domeniilor prioritare cu responsabilităţi şi competenţe în asigurarea securităţii informaţionale a țării noastre, pilonii de bază fiind reziliența 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 reziliență cibernetică și ridicarea nivelului de cultură în domeniul TIC.

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

1. Dezvoltarea mecanismelor de comunicare strategică pentru realizarea intereselor naționale ale Republicii Moldova;
2. Controlul civic și consolidarea cooperării societății civile cu autoritățile publice cu atribuții de asigurare a securității informaționale;
3. Determinarea statutului juridic al publicaţiilor periodice, al agenţiilor de presă şi 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 2023 – al cincilea an de implementare a Hotărârii Parlamentului nr. 257, Serviciul de Informații și Securitate, de comun cu instituțiile responsabile și partenere, au realizat acțiuni întru executarea Planului, inclusiv organizatorice, fiind realizate interacțiuni 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 cincilea 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 discuţiilor 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 „Nerealizat”.

DESCRIEREA PROGRESELOR ACȚIUNILOR REALIZATE ÎN PERIOADA ANULUI 2023

Capitolul relevă progresul executării acţiunilor scadente în anul 2023 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 entității care va exercita rolul de Centru național de reacție la incidente de securitate cibernetică și care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autoritățile publice competente și persoanele fizice și juridice: a) elaborarea și promovarea cadrului normativ relevant; b) crearea Centrului național de reacție 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 Dezvoltării Economice şi Digitalizării.*

În conformitate cu Hotărârea Guvernului Nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale, precum și în vederea executării prevederilor Hotărârii Guvernului Nr.746/2010 „Cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului Republica Moldova – NATO actualizat”, Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” se desemnează în calitate de Centru guvernamental de reacție la incidente de securitate Cibernetică *(CERT Gov MD).*

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
1/2	Desemnarea entității care va exercita rolul de Centru guvernamental de reacție la incidente de securitate cibernetică și care va constitui punctul de raportare a incidentelor de securitate cibernetică al Guvernului; stabilirea interacțiunii acestuia cu Centrul național de reacție la incidente de securitate cibernetică	Anul 2019	Realizat

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

La data de 16 martie 2023 a fost adoptată Legea nr. 48/2023 privind securitatea cibernetică, prin care se stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, se determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, se 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**			
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	Parțial realizat

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

Potrivit Hotărârii Guvernului nr. 1028/2023, cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, Agenția pentru Securitate Cibernetică exercită funcția de echipă de răspuns la incidentele cibernetice la nivel național și cea de punct național unic de contact. Agenția nominalizată urmează a fi creată pe parcursul anului 2024.

Ofițerii SIS au participat la ședințele de lucru pentru elaborarea/ avizarea cadrului normativ *(HG nr. 1028/2023)*, ce reglementează activitatea Agenției pentru securitatea cibernetică *(ASC)*, entitate care va exercita funcția Centrului de răspuns la incidentele de securitate cibernetică la nivel național *(CERT)*. Concomitent, SIS a avizat proiectul de Lege privind securitatea cibernetică *(Legea nr. 48/2023)*.

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	Parțial realizat

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

Prin scrisoarea nr. 1.4/1088/23 din 11.08.2023 STISC a solicitat repetat autorităților publice să informeze despre despre acțiunile și măsurile întreprinse în vederea constituirii CERT-ului departamental cu 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.

De asemenea în perioada 05-06 octombrie 2023, STISC a desfășurat un atelier de lucru cu participarea a 30 specialiștii IT din cadrul mai multor instituții guvernamentale, dar și reprezentanți din infrastructurile critice ale țării, precum: sectorul energetic, servicii de transport, sănătate, comunicații și sectorul financiar. Cei prezenți au subliniat importanța colaborării intersectoriale în abordarea provocărilor legate de securitatea cibernetică.

În același timp, ofițerii SIS au participat la 16 întrevederi bilaterale cu reprezentanții serviciilor partenere, în vederea preluării bunelor practici și

schimbului de experienţe în domeniul securităţii şi apărării cibernetice. Componenta operaţională a CERT-ului instituţional este funcţională şi activează în conformitate cu cadrul normativ intern.

Prin Ordinul Procurorului General nr.33/3 din 03.05.2022 a fost înfiinţată Secţia tehnologii informaţionale în cadrul Aparatului Procuraturii Generale, care conform atribuţiilor sale instituţionale răspunde la incidentele de securitate cibernetică care au avut loc în Procuratură. Prin urmare, orice presupus incident de securitate cibernetică este raportat Secţiei tehnologii informaţionale, care la rândul său în comun cu STISC întreprind măsuri în vederea remedierii situaţiei.

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

Instituţia resonsabilă: *Ministerul Dezvoltării Economice şi Digitalizării*.

În temeiul art. 23 din Legea nr. 100/2017 cu privire la actele normative, pe parcursul anului 2023, a fost adoptată *Legea nr. 48/2023 privind securitatea cibernetică* care stabileşte cadrul normativ primar în domeniul securităţii cibernetice. Legea urmează să intre în vigoare la data de 01 ianuarie 2025 şi cuprinde un set de reglementări care au drept scop instituirea unui model de guvernanţă eficient la nivel naţional în vederea protecţiei şi asigurării securităţii reţelelor şi sistemelor informatice, utilizate de către persoanele juridice, publice sau private, în procesul de prestare a serviciilor considerate a fi esenţiale pentru susţinerea unor activităţi societale şi economice critice.

Una dintre prevederile de bază ale Legii privind securitatea cibernetică vizează instituirea de către Guvern a unei autorităţi competente în domeniul securităţii cibernetice la nivel naţional, care să asigure o protecţie suficientă a sectorului public şi sectorului privat împotriva incidentelor, riscurilor şi ameninţărilor legate de securitatea reţelelor şi a sistemelor informatice. În acest sens, a fost aprobată Hotărârea Guvernului nr. 1028/2023 cu privire la constituirea, organizarea şi funcţionarea Agenţiei pentru Securitate Cibernetică. Agenţia urmează să exercite funcţiile de echipă de răspuns la incidentele de securitate cibernetică *(CSIRT),* de punct unic de contact la nivel naţional, de implementare a politicii de stat, supraveghere şi control în domeniul securităţii cibernetice.

Pentru a asigura implementarea Legii nr. 48/2023 privind securitatea cibernetică, Ministerul Dezvoltării Economice şi Digitalizării a elaborat şi remis spre reavizare proiectul de lege pentru modificarea unor acte normative *(aducerea cadrului legal în concordanţă cu Legea nr. 48/2023 privind securitatea cibernetică) (număr unic 957/MDED/2023)*. În proiectul de lege sunt propuse modificări la 22 de legi, în vederea ajustării normelor cuprinse în actele legislative sectoriale care reglementează activitatea viitorilor furnizori de servicii, precum şi a normelor juridice având un caracter conex normelor care asigură direct aplicarea legislaţiei armonizate. Totodată, sunt propuse norme care vor completa baza juridico-

normativă necesară pentru aprobarea de către Guvern a unor acte normative de punere în aplicare a Legii privind securitatea cibernetică. La 21 martie 2024, Parlamentul a adoptat proiectul de lege *(aprobat prin Hotărârea Guvernului nr. 106 din 14 februarie 2024)*.

Totodată, întru executarea art. 6 alin. (2) din Legea nr. 48/2023, fost elaborat și remis spre avizare proiectul hotărârii Guvernului cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice *(nr. unic 1186/MDED/2023)*. Rolul principal al Consiliului coordonator, așa cum este stabilit și în Legea privind securitatea cibernetică, este de a acționa ca un pilon strategic în coordonarea politicilor de securitate cibernetică, cu accent pe planificarea și coordonarea strategică în domeniul securității cibernetice, pentru a asigura o protecție eficientă a infrastructurii cibernetice. Printre responsabilitățile de bază ale Consiliului se numără: coordonarea elaborării și implementării Strategiei naționale de securitate cibernetică și a altor documente de politici și de planificare în domeniul securității cibernetice; asigurarea îndeplinirii obligațiilor autorităților publice în realizarea documentelor de politici, documentelor de planificare și actelor normative în domeniul securității cibernetice; precum și prezentarea de recomandări autorităților și instituțiilor publice cu competențe în acest domeniu.

Suplimentar, informăm că în septembrie 2023 a fost aprobată Hotărârea Guvernului privind dezvoltarea profesională în domeniul securității cibernetice nr. 671/2023, conform căreia Instituția Publică „Universitatea Tehnică a Moldovei" va asigura dezvoltarea profesională a personalului din autoritățile publice, precum și a altor persoane interesate din sectorul public și sectorul privat, prin programe de instruire, perfecționare și exerciții de antrenament în domeniul securității cibernetice. Institutul Național de Inovații în Securitatea Cibernetică „Cybercor", care urmează a fi inaugurat în primăvara anului curent, acesta urmărește dezvoltarea abilităților în domeniul securității cibernetice a personalului, formarea studenților din cadrul Universității Tehnice a Moldovei și altor instituții, precum și a profesioniștilor în securitate cibernetică, contribuind astfel la consolidarea rezilienței cibernetice a Republicii Moldova.

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

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

În perioada de raportare nu au fost înregistrate progrese pe obiectivul nominalizat.

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	Parțial realizat

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

Pentru anul 2023, AGE a realizat misiuni de audit de securitate cibernetică în cadrul a 4 ministere, formate în 2021 ca entități descendente din alte ministere, după cum urmează:

- Ministerul Mediului;
- Ministerul Culturii;
- Ministerul Muncii și Protecției Sociale;
- Ministerul Infrastructurii și Dezvoltării Regionale.

Concluziile și recomandările rezultate au fost expuse în rapoartele de audit elaborate pentru fiecare autoritate auditată.

În ce privește 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 privind remedierea neconformităților),* precum și despre rezultatele altor misiuni de audit de securitate cibernetică *(plan/raport de remediere a neconformităţilor),* efectuate în cadrul entității.

În contextul evaluării, se constată următoarele:

- STISC, CTIF, MA, CSS, MF au prezentat dovezi concludente privind implementarea recomandărilor de audit, 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.
- ASP, MAEIE au raportat despre realizarea recomandărilor, iar acțiunile parțial realizate sau aflat în derulare, la data raportării urmau să fie realizate dependent de resursele bugetate.
- MAI, MDED, MS, MEC, MAIA, MJ nu au prezentat dovezi privind măsurile de securitate implementate sau planuri/acțiuni ținute la controlul conducerii ministerului.

Astfel, starea securității cibernetice nu poate fie evaluată. Prin urmare, se constată că entitățile cu profil aferent prestării serviciilor bazate pe TIC au realizat o parte considerabilă din recomandările misiunilor de audit.

Totuși, în cadrul autorităților administrației publice ce nu prestează sau sunt la o etapă incipientă de prestare a serviciilor publice bazate pe TIC, se constată un nivel scăzut de implementare a Cerințelor minime de securitate cibernetică, pornind de la măsurile organizaționale și administrative.

Motivul principal se profilează în lipsa resurselor de personal, dar se denotă o problemă majoră în conștientizarea managementului de a aloca/asigura resursele necesare implementării cerințelor minime de securitate cibernetică.

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”.

În perioada de raportare, SIS a examinat solicitările de remediere a riscurilor de securitate identificate *„cyber threat”* în cadrul infrastructurilor de tehnologii informaționale și comunicații a unor autorități publice, în contextul pregătirii pentru Summit-ul Comunității Politice Europene (CPE). În rezultat, SIS a remis în adresa IS „Aeroportul Internațional Chișinău”, ÎS „MoldATSA” și STISC recomandările specializate pentru anticiparea riscurilor de securitate identificate.

În anul 2023, în cadrul MA a fost efectuat 1 *(unu)* audit intern al managementului securității informaționale și apărării cibernetice.

În cadrul Procuraturii Generale a fost efectuat auditul de securitate cibernetică a infrastructurii informaționale, cu întocmirea unui Raport privind starea de securitate cibernetică, cu indicarea recomandărilor pentru remedierea disfuncțiilor și vulnerabilităților. Măsurile urmează a fi întreprinse în conformitate cu posibilitățile instituționale de remediere.

Pe parcursul anului 2023 ASP a efectuat: un audit extern *(23.02.2023 – 24.04.2023)* în privința securității informaționale și un audit intern *(09-10.2023)* privind protecția datelor cu caracter personal. În baza rapoartelor de audit au fost elaborate planuri și executate lucrări de înlăturare a vulnerabilităților depistate și de minimizare a pericolelor în spațiul cibernetic pentru a îmbunătăți protecția resurselor informaționale și a asigura complexitatea serviciilor electronice publice prestate de ASP.

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 contextul serviciilor electronice publice, prestate de către autoritățile și instituțiile guvernamentale, evaluarea aplicării Cerințelor minime de securitate cibernetică de nivelul II în cadrul acestora se asigură prin corelarea recomandărilor misiunilor de audit, efectuate 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 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 2023 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.

Totodată, AGE a asigurat coordonarea și ajustarea a două documente elaborate în cadrul proiectului Moldova Cybersecurity Rapid Assistance, ce reprezintă instrumente importante la implementarea cerințelor de securitate pentru soluțiile utilizate în cadrul prestării serviciilor electronice publice:

- Ghid cu privire la ciclul de viață securizat al dezvoltării de software (SSDLC);
- Cerințe minime de securitate cibernetică pentru produsele TIC, aliniate la standardele naționale și internaționale (versiune draft).

Potrivit ASP, în perioda de raportare a avut loc tratarea riscurilor reziduale de nivel „Înalt" și nivel „Mediu" pe următoarele domenii pentru îmbunătățire:

- Organizarea sistemului intern de securitate cibernetică/informațională,
- Cerințele minime obligatorii de securitate cibernetică de nivelul 2,
- Achiziția /actualizarea sistemelor informaționale,
- Externalizarea administrării/ mentenanței sistemelor informaționale,
- Răspunsul la incidente, continuitatea proceselor și recuperarea.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În anul 2023 în vederea asigurării securității informației la utilizarea resurselor informaționale a avut loc instruirea planificată a personalului ASP pe platforma guvernamentală MLearn, inclusiv introductiv-generală la angajare.

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, nu au fost înregistrate progrese pe obiectivul enunțat.

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

	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		

Instituția responsabilă: *Autorităţile administraţiei publice.*

Potrivit ASP, pentru aplicarea măsurilor de protecție a datelor cu caracter personal și asigurarea securității informaționale a serviciilor electronice care se bazează pe prelucrarea datelor cu caracter personal în corespundere cu legislația în vigoare se consultă și se coordonează Centrul Național pentru Protecția Datelor cu Caracter Personal.

În perioada anului 2023, CNPDCP a avizat 154 de proiecte de acte normative naționale/tratate internaționale sub aspectul protecției drepturilor și libertăților persoanelor fizice în legătură cu prelucrarea datelor cu caracter personal. Opiniile s-au subsumat obiectivului de informare și de consiliere legislativă oferită autorităților sau instituțiilor publice competente, precum și altor entități, în scopul asigurării unei aplicări unitare și corecte a principiilor de protecție a datelor personale.

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

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

Potrivit obiectivului acțiunii, pe parcursul anului 2023 Ministerul Apărării a realizat următoarele acțiuni:

- Desfășurarea ședinței de lucru privind prezentarea viziunii Armatei Naționale pe domeniul securității și apărării cibernetice – factorilor de decizie ale MA și Marelui Stat Major.
- Participarea la consultări publice a proiectului Hotărârii de Guvern, cu privire la aprobarea proiectului de lege privind securitatea cibernetică;
- Participarea la consultările publice cu genericul: „Viziunea strategică privind asigurarea securității cibernetice”, la Chișinău;
- Elaborarea și expedierea în adresă a propunerilor pe domeniu cu privire la Legea securității cibernetice;
- Implicarea în dezvoltarea capabilităților de apărare cibernetică prin intermediul asistențelor externe European Peace Facility (EPF) și Foreign Military Assistance (FMF);
- Participarea Armatei Naționale la instruirile organizate de către STISC în cadrul proiectului European, Cyber Rapid Assistance.

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	Parţial realizat

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

În anul de raportare, SIS nu a identificat careva riscuri și vulnerabilități în cadrul sistemului de infrastructura critică al Armatei Naționale și Ministerului Apărării. Mai mult, SIS a examinat și avizat Proiectul Regulamentului cu privire la organizarea și funcționarea organelor de cifrare în cadrul Ministerului Apărării.

SIS a remis notificări de securitate cibernetică operatorilor de comunicații naționali, în contextul atacului cibernetic asupra companiei „Kyivstar" din Ucraina. Totodată, SIS este în proces de elaborare a unor prescripții pe domeniul securității cibernetice pentru operatorii de infrastructură critică din domeniul energetic.

Pe parcursul anului 2023, MA a întreprins următoarele:

- continuarea elaborării cerințelor de securitate specifică pentru sistemele informaționale atribuite la secretul de stat, precum și pregătirea infrastructurii TI;
- managementul programelor de asistență externă pentru procurarea echipamentelor de criptare a traficului.

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*

Serviciul a acordat suport specializat la crearea subdiviziunilor de securitate pentru tehnologia informației în cadrul:

1. *Centrului Arhivei Naționale;*
2. *Centrului militar din mun. Chișinău;*
3. *Brigăzii nr. 2 Infanterie Motorizată;*
4. *Centrului militar teritorial Hâncești;*
5. *Centrului de Armament și Muniții;*
6. *Inspectoratului General al Poliției de Frontieră;*
7. *Batalionului cu Destinație Specială „Fulger";*
8. *Ministerului Infrastructurii și Dezvoltării Regionale;*
9. *Ministerului Finanțelor;*
10. *Bazei de păstrare a combustibilului ai Armatei Naționale;*
11. *Spitalului Clinic Militar Central;*
12. *Bazei militare de instruire a Armatei Naționale;*
13. *Inspectoratului Național de Securitate Publică;*

14. *Inspectoratului General pentru Migrație al MAI;*
15. *Serviciului Fiscal de Stat;*
16. *Direcției regionale Sud a IGPF;*
17. *Administrației Naționale a Penitenciarilor;*
18. *Detașamentului cu Destinație Specială „Pantera”;*
19. *Centrului de Instruire al ANP;*
20. *Centrului militar teritorial Ungheni;*
21. *Academiei militare a Forțelor Armate;*
22. *Regimentului de rachete antiaeriene al Ministerului Apărării.*

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

Instituția responsabilă: *Serviciul de Informații și Securitate*.

Reieșind din necesitatea de interconectare a sistemelor informaționale din cadrul Aparatului Central și locațiile teritoriale ale SIS, a fost realizată o evaluare a situației existente, fiind stabilite tipul și cantitatea necesară de echipamente de protecție criptografică. Mecanismele de protecție pentru sistemele speciale de comunicații electronice sunt funcționale.

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 comunicații electronice și raportarea către autoritatea responsabilă cu privire la măsurile tehnice și tehnico-organizatorice întreprinse pentru asigurarea securității cibernetice	Permanent, cu verificarea anuală a indicatorilor de progres	Realizat

Instituția responsabilă: *Serviciul de Informații și Securitate*.

Pe parcursul anului 2023, specialiștii SIS au efectuat 2 proceduri de audit de securitate cibernetică a sistemelor informaționale gestionate de către SIS. Totodată, în perioada de raportare, în adresa SIS nu au parvenit rapoarte de audit de la autoritățile statului.

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 comunicații 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**			
4/4	Elaborarea sistemului de atestare a obiectivelor de informatizare *(articole plasate în rețeaua globală Internet, pagini web informative, baze de date sau alte surse cu caracter informațional)* privind îndeplinirea cerințelor de asigurare a protecției informației în timpul efectuării lucrărilor ce țin de prelucrarea și păstrarea informațiilor cu accesibilitate limitată, în special a celei atribuite la secret de stat	2023-2024	În proces de realizare

Instituția responsabilă: *Serviciul de Informații și Securitate*

În anul 2023 a fost creată Agenția pentru securitatea cibernetică *(HG nr. 1028/2023)*, autoritate care va exercita funcția Centrului de răspuns la incidentele de securitate cibernetică la nivel național *(CERT-național)*.

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

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

CNPDCP învederează că, prin Legea nr. 60/2023 pentru modificarea unor acte normative *(stimularea comerțului electronic),* au fost aduse modificări/completări la art. 30 din Legea nr. 133/2011 privind protecția datelor cu caracter personal, denumit „Securitatea prelucrării datelor cu caracter personal”.

Alineatul (2) din articolul prenotat a fost completat cu două enunțuri noi cu următorul cuprins: „Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la toate modificările preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a prezenta obiecții față de modificările respective.”

Mai mult, art. 30 din legea prenotată a fost completat cu alineatele (2^1) și (3^1) cu următorul cuprins:

„(2^1) În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de operațiuni de prelucrare specifică în numele operatorului, aceleași obligații privind protecția datelor cu caracter personal, prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, revin și celei de-a doua persoane împuternicite,

în temeiul unui contract sau al unui alt act juridic, în special care să furnizeze garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentei legi. În cazul în care cea de-a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor cu caracter personal, persoana împuternicită de operator continuă să poarte răspundere deplină față de operator în ceea ce privește îndeplinirea obligațiilor celei de-a doua persoane împuternicite."

„(3^1) Contractul sau celălalt act juridic se încheie în scris, inclusiv în formă electronică."

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 protecția datelor cu caracter personal în cadrul persoanelor juridice de drept public și de drept privat	Anul 2020, cu verificarea trimestrială a indicatorilor de progres	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.

În lumina noilor reglementări, CNPDCP a transmis demersuri, prin care a informat asupra necesității desemnării de către autoritățile/instituțiile publice, precum și subdiviziunile aflate în subordinea acestora, a persoanei responsabile cu protecția datelor.

Astfel, CNPDCP a fost informat despre desemnarea a 115 persoane responsabile cu protecția datelor de către instituțiile publice cât și cele private.

Supletiv, în perioada raportată CNPDCP a desfășurat 61 de activități de instruire, pentru un număr record de instituții publice. Scopul acestora a fost de a spori gradul de percepție a angajaților asupra inovațiilor legislative privind protecția datelor cu caracter personal *(evaluarea impactului, consultarea prealabilă, persoana responsabilă cu protecția datelor, transferul transfrontalier a datelor cu caracter personal),* precum și asupra asigurării aplicării corecte a prevederilor legale din domeniu în activitatea pe care o desfășoară.

Adițional, CNPDCP a organizat în mod special 5 cursuri de instruire pentru persoanele desemnate de către operator sau persoana împuternicită de către operator, în calitate de Responsabil cu Protecția Datelor.

Scopul acestor cursuri de instruire a constat în dezvoltarea cunoștințelor teoretice în domeniul protecției datelor cu caracter personal și a deprinderilor practice privind aplicarea actelor normative și cerințelor legislației din domeniu. În cadrul evenimentelor au fost discutate subiecte de importanță, cum ar fi: definirea noțiunilor generale aferente domeniului protecției datelor cu caracter personal;

drepturile subiecților de date cu caracter personal; prelucrarea categoriilor speciale de date cu caracter personal; principii și temeiuri legale pentru prelucrarea datelor cu caracter personal; asigurarea securității și confidențialității datelor cu caracter personal prelucrate; aspecte ce țin de Responsabilul cu protecția datelor (DPO); aspecte ce țin de Evaluarea Impactului asupra Protecției Datelor etc.

Până în prezent, au fost instruiți circa 45 de DPO atât din cadrul sectorului public, cât și a mediului privat.

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

Instituția responsabilă: *Serviciul de Informații și Securitate*.

În perioada vizată, SIS a emis 3 certificate de conformitate pentru mijloace de protecție tehnică și criptografică a informației, inclusiv a verificat corespunderea condițiilor de licențiere a agenților economici:

1. SA „MOLDCELL”;
2. SA „BTS PRO”;
3. SA „EURO SIGURANȚA”.

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

Instituția responsabilă: *Serviciul Vamal, 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 I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
5/3	Alinierea cadrului normativ în domeniul protecției criptografice a informației la cadrul normativ european	Anul 2021, cu verificarea anuală a indicatorilor de progres în cazul realizării înainte de termen	Realizat

Instituția responsabilă: *Serviciul de Informații și Securitate*.

În perioada 1 - 3 martie 2023 MAEIE a prezentat avizele pe marginea proiectului HG privind aprobarea proiectului de Lege privind securitatea cibernetică *(număr unic 41/ME/2023).* La 17 iulie a fost prezentat avizul cu referire la HG cu privire la organizarea instruirii în domeniul securității cibernetice *(număr unic 507/MDED/2023).*

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 Informaţii şi Securitate.*

În anul 2023, SIS a examinat raportul de activitate a prestatorului de servicii de certificare din cadrul STISC, nefiind depistate încălcări ale cadrului normativ în domeniul semnăturii electronice.

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

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

Pe parcursul anului 2023 angajații Poliție au participat la 18 activități în scopul sporirii capacităților specialităților cu atribuții în domeniul criminalității informatice, fiind instruiți 26 angajați, după cum urmează:

Instruiri:

- în perioada 01-03.02.2023, 2 angajați au participat la cursul de instruire în domeniul gestionării cazurilor de alertă cu bombe, organizat în parteneriat cu reprezentanții Institutului Interregional al Națiunilor Unite privind Crima şi Justiţia *(UNICRI);*
- la 02.02.2023, 2 angajați au participat la cursul de instruire on-line, cu genericul „All assigned Digital Investigation in Hansken”;
- în perioada 06-10.02.2023, 1 angajat a participat la cursul de instruire „Investigarea crimelor de război”, în contextul implementării proiectului TOPCOP;
- în perioada 13-17.02.2023, 1 angajat a participat la sesiunea de instruire privind echipele comune de investigație *(JIT)* și îmbunătățirea cooperării cu furnizorii de servicii străini în cadrul celui de-al doilea protocol adițional la Convenția de la Budapesta, organizat sub egida proiectului „CyberEst” și în cooperare cu Procuratura Generală a Portugaliei în Lisabona, Portugalia;
- în perioada 21-22.03.2023, 5 angajați au participat la cursul de formare profesională cu genericul „Criminalitatea cibernetică”, organizat de către Direcția dezvoltare profesională a Academiei Ștefan cel Mare” a MAI în parteneriat cu Consiliul Europei, mun. Chișinău;
- în perioada 08-09.06.2023, 3 angajați au participat la sesiunea de instruire privind clasificarea și tratarea incidentelor cibernetice și a criminalității cibernetice în conformitate cu Procedurile Operaționale Standard, organizat în cadrul Proiectului Proiectul CyberEast al Uniunii Europene și al Consiliului Europei;

- în perioada 12-13.06.2023, 1 angajat a participat la cursul regional de instruire cu genericul „TTX-Assess, Organize, Communicate and React”, ce prevede exersarea și testarea capabilității de reacție din partea instituțiilor guvernamentale la situații de criză;
- în perioada 18-23.06.2023, 2 angajați au participat la cursul regional de instruire cu genericul „Investigații Dark Web, dovezi electronice și criptomonede”, organizat în contextul implementării proiectului TOPCOP la Budapesta, Ungaria;
- în perioada 30.10-02.11.2023, 1 angajat a participat la cursul de instruire avansată privind investigarea activelor virtuale, organizat de Oficiul Coordonatorului pentru Activități Economice și de Mediu al OSCE, în colaborare cu oficiul ONU pentru Droguri și Crimă
- în perioada 13-17.11.2023, 3 angajați au participat la cursul de instruire cu genericul „Activitatea de prevenire și combatere a fraudelor prin utilizarea mijloacelor de plată electronice”, în cadrul Centrului Multifuncțional de Pregătire Schengen, sediul Buzău, România;
- în perioada 28-29.11.2023, 1 angajat a participat la cursul de instruire „Europol Malware Analysis Solution Workshop *(EMAS)*”organizat de către OEP Europol, la București, România,
- în perioada 04-08.12.2023, 2 angajați au participat la cursul de instruire axat pe abordarea subiectelor aferente analizei din surse deschise *(OSINT)* și patrularea în mediul online, eveniment organizat sub egida Biroului de control pentru Europa de Sud-Est asupra armelor de calibru mic și a armamentului ușor *(SEESAC).*

Vizite de studiu:

- în perioada 05-11.03.2023, 1 angajat a efectuat o vizita de studiu în Regatul Țărilor de Jos Și Belgia în cadrul proiectului de „Asistență rapidă în domeniul securității cibernetice din Moldova *(CRA);*
- în perioada 15-18.03.2023, 1 angajat a realizat o vizita de studiu în cadrul Centrului de Crime Cibernetice EC3, în Haga, Regatul Țărilor de Jos, organizată sub egida Agenției Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii;
- în perioada 03-05.05.2023, 1 angajat a realizat o vizită de studiu în domeniul securității cibernetice, în cadrul Ministerului Apărării din Luxemburg;
- în perioada 13-17.05.2023, 2 angajați au realizat o vizită de studiu la Academia de Guvernare Electronică din Estonia, Tallin;
- în perioada 14-17.05.2023, 2 angajați au efectuat o vizită de studiu în domeniul combaterii criminalității cibernetice, în cadrul structurilor franceze OLTI și COMCYBERGENG, în Franța, Paris;
- în perioada 23-26.05.2023, 1 angajat a realizat o vizită de studiu în Regatul Spaniei, Madrid, scopul căreia este familiarizarea cu experiența instituțiilor pe subiectul protecția infrastructurii critice, crime cibernetice și combaterea terorismului.

În perioada anului 2023 angajații Poliției au participat și acordat suport în cadrul a unei acțiuni comune de investigații cu caracter internațional, după cum urmează:

Suport acordat omologilor din România cu privire la fraudele comise prin metoda „Investment Scam”, fiind realizat și un schimb de informații cu privire la platformele și mijloace de plată utilizate la comiterea infracțiunilor.

În urma participării în cadrul instruirilor nominalizate, ofițerii de poliție au obținut:

1) cunoștințe și abilități de investigare operațională a criminalității informatice, cât și în domeniul securității cibernetice.

2) au fost îmbunătățite capacitățile de cooperare și reacție din partea instituțiilor guvernamentale pe cazurile de crime cibernetice, de cooperare cu furnizorii de servicii, inclusiv străini.

3) au fost stabilite relații de cooperare privind schimbul de informații operative.

Potrivit PG, numărul de procurori din procuraturile specializate și teritoriale specializați în domeniu - 39.

Numărul de persoane instruite - 22.

Numărul de cauze transmise în judecată: 14/15 cauze/persoane.

- Art. 177 CP – 9 cauze penale;
- Art. 178 CP – 1 cauză penală
- Art. 260^5 CP – 4 cauze penale.

În perioada anului 2023, de către instanțele de fond au fost examinate 14 cauze penale cu pronunțarea sentințelor în privința a 20 persoane:

- Art. 177 CP – 12 cauze penale / 18 persoane;
- Art. 260 CP – 1 cauză penală / 1 persoană;
- Art. 260^5 CP – 1 cauză penală / 1 persoană.

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	Parțial realizat

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

Angajații Poliției *(CCCC al INI)* au participat în calitate de formatori în cadrul a 2 sesiuni de instruire, după cum urmează:

- în perioada 28.02-02.03.2023, 2 angajați au participat în calitate de formatori la trainingul „Prevenirea și combaterea exploatării și abuzului sexual asupra copiilor în mediul online”, organizat de CoE în cadrul proiectului „Protecția copiilor împotriva violenței și prevenirea acesteia, inclusiv în mediul online” https://www.coe.int/en/web/chisinau/-/training-for-specialists-in-preventing-and-combating-online-child-exploitation-and-abuse-ocsea-?pk_campaign=newsletter;
- la 22.03.2023, 1 angajat a participat în calitate de formator la cursul de instruire privind criminalitatea informatică, organizat de CoE în cadrul proiectului „Cyber East”, eveniment desfășurat în cadrul Academiei ”Ștefan cel Mare” a MAI.

Potrivit raportului Procuraturii Generale, la solicitare este acordat suport metodologic și practic procurorilor teritoriali la investigarea infracțiunilor informatice.

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.*

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

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
6/4	Perfecționarea cadrului legal ce reglementează salarizarea efectivului specializat în combaterea criminalității informatice și investigarea infracțiunilor informatice	Anul 2020	Parțial realizat

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

Ținând cont de documentele de planificare strategică pe termen mediu, Ministerul Finanțelor urmează să asigure consolidarea sistemului unitar de salarizare în sectorul bugetar printr-o reformă structurală salarială. În vederea atingerii acestui obiectiv, în baza unui proces desfășurat de asistența tehnică din partea donatorilor externi, urmează a fi elaborată o propunere tehnică de reformă cuprinzătoare a structurii salariale pe termen mediu, care să limiteze presiunile pe masa salarială, inclusiv reducerea numărului de valori de referință.

Pentru a îmbunătăți raportul de comprimare a salariilor și pentru a răspunde nevoilor critice de personal, analiza va cuprinde întregul sistem de salarizare cu o perspectivă pe termen mediu sincronizată cu procesul CBTM, creșterile salariale viitoare vor ține cont de un set bine definit de criterii, aliniind titlurile și funcțiile din sectorul bugetar.

În acest sens, ținând cont de procesul de negocieri cu donatorilor externi, începând cu trimestrul I 2024, Ministerul Finanțelor urmează să beneficieze de un proces desfășurat de asistență externă pe marginea realizăriii exercițiului de revizuire a sistemului de salarizare în sectorul bugetar, inclusiv ținând de reevaluare a funcțiilor din sectorul bugetar. Exercițiul în cauză urmează a fi definitvat în trimestrul IV 2024, termen stabilit inclusiv conform acțiunii nr. 6 din Hotărârea Guvernului nr. 829/2023 cu privire la aprobarea Planului național de acțiuni pentru aderarea Republicii Moldova la Uniunea Europeană pe anii 2024-2027.

Astfel, implementarea acțiunii nr. 4) din Planul de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii

2019-2024, urmează a fi analizată în contextul procesului de reevaluare sistemică a funcțiilor în sectorul bugetar, în strânsă corealare cu disponibilitățile financiare ale bugetului de stat și în corespunderea cu principiul de sustenabilitate bugetară.

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	Parțial realizat

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

În perioada de raportare Angajații Poliției *(CCCC al INI)* au participat în calitate de formatori la 6 instruiri, fiind instruiți peste 65 de judecători și procurori, peste 20 specialiști în domeniul protecției drepturilor copiilor, după cum urmează:

- la 16.02.2023, 1 angajat a participat în calitate de formator la cursul de instruire „Metodici și tactici de investigare și examinare a cauzelor privind infracțiunile cu caracter sexual comise prin intermediul tehnologiilor informaționale. Aspecte privind abuzul online a minorilor”, organizat de INJ;
- în perioada 28.02-02.03.2023, 2 angajați au participat în calitate de formatori la trainingul „Prevenirea și combaterea exploatării și abuzului sexual asupra copiilor în mediul online”, organizat de CoE în cadrul proiectului „Protecția copiilor împotriva violenței și prevenirea acesteia, inclusiv în mediul online” https://www.coe.int/en/web/chisinau/-/training-for-specialists-in-preventing-and-combating-online-child-exploitation-and-abuse-ocsea-?pk_campaign=newsletter;
- la 10.04.2023, 1 angajat a participat în calitate de formator la seminarul „Particularitățile investigării și judecării infracțiunilor în domeniul informaticii și telecomunicațiilor”, organizat de INJ;
- la 12.04.2023, 1 angajat a participat în calitate de formator la Școală tematică de primăvară: „Metodici și tactici de investigare și examinare a cauzelor privind infracțiunile cu caracter sexual comise prin intermediul tehnologiilor informaționale. Aspecte privind abuzul online al minorilor”, organizată de CI „La Strada”;
- în perioada 02-03.10.2023 și la 13.11.2023, 1 angajat a participat în calitate de formator la cursul de instruire cu tematica: „Metodici și tactici de investigare și examinare a cauzelor privind infracțiunile cu caracter sexual comise prin intermediul tehnologiilor informaționale. Aspecte privind abuzul online al minorilor”, organizat de către CI „La Strada”;
- la 04.12.2023 și la 14.12.2023, 1 angajat a participat în calitate de formator la atelierul „Măsuri de reducere a vulnerabilității fetelor și băieților față de violența din spațiul digital”, organizat de Cancelaria de Stat și CI „La Strada”, cu participarea specialiștilor din domeniul protecției drepturilor copilului.

Totodată, în scopul formării profesionale a personalului responsabil de investigarea infracțiunilor de exploatare sexuală online a copiilor, angajații Poliției au participat în cadrul a 5 cursuri de instruire, fiind instruiți 5 ofițeri:

- în perioada 21-25.02.2023, 1 angajat a participat la cursul de instruire în domeniul utilizării bazei de date internaționale a INTERPOL privind exploatarea sexuală a copiilor *(ICSE)* în Lyon, Franța;
- în perioada 28.02-02.03.2023, 1 angajat a participat la cursul de formare profesională cu genericul „Prevenirea și combaterea exploatării și abuzului sexual asupra copiilor în mediul online”;
- în perioada 09-10.03.2023, 5 angajați au participat la cursul de formare profesională cu genericul „Modalitatea de lucru cu copii victime al abuzului/exploatării sexuale online și/sau trafic de ființe umane”, organizat de ONG „Operation Underground Railroad”;
- în perioada 20-24.03.2023, 1 angajat a participat la cursul online „Investigațiile Abuzului și Exploatării Sexuale a Minorilor” organizat de către BNC Interpol New Delhi;
- în perioada 04-13.10.2023, un 1 angajat a participat la cursul Anual „Combaterea Exploatării Sexuale Online a Minorilor” *(EC3 COSEC)* organizat de către Interpol, Düsseldorf, Germania;

În perioada vizată a fost desfășurată și o vizită de studiu:

- în perioada 04-07.12. 2023, 1 angajat a participat la vizita de studiu privind preluarea bunelor practici de funcționare a serviciilor de raportare a materialelor ce reprezintă abuz sexual asupra copiilor în mediul online, organizată de către „INHOPE”, Amsterdam, Regatul Țărilor de Jos.

În perioada anului 2023 de către subdiviziunea CCCC al INI au fost înregistrate și investigate 31 cazuri de abuz sexual în mediul online asupra copiilor, dintre care:

- art.208/1 *(pornografia infantile)* – 23 cazuri;
- art. 175 *(acțiuni perverse)* – 1 caz;
- art. 177 *(încălcarea inviolabilității vieții personale)* – 2 cazuri;
- art. 173 *(hărțuire sexuală)* – 5 cazuri.

Totodată în perioada de referință de către subdiviziunea CCCC al INI al IGP a fost acordată asistență pentru 4 minori și audierea cu participarea psihologului din cadrul CI „La Strada”.

În anul 2023, potrivit PG pentru comiterea infracțiunilor prevăzute la art. 208[1] din Codul penal al Republicii Moldova a fost înregistrat un număr de 46 de cauze penale *(în 2022 – 39 cauze),* cauze transmise în judecată – 16 *(în 2022 – 33 cauze).*

Au fost adoptate sentințe de condamnare în număr de 20 în privința a 20 de inculpați *(în 2022 – 22 cauze în privința a 22 inculpați).*

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 Poliției), Procuratura Generală.*

În perioada anului 2023 de către subdiviziunea CCCC al INI al IGP a fost înregistrat un caz de ademenire a copiilor în mediul online *(art. 175 CP).*

Procuratura Generală – Pentru comiterea infracțiunilor prevăzute la art. 175[1] din Codul penal al Republicii Moldova *(ademenirea minorului în scopuri sexuale),* în anul 2023, au fost pornite 18 cauze. În instanța de judecată pe această categorie de infracțiune a fost pronunțată 1 sentință de condamnare în privința la 1 persoană.

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

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

Întru realizarea acțiunii în perioada de raport de către IGP al MAI a fost întreprinse următoarele acțiuni:

1. La 07.02.2023, a fost realizată o lecție de informare și sensibilizare în cadrul Liceului „Mihail Sadoveanu” din mun. Chișinău, cu referire la prevenirea și informarea despre securitatea cibernetică, bullying și pornografie infantilă;
2. La 30.03.2023, a fost desfășurată o lecție pe tematica „Siguranța online a copiilor” la Liceul „Socrate” din mun. Chișinău;
3. La 24.10.2023, a fost realizată o lecție de informare în liceul teoretic „Lucian Blaga” din or. Telenești cu tematica: „Prevenire privind abuzul sexual asupra copiilor în mediul online” și „Tipurile de infracțiuni cu utilizarea mijloacelor de plată electronice”;
4. La 24.10.2023, a fost realizată o lecție de informare în liceul teoretic „Adrian Păunescu” din s. Căzănești, r-l Telenești cu tematica: „Prevenire privind abuzul sexual asupra copiilor în mediul online” și „Tipurile de infracțiuni cu utilizarea mijloacelor de plată electronice”;
5. La 25.10.2023, a fost realizată o lecție cu caracter preventiv privind abuzul sexual online asupra copiilor în incinta liceului Internat Republican cu Profil Sportiv din mun. Chișinău;
6. La 10.11.2023 a fost realizată o sesiune de informare și sensibilizare privind securitatea cibernetică în incinta liceului Teoretic Orizont din mun. Chișinău.

Totodată, în scopul promovării siguranței copiilor în mediul online Poliția în cooperare cu CI „La Strada”, organizația „INHOPE”, cu suportul Ambasadei SUA la Chișinău au realizat un șir de acțiuni în vedere instituirii în Republica Moldova a unui Mecanism de raportare a materialelor de abuz sexual asupra copiilor.

Ca rezultat, a fost înființat în RM un instrument de tip Hotline, iar la 23 februarie 2023 a fost semnat Acordul de colaborare dintre Inspectoratul General al Poliției și Centrul International „La Strada”, care la rândul său au fost acceptați ca membri provizorii ai rețelei internaționale INHOPE.

Drept urmare, au fost instruiți atât analiștii care vor primi și cerceta materialele de abuz sexual asupra copiilor în mediul online, cât și ofițerii de poliție delegați pentru acest segment, care vor prelua informațiile, iar după caz vor informa alte organe de aplicare a legii din alte țări.

1. Din 16.05.2023 analiștii site-ului SigurOnline (https://siguronline.md/), care prelucrează informațiile raportate, activează în regim de ICCAM funcțional.

2. La 12 septembrie 2023 a fost desfășurată Conferință de presă cu tematica „Mecanismul național de raportare și înlăturare a materialelor ce reprezintă abuz sexual asupra copiilor" https://igp.gov.md/ro/content/1705-raportari-inregistrate-de-catre-serviciul-national-de-raportare-continutului-ce.

De asemenea, pe pagina oficială a Poliției au fost publicate 5 comunicate privind siguranța copiilor în internet, și 2 participări la emisiuni, 2 interviuri. Astfel, la 07.02.2023, 1 angajat al poliției a participat la o emisiune a TVR Moldova, unde a vorbit despre luna Siguranței în Internet și anume riscurile în mediul online, precum și mobilizarea societății civile, autoritățile, dar și companiile private întru asigurarea unui Internet mai sigur pentru tinerii utilizatori https://tvrmoldova.md/article/c03159df696e68fc/7-februarie-ziua-sigurantei-pe-internet.html.

Potrivit Ministerului Sănătății, complexul de acțiuni privind realizările infrastructurii de securitate cibernetică și informațională ce contribuie la protecția datelor și a utilizării sistemelor de sănătate, cuprinde consolidarea infrastructurii de securitate cibernetică, sensibilizarea, educația și dezvoltarea capacităților de combatere a amenințărilor cibernetice prin instruirea personalului, îmbunătățirea cooperării internaționale și schimbul de bune practici, protejarea datelor sensibile ale pacienților prin implementarea sistemelor actualizate și securizate, modernizarea infrastructurii IT precum și cooperarea interinstituțională.

Strategia de securitate informațională în sectorul sănătății, are ca scop digitalizarea sistemelor informaționale securizate de înaltă calitate orientată spre cetățeni, asigurând o abordare coerentă pentru securizarea infrastructurii informaționale ale datelor personale de sănătate și a Republicii Moldova.

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	Parţial realizat

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

Potrivit raportului MAI, în scopul combaterii fraudelor săvârșite cu utilizarea mijloacelor de plată electronice, Centrul pentru combaterea crimelor cibernetice efectuează permanent schimb de informații cu Departamentele de securitate ale instituțiilor financiare. În acest scop pe parcursul anului 2023 fiind realizate 3 (trei) ședințe operaționale cu reprezentanții băncilor comerciale „Moldindconbank";

„MAIB”, inclusiv și cu participarea conducerii INI și CCCC a IGP. Pe parcursul perioadei de raport MAI nu a semnat careva acorduri.

Procuratura Generală a menționat drept indicatori de progres, încheierea unui Acord de colaborare cu Banca Națională a Republicii Moldova. Totodată, mecanismele de interacțiune interinstituțională pentru schimb sistematic de informații sunt prevăzute în Legea nr.20/2009 privind prevenirea şi combaterea criminalității informatice**.**

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 2023, în cadrul ședințelor operaționale ale IGP cu reprezentanții băncilor comerciale „Moldindconbank”; „MAIB” au fost abordate inclusiv măsurile de securitate în privința ATM-urilor.

Procuratura Generală de comun cu Banca Națională a Republicii Moldova, Inspectoratul General de Poliție urmează să identifice necesitatea efectuării Studiului cu privire la investigarea infracțiunilor generate de ineficiența măsurilor de securitate sporită în privința bancomatelor *(ATM-urilor)* la nivel de hardware și software.

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 tranzacțiile cu card și fără card (card present și 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.*

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

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*.

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.

Drept urmare, prin Ordinul IGP nr. 255 ef. din 19.07.2023, statele de organizare a INI a IGP au fost modificate.

În acest sens, în cadrul CCCC al INI au fost create unități responsabile de monitorizare a spațiului digital/virtual ascuns *(Darknet),* totodată au fost create unități responsabile de domeniului investigării infracțiunilor informatice, în cadrul Direcțiilor Nord și Sud a INI a IGP.

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.

De asemenea, periodic, procurorii specializați participă la instruiri în domeniu pe diverse platforme, inclusiv pe platforma Institutului Național al Justiției.

În anul 2023, SIS a desfășurat cursuri de formare profesională continuă cu tematicile: „Securitatea informațională” și „Conștientizarea amenințărilor cibernetice”, în cadrul cărora au fost instruiți 59 ofițeri de informații.

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.*

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

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

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

Potrivit MAI, la moment, în cadrul Sistemului informațional automatizat „Registrul informației criminalistice și criminologice" sunt supuse evidenței centralizate toate tipurile de infracțiuni, prevăzute de Codul penal, inclusiv infracțiunile în domeniul criminalității informatice.

În cazul apariției unor noi necesități, ajustarea Băncii centrale de date a SIA RICC va fi inițiată de către STI în baza solicitării respective din partea Participantului la Sistem. Pe parcursul perioadei de raportare din partea IGP nu au parvenit careva solicitări/demersuri în acest sens.

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.

Mecanismul de conectare a SIS la banca centrală de date a Sistemului Informațional Automatizat (SIA) „Registrul informațiilor criminalistice și criminologice" este creat și funcțional.

Actualizarea datelor din Registrul informațiilor criminalistice și criminologice privind materialele și cauzele penale instrumentate de CNA pe infracțiuni de corupție relaționate cu cele informatice. Pe parcursul anului 2023, „Registrul informațiilor criminalistice și criminologice" a fost completat de către organul de urmărire penală al Centrului, 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 săvîrşit 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.*

Pe parcursul anului 2023, au fost înaintate propuneri privind elaborarea proiectului Hotărârii de Guvern cu privire la aprobarea conceptului sistemului informațional automatizat „E-Dosar".

Totodată la finele anului 2023, a avut loc avizarea prealabilă a proiectului Hotărârii Guvernului pentru aprobarea Conceptului tehnic al Sistemului informațional „e-Dosar" și a Regulamentului cu privire la organizarea și funcționarea Sistemului informațional „e-Dosar".

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

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

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

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 2023, au fost elaborate 108 comunicate de presă/articole informative plasate pe pagina web oficială, dar și distribuite în mediul online pentru sporirea conștientizării.

De asemenea, au fost plasate 3 ghiduri de informare pe pagina web oficială https://stisc.gov.md/ro/ghiduri și 40 anunțuri/publicații pe rețelele de socializare privind pericolele din spațiul cibernetic și măsurile de protecție ce pot fi luate de către persoanele fizice și juridice, 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.

În același context, au fost distribuite în spațiul public 24 de mesaje tematice și desfășurate două campanii de informare online, cu tematica: „Ziua siguranței pe Internet” și „Săptămâna backup-ului”.

Totodată, pe întreaga perioadă, STISC a distribuit pe rețelele sociale 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.

Distribuirea în spațiul public a informațiilor a avut impact pentru 187,5 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.

În anul 2023, SIS a informat/ notificat autoritățile statului privind amenințările, vulnerabilitățile și riscurile la adresa securității cibernetice, precum:

1. Conducerea Aeroportului Internațional Chișinău *(AIC)* înaintate recomandări pentru anticiparea vulnerabilităților ce țin de gestiunea sistemelor informaționale critice;

2. STISC notificată privind conexiunea unor autorități guvernamentale la domenii *(site-uri)* malițioase;

3. STISC remise 2 notificări privind compromiterea infrastructurii TI guvernamentale;

4. Operatorii infrastructurilor critice notificați privind neadmiterea utilizării produselor software/ hardware fabricate în FR;

5. ASP remise recomandări privind identificarea vulnerabilităților în gestionarea infrastructurilor TI în rezultatul desfășurării de către partenerii externi a activităților de „Threat hunting".

În anul 2023, AGE a continuat să desfășoare acțiuni 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, Agenția de Guvernare Electronică, a lansat în 2023 Campania de informare și educație digitală, prin care se promovează dezvoltarea abilităților de utilizare a serviciilor electronice și sporirea încrederii în instrumentele guvernamentale de interacțiune online.

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.*

Potrivit Hotărârii Guvernului nr. 1028/2023, cu privire la constituirea, organizarea şi funcționarea Agenției pentru Securitate Cibernetică, Agenția pentru Securitate Cibernetică exercită funcția de echipă de răspuns la incidentele cibernetice la nivel național şi cea de punct național unic de contact. Agenția urmează să fie creată pe parcursul anului 2024.

Ofițerii SIS au participat la ședințele de lucru pentru elaborarea/ avizarea cadrului normativ ce reglementează activitatea Agenției pentru Securitate Cibernetică.

Nr *(din Plan)*	**Acțiunea**	**Termenul de implementare**	**Statut**
Pilonul I **Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice**			
11/3	Desfășurarea unor exerciții și antrenamente comune de consolidare a capacităților de reacție 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 raportare, angajații STISC au participat în cadrul a 13 evenimente care au presupus exerciții tehnice, ateliere de instruire și training, în particular:

1. 13-17 februarie 2023, STISC a participat la cursul de instruire privind aplicarea normelor de drept internațional în contextul desfășurării de operațiuni/acțiuni cu caracter ofensiv și/sau defensiv în spațiul cibernetic „International Law of Cyber Operations", Cyber Law International's executive course, Skopje, Republica Macedonia de Nord. Cursul a fost organizat cu suportul OSCE, Ministerul Afacerilor Externe a Regatului Țărilor de Jos și University of Reading.
2. 08-28 februarie 2023, STISC a participat la training-ul, în format online, „Policy Making in a Digital Age", organizat de Japan International Cooperation Agency.
3. 21-23 martie 2023, STISC a participat la cursul „CSIRT Technical Exchange and Training", Munich, Germania. Evenimentul a fost organizat și coordonat de către Software Engineering Institute (SEI) și Biroul de United States Department of State's Cyber and Digital Policy Bureau (CDP).
4. 19-21 aprilie 2023, STISC a participat la exercițiu regional de cooperare în domeniul securității cibernetice, Iași, România. Evenimentul a fost organizat de CyberEast, cu suportul Uniunii Europene.
5. 26-27 aprilie 2023, STISC a participat în cadrul atelierului de lucru, „Comprehensive Defence: Resilience and Resistance" care a prevăzut ședințe plenare cu participarea factorilor de decizie din RM, cât și reuniuni tematice în cadrul Grupului de lucru interdepartamental. Evenimentul a avur loc la Chișinău și a fost organizat de Ministerul Apărării al Republicii Moldova cu participarea experților internaționali.
6. 22-23 mai 2023, STISC a participat la curs ISO/IEC 27001 Foundation, organizat de Fundația Academia de Guvernare Electronică, Estonia, în cadrul Proiectului Moldova Cybersecurity Rapid Assistance.
7. 24-25 mai 2023, STISC a participat la curs ISO/IEC 27005 Foundation, organizat de Fundația Academia de Guvernare Electronică, Estonia, în cadrul Proiectului Moldova Cybersecurity Rapid Assistance.
8. 6-7 iunie 2023, STISC a participat la curs ISO/IEC 27032 Foundation, organizat de Fundația Academia de Guvernare Electronică, Estonia, în cadrul Proiectului Moldova Cybersecurity Rapid Assistance.
9. 8-9 iunie 2023, STISC a participat la training privind incidentele cibernetice, taxonomia și gestionarea crimelor cibernetice în conformitate cu procedurile standard operaționale. Evenimentul a fost organizat de CyberEast, cu suportul Uniunii Europene.
10. 14-16 iunie 2023, STISC a participat în cadrul exercițiului tehnic „Cybersecurity Capacity Building Exercise", organizat de Fundația Academia de Guvernare Electronică, și compania Cybexer, Estonia, în cadrul Proiectului Moldova Cybersecurity Rapid Assistance.

11. 2-6 octombrie 2023, STISC a organizat un program de instruire „Cloud+CompTIA”, instruind cca 30 specialiști IT din cadrul mai multor instituții guvernamentale din Republica Moldova și Ucraina pentru a cunoaște noi soluții de gestionare și securizare a cloud-ului și a-și consolida cunoștințele și competențele în domeniul tehnologiilor cloud și securității cibernetice, contribuind astfel la sporirea rezilienței cibernetice în regiune.

12. 24-27 Octombrie 2023, specialiștii STISC împreună cu reprezentanți ai forțelor de ordine și instituțiilor de drept au participat la un exercițiu regional de cooperare în domeniul criminalității cibernetice, desfășurat în Georgia, sub egida proiectelor CyberEast și iPROCEEDS-2.

13. STISC a organizat, în perioada 23 -27 octombrie 2023, training CompTIA PenTest+, pentru cca 30 funcționarilor publici, specialiștilor din infrastructura critică și profesioniștilor din sectorul privat în domeniul evaluării vulnerabilităților, testării de penetrare și protecției cibernetice. Acțiunea a fost parte integrantă a proiectului EU4Digital: „Cybersecurity EAST”.

În contextul consolidării capacităților de reacție a SIS la atacuri cibernetice, ofițerii SIS au participat la următoarele exerciții:

- „TTX Asses Organize Communicate and React” *(12-13.06.2023);*
- „Cybersecurity Exercise in Moldova” *(14-16.06.2023);*
- „Cybersecurity incident response”.

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.*

În perioada ianuarie – iunie 2023, STISC a organizat și desfășurat în total 4 evenimente, în domeniul securității cibernetice, cu implicarea unui număr total de 470 angajați din cadrul STISC și alte entități guvernamentale, după cum urmează:

1. Atelier de instruire în domeniul securității cibernetice, și anume „Internet of Things - security risks and challenges”. Obiectiv: cunoașterea principalelor concepte ale Internetului lucrurilor, arhitectura sistemului IoT, tipurile de riscuri și vulnerabilități, metode și instrumente de evaluare, și mitigare a riscurilor. Auditoriu țintă: specialiștii și experții IT, și securitate cibernetică. Au participat 80 de angajați din cadrul entităților publice.

2. Exercițiu practic în securitate cibernetică cu tematica „TTX – Assess, Organize, Communicate and React”, în parteneriat cu CRDF Global și Academia Militară „General Mihailo Apostolski”. Obiectiv: îmbunătățirea modului de cooperare inter-instituțională pentru soluționarea incidentelor cibernetice cu impact major, prin schimbul de informații și practici, în vederea creării unui lanț decizional

fiabil, care să asigure în continuare funcționarea unui model stabil. Au participat 30 de angajați din instituții guvernamentale

3. La 1 martie 2023, a fost realizat 1 exercițiu de simulare a unui atac de tip Phishing în cadrul STISC. Scopul: sporirea gradului de conștientizare referitor la aceste tipuri de atacuri cibernetice care pot sustrage datele de acces, precum și responsabilizarea asupra importanței verificării autenticității mesajului care a fost transmis și utilizarea autentificării în doi pași.

4. 3-4 august 2023 STISC în colaborare cu CRDF Global a organizat un atelier de instruire în format hibrid, cu tematica „Inginerie Socială – tehnici de recunoaștere și metode de apărare", la instruire au participat cca 200 de reprezentanți ai instituțiilor din sectorul public din țara noastră.

5. La 11-12 octombrie 2023 STISC a facilitat organizarea unui Dialog strategic în vederea securizării infrastructurii critice a RM. Evenimentul a întrunit 20 oficiali ai instituțiilor guvernamentale împreună cu reprezentanți ai sectorului privat.

În anul 2023 procurori și specialiștii angajați ai Secției tehnologii informaționale din cadrul PG au participat la următoarele ateliere de lucru și instruiri în materie de securitate cibernetică:

1. instruirea în domeniul sistemului de management al securității informaționale – ISO/IEC 27001, 27005 și 27032.
2. reuniunea în domeniul criminalității cibernetice „CyberWeek 2023" organizată de către Serviciul Tehnologia Informației și Securitate Cibernetică, în cadrul Proiectului *„CyberEast"* cu suportul Consiliului Europei.

În anul 2023, ofițerii SIS au participat la 11 ateliere de lucru în domeniul securității cibernetice:

- ședința Grupului de lucru interinstituțional pentru securitatea cibernetică a infrastructurilor critice din Moldova *(19.01.2023);*
- ședința Microsoft Cybersecurity Reference Architecture *(26.01.2023 și 15.03.2023);*
- reuniunea „Resilience Advisory Support Team" (RAST) for Moldova *(31.01.2023 - 02.02.2023);*
- workshop-ul online cu tematica „Utilizarea Inteligenței Artificiale (IA) în investigațiile digitale prin intermediul platformei Hasken" *(02.02.2023);*
- seminarul cu tematica „Increasing cyber resilience: Strengthening the risk and incident management practices as well as the governmental structure", organizat de e-Governance Academy *(16.02.2023);*
- vizita de studiu în orașul Haga, Regatul Țărilor de Jos și în orașul Bruxelles, Belgia, organizată de către „Academia de Guvernare Electronică din Estonia" *(E-Governance Academy)*, în cadrul proiectului „Moldova Cybersecurity Rapid Assistance" *(06 – 10.03.2023);*
- workshop-ul „EUSecureConnect EaP-Black Sea-Central Asia: protecting connectivity infrastructure and improving cyber security" *(14 - 18 martie 2023);*
- cursurile de formare inițială în „Standardul ISO 27001 Information security", „ISO 27005 Analiza riscurilor", „ISO 27032 Securitatea cibernetică *(mai-iunie 2023);*

- cursul online „IoT - Internet of things” *(17 – 18.05.2023);*
- curs „Cloud – based solutions for ensuring Government continuity, Cyber security and Fighting misinformation” *(03.05.2023);*
- curs la „Academia de Guvernare Electronică din Estonia” (E-Governance Academy), în cadrul proiectului „Moldova Cybersecurity Rapid Assistance” *(28.05-03.06 2023).*

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.*

Reieșind din atribuțiile de interacțiune cu instituțiile publice *(efectuarea auditului de securitate cibernetică),* AGE a propus organizarea în cadrul proiectului Moldova Cybersecurity Rapid Assistance a diferitor cursuri specializate, conform necesităților de rigoare, cu certificarea specialiștilor, după caz. Astfel, pe parcursul anului 2023, cu suportul STISC, în cadrul proiectului au fost organizate instruiri tematice pentru specialiștii instituțiilor publice *(ISO27001 / ISO27005 / ISO27032 Foundation),* cu certificarea cunoștințelor și abilităților obținute.

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.

În cadrul MAE anual este angajat, pe bază de contract prestări servicii, Consultantul Expert *(Maxim Catanoi)* pentru implementarea și asigurarea sistemului de securitate informațională. Specialist Certificat EC-Council, Certified Ethical Hacker (CEH) - EC-Council, Certified Security Analyst.

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

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.*

În anul 2023, SIS a elaborat un material didactic privind securitatea cibernetică.

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

Instituția responsabilă: *Agenția Guvernarea Electronică*

În cadrul proiectului Moldova Cybersecurity Rapid Assistance, după caz, cu suportul AGE, pentru angajații instituțiilor publice au fost organizate instruiri tematice în domeniul securității cibernetice, precum: ISO27001 / ISO27005 / ISO27032 Foundation, Inginerie socială – tehnici de recunoaștere și metode de apărare, precum și diferite ateliere de lucru pentru consolidarea capacităților de reziliență cibernetică.

Totodată, prin recomandările prezentate instituțiilor publice în cadrul misiunilor de audit de securitate cibernetică, AGE promovează utilizarea Platformei guvernamentale de instruire la distanță *(mlearn.gov.md),* pe care sunt publicate un cursuri/module dedicate securității cibernetice, pentru diferite categorii de utilizatori *(conștientizare generală, administratori TI, dezvoltatori, manageri).*

Respectiv, în anul 2023 pe platforma MLearn a fost publicat cursul „Siguranța digitală”, care a fost dezvoltat în cadrul proiectului Moldova Cybersecurity Rapid Assistance.

În anul 2023 specialiștii din cadrul CTIF au participat la 3 cursuri de formare:

- ISO/IEC 27001 *(4 angajați);*
- ISO/IEC 27005 *(4 angajați);*
- ISO/IEC 27032 *(4 angajați).*

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.*

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.

În cadrul MAE, în anul 2023, a fost realizată misiunea de audit intern pe orizontală privind protecția datelor cu caracter personal.

În anul 2023, SIS a informat Secretarul general al Guvernului Republicii Moldova referitor la lipsa cadrului legal național orientat spre reglementarea activității mijloacelor de informare în masă în mediul online, inclusiv despre:

- *lipsa reglementărilor de natură să determine statutul entităților virtuale, fără persoană juridică sau identificare cu persoana fizică;*
- *lipsa mecanismelor practice de sancționare (de blocare a resurselor web care conțin informații false, propagandistice și incitatoare) care pot submina securitatea informațională a RM excluzând dispozițiile Comisia pentru situații Excepționale (CSE).*

În cadrul CTIF anual se efectuează testarea vulnerabilităților pentru sistemele informatice gestionate de către CTIF pentru Ministerul Finanțelor și autoritățile administrative din subordinea sa, în conformitate cu Planul pentru efectuarea testelor de vulnerabilitate aprobat de către Directorul CTIF.

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 securității spațiului informațional-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 Informații și Securitate.*

În conformitate cu HG nr. 467/2022, a fost creat Consiliul coordonator pentru asigurarea securității informaționale *(CCASI)*, fiind aprobată componența și

statutul Consiliului. Reieșind din crearea Centrului pentru Comunicare Strategică și Combaterea Dezinformării *(CCSCD),* acesta poate prelua poziția de platformă informațională de comunicare strategică.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
13/4	Elaborarea și organizarea unor cursuri de instruire tematică pentru radiodifuzori, distribuitorii de servicii, formatorii de opinie publică, jurnaliști și ONG-urile de profil cu privire la tehnicile de dezinformare și/sau de informare manipulatorii utilizate pentru prejudicierea securității informaționale a statului	Permanent	Parțial realizat

Instituții responsabile: *Societatea civilă, mass-media*

Ofițerii SIS au participat la 3 evenimente cu reprezentanții instituțiilor de drept și societatea civilă, pe subiecte ce vizează identificarea și prevenirea amenințărilor în spațiul informațional:

- *Atelier de lucru „Consolidarea rezilienței societății civile în contracararea dezinformării în domeniul securității", (Platforma pentru Inițiative de Securitate și Apărare, cu sprijinul Ambasadei Republicii Lituania);*
- *Atelier de lucru privind comunicarea strategică (Cancelaria de Stat, în parteneriat cu NATO);*
- *Training privind securitatea cibernetică pentru specialiștii în comunicare și relații publice (Guvernul Republicii Moldova).*

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul II **Asigurarea securităţii spaţiului informaţional-mediatic**			
14/1	Evaluarea spațiului Internet din perspectiva identificării entităților/ subiecților implicați în producerea și diseminarea conținutului media on-line și a altor intermediari și servicii auxiliare ce au impact pentru securitatea informațională	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 contextul informațiilor prezentate de SIS au fost blocate resurse informaționale finanțate de Federația Rusă *(64 resurse web),* care prezentau riscuri la securitatea națională și care au contribuit masiv la alterarea conținutului informațiilor vehiculate în spațiul public;

În același sens au fost elaborate mai multe studii analitice (remise beneficiarilor legali), cu următoarele tematici:

- *Dezordinea informațională în contextul evenimentelor din 30.06.2023, pe AIC. Rezultat: Înaintarea evaluărilor și recomandărilor;*
- *Profilul Companiei Internaționale de Televiziune și Radio „MIR". Rezultat: Guvernul RM a denunțat acordul privind activitatea „MIR" pe teritoriul național;*

- *Accelerarea campaniei informaționale tendențioase, pe fonul organizării Summit-ului Comunității Politice Europene 2023;*
- *„Operațiunile informaționale pro-Kremlin desfășurate în spațiul informațional al Republicii Moldova”.*
- *Reacții și narative promovate în contextul organizării Adunării Naționale „Moldova Europeană”.*

SIS a realizat acțiuni de competență în raport cu mediile și persoanele care realizează acțiuni de influență în scopul destabilizării a mediului de tineret prin intermediul platformelor de socializare: „TikTok”, „Facebook.com” și „Telegram”.

SIS a identificat și a solicitat blocarea 11 resurse mediatice, care distribuiau pe teritoriul RM informații false, ce incită la ură și război, sau după caz, conțin elemente de dezinformare cu impact asupra securității naționale, și anume: *eadaily.com, bloknot.ru, rubaltik.ru, sputniknews.com, md.sputniknews.com, ro.sputniknews.com, sputniknews.ru, md.sputnik.ru, politnavigator.news, politnavigator.net, news-front.info.*

SIS a remis în adresa beneficiarilor nota analitică privind ilegalitățile unui partid politic la compartimentul publicității online.

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

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

Reprezentanții SIS au participat la 3 ședințe comune cu MJ, în cadrul cărora au fost abordate subiectul ajustării cadrului normativ pe sectorul de referință.

Astfel, SIS a prezentat propunerile instituționale pentru modificarea:

1. *Legii nr. 54/2003 privind contracararea activităţii extremiste;*
2. *Legii presei nr. 243/1994;*
3. *Legii comunicațiilor electronice nr.241/2007;*
4. *Legii nr. 64/2010 cu privire la libertatea de exprimare.*

Consiliul Audiovizualului reglementează doar domeniul audiovizual – TV și Radio, și nu deține dreptul la inițiativă legislativă.

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.*

SIS a elaborat 2 rapoarte de evaluare pe palierul mediatic și extremist, care au fost remise în adresa Consiliului Coordonator pentru Asigurarea Securității Informaționale *(CCASI),* pentru elaborarea proiectelor de acte normative care ar înlătura lacunele depistate și ar reglementa spațiului mediatic online.

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.*

În scopul excluderii posibilității de manipulare a informațiilor pe cazuri de corupție, pe parcursul anului 2023, CNA a asigurat tot suportul tehnic necesar pentru a asigura transparența și accesul la informație, cazurile de corupție investigate sunt publicate pe pagina web oficială.

Publicarea acestor informații pe pagina web oficială contribuie la contracararea manipulării informațiilor. Prin furnizarea accesului direct la informațiile despre cazurile de corupție investigate, se elimină riscul ca aceste informații să fie distorsionate sau manipulate de către părți interesate.

Faptul că CNA oferă acces public la informații despre cazurile de corupție investigație poate contribui la creșterea încrederii publice în instituție și în eforturile sale de combatere a corupției. O astfel de transparență poate consolida încrederea cetățenilor în integritatea și eficacitatea activităților desfășurate de CNA.

În anul 2023, Consiliul Audiovizualului nu a recepționat solicitări din partea Serviciului de Informații și Securitate, a Ministerului Justiției și Centrului Național Anticorupție în vederea elaborării, 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.

Consiliul Audiovizualului, în anul 2023, în contextul aproximării la practicile din UE, a dezvoltat și supus consultărilor publice trei metodologii.

Prin Decizia nr. 219 din 21 iulie 2023, CA a aprobat Metodologia privind constatarea și evaluarea cazurilor de dezinformare în conținuturile audiovizuale.

Metodologia de monitorizare și evaluare a pluralismului audiovizual intern în serviciile media liniare și Metodologia de monitorizare și evaluare a pluralismului audiovizual extern în Republica Moldova *(supuse consultărilor publice prin Decizia nr. 211 din 14 iulie 2023)* urmează a fi aprobate în anul 2024.

Măsura urmează a fi implementată după abordarea subiectului de referință în cadrul Consiliului coordonator pentru asigurarea securității informaționale.

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 2023, SIS a informat Cancelaria de Stat privind unele deficiențe și propuneri de modificări legislative, precum:

- *descrierea noilor noțiuni, calificări/ fapte care pun în pericol securitatea informațională a statului pe dimensiunea de dezinformare/ știri false;*
- *stabilirea statutului juridic al redacțiilor online, publicațiilor periodice online și al agențiilor de presă carte activează în format electronic și difuzează informațiile prin Internet;*
- *reglementarea modului de achiziționare și administrare a domeniului „MD” de către redacțiile, publicațiile periodice și agențiile de presă carte activează în Internet;*
- *stabilirea setului de cerințe pentru genul de activitate în domeniul de editare, persoanelor juridice care activează în format electronic cu interzicerea anonimatului a site-urilor web de știri/ informaționale, care utilizează domeniul „MD” sau alte domenii internaționale: „COM”, „INFO”, „ORG”, „NET” ș.a. care activează în spațiul mediatic autohton.*

În perioada de raport, în adresa CNA nu au parvenit solicitări pentru acordarea suportului respectiv.

Furnizorii privați de servicii media au avut obligația să prezinte Consiliului Audiovizualului și să publice pe propriile pagini web, anual, până la data de 31 martie, un raport de activitate, conform modelului aprobat de CA, pentru anul de activitate precedent. Modelul Raportului de activitate anual al furnizorilor privați de servicii media a fost aprobat de CA prin Decizia nr. 7 din 20.01.2023.

Astfel, întru realizarea atribuțiilor legale privind examinarea, aprobarea/ respingerea rapoartelor anuale de activitate ale furnizorilor privați de servicii media audiovizuale, Consiliul Audiovizualului a adoptat 8 decizii și o Analiză a rapoartelor anuale ale furnizorilor de servicii media audiovizuale de televiziune pentru anul 2022 *(Decizia nr. 191 din 30 iunie 2023),* angajament stabilit în Planul de acțiuni pentru implementarea măsurilor propuse de către Comisia Europeană în Avizul său privind cererea de aderare a Republicii Moldova la Uniunea Europeană (pct. 4.6), aprobat de Comisia Națională pentru Integrare Europeană la 04 august 2022 *(Deciziile nr. 112 din 28 aprilie, nr. 123 din 12 mai, nr. 141 din 19 mai, nr. 154 din*

26 mai, nr. 161 din 09 iunie, nr. 184 din 23 iunie, Decizia nr. 197 din 06 iulie 2023 și Decizia nr. 225 din 28 iulie 2023).

Astfel, CA a aprobat 116 rapoarte anuale de activitate ale furnizorilor de servicii media audiovizuale: TV – 65, Radio – 51; a respins 3 rapoarte anuale de activitate: TV – 2, Radio – 1.

Pentru a asigura transparența proprietății și finanțării furnizorilor privați de servicii media, pe pagina web oficială a Consiliului Audiovizualului au fost publicate 116 rapoarte anuale de activitate ale furnizorilor de servicii media audiovizuale privați.

Totodată, în contextul eforturilor de apropiere de standardele europene vizând transparența proprietății media, Consiliul Audiovizualului a raportat lunar, informațiile necesare pentru completarea și actualizarea bazei de date MAVISE (*Mecanismul european de raportare a informațiilor privind acționarii și proprietarii beneficiari ai furnizorilor de servicii media de televiziune*), gestionată de Observatorul european al audiovizualului.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

SIS a informat Cancelaria de Stat cu referire la lacune de ordin normativ, care generează blocaje în realizarea obiectivelor Strategiei, și anume:

1. Lipsa cadrului legal național orientat spre reglementarea activității mijloacelor de informare în masă în mediul online;

2. Lacune în aplicarea reglementărilor legislative pe segmentul de contracarare a activității extremiste în spațiul informațional.

Conform atribuțiilor prevăzute în regulamentul PG aprobat prin Ordinul Procurorului General nr.33/3 din 03.05.2022, cu modificările ulterioare, PG 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 național, a entității cu competențe de promovare și coordonare a politicilor de securitate informațională într-o societate democratică în funcție de dezvoltarea tehnologiei, raporturile juridice și de altă natură din sectorul societății informaționale la nivel național și internațional (Consiliul coordonator pentru asigurarea securității informaționale): a) identificarea și integrarea componentelor existente cu funcții și atribuții în domeniul cibernetic și mediatic, a autorităților administrației publice locale, precum și a componentelor care vor fi create pe parcurs;	Anul 2019	Realizat

	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		

Instituţia responsabilă: *Serviciul de Informaţii şi 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**			
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

Instituţia responsabilă: *Serviciul de Informaţii şi Securitate.*

Pe parcursul perioadei re raport, MAEIE a valorificat prevederile Acordului RM – UE privind procedurile de securitate pentru schimbul de informații clasificate. MAEIE, împreună cu SIS au depus eforturi *(cu succes)* pentru identificarea companiei și Statului Membru UE – care ar oferi sprijin în procurarea echipamentului necesar pentru gestionarea informației clasificate în cadrul serviciului diplomatic al RM.

Dialogul cu Centrul satelitar al UE *(SatCen)* a fost consolidat. RM a continuat să beneficieze de produse de analiză elaborate de SatCen, inclusiv să recepționeze rapoarte în format digital *(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

Instituţia responsabilă: *Serviciul de Informaţii şi 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**			
17/1	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

Instituţia responsabilă: *Serviciul de Informaţii şi 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**			
17/2	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 2023 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 2023, urmare a solicitării Serviciului European de Acțiuni Externe *(SEAE)*, SIS a completat Chestionarul pe Amenințări Hibride *(AH)*.

Ofițerii SIS au participat la evenimente inter-instituționale care au generat creșterea gradului de conștientizare a fenomenului AH, și anume:

- *a VII-a rundă de consultări Republica Moldova - Uniunea Europeană în domeniul de securitate și apărare (Security situation overview; Hybrid threats activities; Implementation of EU Hybrid risk survey recommendations);*
- *întâlnirea trilaterală NATO-RM-UA pe dimensiunea de contracarare a amenințărilor hibride – „Current hybrid threats, challenges and government response”;*
- *evenimentul „EU Support Hub on internal security and border management in Moldova on countering hybrid threats”, cu prezentarea expertizei SIS la subiect „Republica Moldova în contextul actual de securitate regională și contracararea amenințărilor hibride” și „Strategii de contracarare a amenințărilor hibride: EU, NATO, RM”.*

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
17/5	Efectuarea exercițiilor pentru dezvoltarea capacităților autorităților specializate în combaterea amenințărilor hibride de securitate	Perioada 2020-2024, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În cadrul ședințelor interinstituționale pe platforma MAE, a fost abordat subiectul exercițiilor pentru dezvoltarea capacităților autorităților specializate în combaterea amenințărilor hibride.

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 RM-NATO *(IPAP)* pentru anii 2022-2023, 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.

În ianuarie 2023, la întrevederea ministrului de externe Nicu Popescu cu Directorul Centrului de Excelență NATO Jānis Sārts au fost abordate subiectele privind dezvoltarea cooperării în domeniul comunicării strategice și al diplomației publice, schimbul de bune practici pentru instituționalizarea comunicării strategice și contracararea dezinformării. De asemenea, au avut loc discuții între membrii Parlamentului RM cu reprezentanții Centrului de excelență NATO în februarie 2023.

În perioada 26-28 iunie 2023, au avut loc atelierele de lucru în domeniul comunicării strategice pentru funcționarii publici *(de conducere și execuție)* responsabili de comunicare, în cadrul Programului de dezvoltare profesională NATO-RM.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
18/1	Crearea în cadrul Forțelor Armate a entității responsabile de apărarea cibernetică la nivel național	Perioada 2019-2020, cu verificarea anuală a indicatorilor de progres	Realizat

Instituția responsabilă: *Ministerul Apărării*

Pe parcursul anului 2023, MA a întreprins următoarele acțiuni:

- a lucrat la elaborarea statelor de organizare privind crearea și funcționarea Agenției de apărare cibernetică a Ministerului Apărării *(Centrul de reacție la incidente cibernetice – independent).*

- a lucrat asupra dezvoltării capabilităților de apărare cibernetică și identificării potențialelor cooperări pe domeniu atât din țară, cât și peste hotare;

- a înaintat scrisoarea oficială către oficiul „Federated Mission Networking", NATO, Bruxelles.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
18/2	Consolidarea capacităților de instruire și formare cibernetică prin participarea la exerciții interstatale și internaționale de apărare cibernetică	Perioada 2019-2024, cu verificarea anuală a indicatorilor de progres	Parțial realizat

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

Pe parcursul anului 2023, MA a desfășurat următoarele activități:

- Participarea la cursul „Managementul securității informaționale";
- Participarea delegației AN la seminarul organizat de „Elbyt System LTD" pe domeniul securității informaționale;
- Participarea la Reuniunea privind securitatea cibernetice cu participarea expertilor NATO;
- Participarea reprezentantului MA la vizita de studiu destinată creșterii gradului de conștientizare și contribuție a organizațiilor internaționale la stabilitatea și reziliența cibernetice, Belgia;
- Participarea în cadrul exercițiilor internationale de Securitate cibernetică LockShield 2023, Cyber Man 2023 la București, România.
- Participarea în cadrul forumului Europei de Sud-Est cu genericul: Securitatea
- cibernetică în Europa de Sud- Est Garmish, Germania;
- Participarea la conferința CYCON 2023 destinată discuțiiolor privind conflictele cibernetice testate de evenimentele actuale, Tallin Estonia;
- Participarea la reuniunea inițială a grupului de lucru pentru Securitate cibernetice a infrastructurilor critice din Moldova (CICWG).

MAE remarcă că 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). A fost implementat proiectul „Dezvoltarea capacităţilor de apărare cibernetică ale Forţelor Armate ale Republicii Moldova".

Contracararea amenințărilor hibride, precum și asigurarea securității cibernetice au constituit subiecte discutate cu UE în cadrul celei de-a doua reuniuni a Dialogului la nivel înalt în domeniul politic și de securitate *(23 – 24 martie 2023).*

MAE în colaborare cu Ministerul de Externe al Lituaniei a organizat în RM 2 sesiuni de instruire în perioada 11-12 și 18-19 octombrie cu tematica amenințărilor hibride la sediul MAE, la care au participat angajați ai instituțiilor de forță *(MAI,*

MA, SIS) precum și angajași din cadrul STISC, AGE, CA, CSS, Parlament, MDED, Stratcom și MAE.

În perioada 23-24 noiembrie 2023, MAE a organizat la Chișinău consultările NATO-Ucraina-Moldova pe tema combaterii amenințărilor hibride.

Ofițerii SIS au participat la 16 evenimente internaționale *(ateliere de lucru, instruiri, mese rotunde seminare, conferințe)* în vederea consolidării potențialului de apărare cibernetică.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul III **Consolidarea capacităților operaționale**			
18/3	Identificarea, prevenirea și contracararea factorilor de risc cu potențial informativ-subversiv în adresa apărării cibernetice a Republicii Moldova prin implementarea unui management integrat al spațiului virtual și 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 a sesizat Agenția Națională pentru Reglementarea în Comunicații Electronice și Tehnologia Informației *(ANRCETI)* despre vulnerabilitățile pentru securitatea națională, derivate din ascendența fenomenului *„online SIM”,* atestat pe teritoriul RM.

SIS a informat CNA privind implicarea în activități de corupție a unor factori de decizie din cadrul *SA „MOLDTELECOM”*, manifestată prin trucarea procedurilor de achiziții, contractarea procurărilor de bunuri sau lucrări la prețuri majorate excesiv, care prejudiciază financiar întreprinderea și diminuează nivelul de securitate informațională și cibernetică a acesteia.

Serviciul a sesizat atacuri cibernetice asupra sistemelor informaționale ale instituțiilor medicale fiind informat Ministerul Sănătății despre necesitatea implementării măsurilor suplimentare de asigurare a securității informaționale în cadrul instituțiilor din subordine.

Totodată, în urma evaluării dinamicii atacurilor cibernetice asupra sistemelor informaționale pentru perioada 2020-2023, au fost stabilite tentative de preluare ilegală a datelor cu caracter personal de pe platforma națională *www.programare-vaccinare.gov.md*, realizate din afara țării, prin virusul *„boot”*.

De către SIS au fost analizate implicațiile/ incidentele de securitate cibernetică și tentativele de indisponibilitate a infrastructurii de tehnologie a informației a Comisiei Electorale Centrale. În rezultat, au fost propuse măsurile necesare pentru contracararea finanțării ilicite a partidelor politice și corupției electorale, precum și pentru consolidarea infrastructurii cibernetice electorale.

De asemenea, Serviciul a identificat vulnerabilități și a înaintat propuneri de rigoare cu referință la criptarea sistemelor informaționale din cadrul unor instituții medicale din țară, prin utilizarea diverselor tipuri de „Ransomware”.

SIS a oferit suportul de specialitate în procesul de securizare cibernetică a *Summitului CPE 2024*. Ofițerii SIS participat la asigurarea

securității cibernetice la obiectivele de infrastructură aeronautică din Republica Moldova: ÎS „MoldATSA” și ÎS „Aeroportul Internațional Chișinău”.

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. Astfel, în scopul de a reduce influența informației rău intenționate asupra proceselor decizionale din Republica Moldova și de a dezvolta mijloace de comunicare între stat și cetățean, pe probleme de politică internă și externă a fost adoptată Legea nr. 242/2023 privind Centrul pentru Comunicare Strategică și Combatere a Dezinformării. Prin urmare, în scopul protejării spațiului audiovizual național și a asigurării securității informaționale au fost introduse noțiuni și prevederi noi ce țin de „comunicare strategică, dezinformare, acțiuni de manipulare a informațiilor și ingerințe străine” ș.a. În conformitate cu art. 6 alin. (1) s-a instituit Centrului pentru Comunicare Strategică și Combatere a Dezinformării care are drept scop coordonarea, planificarea și dezvoltarea mecanismelor de identificare, evaluare, prevenire și combatere a dezinformării.

CA a întreprins eforturi de protejare a spațiului audiovizual național, în vederea combaterii dezinformării și a discursului de ură.

I. Prin Decizia nr. 223 din 21.07.2023, Consiliul Audiovizualului a dispus un control privind respectarea art. 17 din CSMA de către distribuitorii de servicii media, ca urmare a retransmisiunii serviciului media audiovizual de televiziune „Союз”, solicitând să fie monitorizați cei cinci cei mai mari distribuitori: „MOLDTELECOM” SA, „ARAX-IMPEX” SRL, „TV-BOX” SRL, „ORANGE MOLDOVA” SA și ÎM „MOLDCELL” SA, în calitate de temei fiind petiția depusă online prin intermediul paginii web oficiale a CA de către Profir Marin cu privire la serviciul media audiovizual de televiziune rusesc „Союз”.

Patru cei mai mari distribuitori de servicii media *(„MOLDTELECOM” SA, „TV-BOX” SRL, „ORANGE MOLDOVA” SA și ÎM „MOLDCELL” SA)* care au retransmis postul de televiziune „Союз”, ce difuza știri din Federația Rusă cu mesaje de susținere a invaziei și agresiunii militare asupra Ucrainei, interzise prin legislație, au fost sancționați cu amenzi a câte 40 000 de lei și au exclus din oferta lor acest post *(Decizia nr. 292 din 22 septembrie 2023).*

II. În UTA Găgăuzia a fost documentată, în cadrul acțiunilor de control ale CA, activitatea fără actele permisive desfășurată de două companii. Acestea retransmit programe audiovizuale cu conținut informativ și informativ-analitic din

Federația Rusă și Belarus, precum și serviciul media de televiziune „Первый народный” fără licență de emisie eliberată de autoritatea de reglementare.

Astfel, în urma controalelor de identificare a activității de retransmisiune a posturilor de televiziune fără actul permisiv *(autorizația de retransmisiune)* emis de Consiliul Audiovizualului, au fost sancționați:

- „Oguzsatlink” SRL, prin Decizia nr. 199 din 06 iulie 2023: cu amenzi în mărime de 69 000 de lei pentru retransmisiunea serviciilor media audiovizuale fără autorizație de retransmisiune și pentru încălcarea art. 17 alin. (4) lit. a) din CSMA; prin Decizia nr. 344 din 27 octombrie 2023, cu amenzi în mărime de 130 000 de lei pentru comiterea repetată a încălcărilor privind retransmisiunea serviciilor media audiovizuale fără autorizație de retransmisiune și a art. 17 alin. (4) lit. a) din CSMA;
- „ILK HALK TELEVIZIONU” SRL, prin Decizia nr. 199 din 06 iulie 2023, cu amenzi în mărime de 88 000 de lei pentru retransmisiunea serviciilor media audiovizuale fără autorizație de retransmisiune, pentru încălcarea art. 17 alin. (4) lit. a) din CSMA și pentru transmisiunea serviciilor media audiovizuale (serviciul media audiovizual de televiziune „Первый народный”) fără licență de emisie; și prin Decizia nr. 344 din 27 octombrie 2023, cu amenzi în mărime de 160 000 de lei pentru comiterea repetată a încălcărilor privind retransmisiunea serviciilor media audiovizuale fără autorizație de retransmisiune, a art. 17 alin. (4) lit. a) din CSMA și pentru transmisiunea serviciilor media audiovizuale *(serviciul media audiovizual de televiziune „Первый народный”)* fără licență de emisie.

Pentru activitate ilegală, CA a aplicat sancțiuni în sumă totală de 447 000 lei și a sesizat autoritățile statului în această privință.

În anul 2023, SIS a avizat proiectul de Lege privind Centrul pentru Comunicare Strategică și Combatere a Dezinformării și privind modificarea unor acte normative.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În anul 2023, SIS a avizat proiectul de Lege privind Centrul pentru Comunicare Strategică și Combatere a Dezinformării și privind modificarea unor acte normative.

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

Instituția responsabilă: *Serviciul de Informații și Securitate.*

În perioada de referință, SIS a informat autoritățile responsabile cu referință la vulnerabilitățile spațiului informațional național, cu înaintarea recomandărilor și propunerilor de rigoare.

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

Instituția responsabilă: *Serviciul de Informații și Securitate*

În anul de referință, prin Ordinului MAI nr.617/ 2023 a fost instituit Grupul de lucru din care face parte SIS, care are ca scop elaborarea proiectelor de acte normative care ar reglementa identificarea, desemnarea și protecția infrastructurilor critice.

Reprezentanții SIS au participat la 7 ședințe ale Grupului de lucru creat pentru elaborarea și aprobarea actelor normative privind identificarea, desemnarea și protecția infrastructurilor critice.

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

Instituția responsabilă: *Serviciul de Informații și Securitate*.

În perioada de raport, SIS a desfășurat 5 teste antiteroriste la obiectivele infrastructurii critice naționale. Despre rezultatele testelor realizate, au fost informați beneficiarii legali.

Serviciul a realizat schimbul de informații cu 17 operatori ai obiectivelor infrastructurii critice.

Totodată, SIS a inițiat procedura de aprobare a 5 planuri de securitate ai agenților aeronautici, operatorilor aeroportuari, operatorilor aerieni înregistrați în RM și furnizorilor de servicii de navigație aeriană.

În ianuarie 2023 – MAEIE a colectat, sintetizat/elaborat și transmis în adresa Serviciului European de Acțiune Externă *(SEAE)* răspunsurile la Chestionarul privind Amenințările Hibride (*EU Hybrid Risk Survey*), document cuprinzător, care abordează riscurile și vulnerabilitățile ce țin de domeniul hibrid, securitatea energetică și protejarea infrastructurii critice. Ca rezultat al acestui exercițiu, SEAE a evaluat textul răspunsurilor transmise de către RM și a remis în adresa MAEIE – recomandări prealabile, inclusiv la subiectul măsurilor menite să contribuie la îmbunătățirea protecției infrastructurii critice.

MAEIE a participat la reuniunile interinstituționale ale proiectului UE „Moldova Cyber Rapid Assistance”, în cadrul cărora s-a discutat inclusiv

armonizarea legislației naționale la Directiva UE – CERT – Reziliența Entităților Critice.

În octombrie și decembrie 2023 MAEIE a participat la reuniunile interinstituționale ale proiectului UE „Moldova Cyber Rapid Assistance", în cadrul cărora s-a discutat inclusiv armonizarea legislației naționale la Directiva UE – CERT – Reziliența Entităților Critice.

În perioada 26-27 octombrie 2023 MAEIE a participat la reuniunile interinstituționale organizate cu ocazia încheierii fazei I a Proiectului de asistență a României pentru consolidarea capacităților Republicii Moldova în domeniile securității cibernetice și rezilienței infrastructurii critice.

Portivit MF, planul pentru efectuarea testelor de vulnerabilitate 2023 a fost aprobat la data de 31.05.2023. Nivelul de realizarea a planului se raportează către Comisia de securitate cibernetică din cadrul CTIF.

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.*

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**			
21/2	Raportarea din partea instituțiilor statului cu competențe în domeniu către Serviciul de Informații și Securitate a informațiilor privind starea de risc la adresa securității informaționale.	Perioada 2020-2022, cu verificarea anuală a indicatorilor de progres	Parțial realizat

Instituția responsabilă: *Autoritățile administrației publice*

Pe parcursul anului 2023 în adresa SIS nu au parvenit rapoarte privind starea de risc la adresa securității informaționale.

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

Instituții responsabile: *Autorităţile administraţiei publice, Consiliul Audiovizualului, Ministerul Dezvoltării Economce și Digitalizării, Ministerul*

Apărării, Ministerul Afacerilor Interne, Procuratura Generală, Serviciul de Informaţii şi Securitate, organizaţiile neguvernamentale.

În cadrul MAI, în perioada 27-30.08.2023 a fost organizat cursul de formare continuă cu genericul „Prevenirea și cercetarea infracțiunilor informatice și a celor conexe” pentru 20 de funcționari publici cu statut special din cadrul MAI. Totodată, tema de referință s-a studiat și la Modulul „Securitatea cibernetică” din cadrul programului de formare managerială de nivelul I-management de bază. În acest context, în perioada de referință au fost organizate 6 cursuri de formare managerială de Nivelul I-management de bază, unde au fost instruiți 267 de funcționari publici cu statut special.

În cadrul modulului de instruire cu tematica *„Securitatea informațională*”, SIS a realizat testarea și evaluarea nivelului de pregătire și cunoaștere a ofițerilor de informații în domeniul igienei cibernetice.

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

Instituția responsabilă: *Autorităţile administraţiei publice*

În perioada de raportare, ofițerii SIS au participat la următoarele cursuri/ treninguri în domeniul securității informaționale:

- *atelierul de lucru „National Security” (organizat de PDP NATO), cu tematica „problematicile/ asimilarea bunelor practici conexe formulării și implementării politicilor publice”;*
- *treninguri/ workshop-uri cu tematica implementării documentelor de politici, organizate de către Serviciul CSS;*
- *treningul „Foreign Information and Manipulation interference” (pe dimensiunea amenințărilor la adresa spațiului informațional: propagandă, manipulare, factcheking, precum și cyber-analysis: analiza atacurilor de tip DDoS), organizat de către misiunea EUPM Moldova.*

În anul 2023, Serviciul Audit Intern al MAE a participat la instruiri in domeniul Managementul Securității Informaționale conform ISO 27001, ISO 27002.

CTIF a desfășurat în anul 2023 pentru angajații din cadrul Ministerului Finanțelor cursuri de instruire cu tematica Securitatea informațională, după cum urmează:

- 26.04.2023, „Securitatea informațională”, 3 ore, on-line, 87 persoane;
- 02.11.2023, „Securitatea informațională și politica de protecție a datelor cu caracter personal”, 3 ore, on-line, 85 persoane.

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

Instituția responsabilă: *Autorităţile administraţiei publice*

În perioada de referință 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**			
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 anul 2023, SIS a elaborat și implementat un program de instruire, structurat în 8 module ce țin de: *„Securitatea informațională”*. În cadrul programului au fost instruiți 40 ofițeri de informații.

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

Instituția responsabilă: *Autorităţile administraţiei publice*

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*

În anul 2023, MAE nu a recepționat nici-un proiect de acord internațional ce s-ar referi la conceptul de „armă informațională”.

În perioada de raport, ofițerii SIS au participat la ședințe, conferințe internaționale, precum și cursuri de instruire ce vizează nemijlocit subiectul AH în spațiul informațional, după cum urmează:

- *Seminar pe tematica „Increasing cyber resilience”, organizat sub egida UE;*
- *Vizită de studiu în cadrul proiectului „Moldova cyber security Rapid Assistance Project”;*
- *Workshop „EU Secure Connect EaP Black Sea- Central Asia: protecting connectivity infrastructure and improving cyber security”;*
- *Curs de instruire organizat de MAI în parteneriat cu UNICRI pe subiectul „Dezinformarea și combaterea știrilor false”;*
- *Conferințe e-Government pe tematica „Digital Innovation as Catalyst for Social Change” și „CyCon 2023”;*
- *Curs pe tematica „Cybercrime Investigator”, organizat sub egida INTERPOL;*
- *a 18-ea întâlnire a comitetului de conducere al Platformei NATO MISP (Malware Information Sharing Platform);*
- *Instruire „Training session on cyber incident and cybercrime taxonomy and handling”.*
- *Vizita de lucru la compania de telecomunicații „Secunet”, organizată de MAE;*
- *Webinar „Cyber Threats and Trends”, organizat sub egida INTERPOL;*
- *Întrevedere în cadrul Proiectului RoAid în domeniul securității cibernetice și protecției infrastructurii critice;*
- *a VI-a sesiune a ONU privind elaborarea convenției cibernetice, organizat de către DGPI a MAI sub egida INTEROL.*

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	Parțial realizat

Instituția responsabilă: *Autorităţile administraţiei publice*

La 13 iunie 2023, Republica Moldova s-a aliniat pentru prima data la un regim orizontal autonom de sancțiuni cibernetice, și anume la măsurile restrictive ale UE împotriva atacurilor cibernetice care reprezintă o amenințare la adresa UE sau a statelor sale membre. Acest regim de sancțiuni are drept scop să prevină, să descurajeze și să răspundă la comportamentul răuvoitor continuu și în creștere în spațiul cibernetic.

În perioada de raport, în cadrul SIS a fost ajustat cadrul normativ intern prin aprobarea:

- *Politicii de securitate a sistemelor informaționale ale Serviciului de Informații și Securitate al RM;*

- *Procedurii de evaluarea riscurilor pentru sistemele informaționale ale Serviciului de Informații și Securitate al RM;*

- *Regulamentului privind management informației în format electronic în cadrul sistemelor informaționale ale Serviciului de Informații și Securitate al RM.*

În conformitate cu bunele practici internaționale din domeniu, în partea ce ține de implementarea securității informaționale în cadrul Serviciului Fiscal de Stat, prin Ordinul SFS nr. 251 din 14.07.2023, a fost actualizată și aprobată Politica de securitate informațională a Serviciului Fiscal de Stat.

Totodată, în scopul asigurării securității informaționale în cadrul Serviciului Fiscal de Stat, au fost aprobate:

- *Regulamentul privind prelucrarea și protecția datelor cu caracter personal din cadrul Serviciului Fiscal de Stat (Ordinul SFS nr. 39 din 27.01.2020);*

- *Politica internă privind securitatea cibernetică a Serviciului Fiscal de Stat (Ordinul SFS nr. 612 din 13.12.2021).*

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
25/1	Crearea/ implementarea cadrului de cooperare interinstituțională 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.*

În perioada de raportare, MA raportează următoarele rezultate:

- Întrevederea general maiorului W. Hartman – Comandant al Forței de misiune Națională pe materie cibernetică al SUA cu factorii de decizie ai Ministerului Apărării și Marelui Stat Major al Armatei Naționale, privind colaborarea AN pe domeniul securității și apărării cibernetice;

- Elaborarea, consultarea instituțională și pregătirea materialelor pentru consultarea insterinstituțională a proiectului Acordului între Ministerul Apărării al Republicii Moldova și Ministerul Apărării Naţionale al României privind colaborarea în domeniul comunicațiilor, tehnologiilor informaționale, asigurării securității și apărării cibernetice.

Pe parcursul anului 2023, STISC a participat la 6 evenimente, în vederea dezvoltării naționale și internaționale, plus semnarea unui Memorandum cu echipa CERT-UA.

1. 01-02.02.2023 I.P. STISC a găzduit reuniunea privind securitatea cibernetică, la care au participat echipa de experți Resilience Advisory Support Team *(NATO).*

2. „Digital Innovation as Catalyst for Social Change”, în cadrul căreia au fost abordate ultimele tendințe în domeniul transformării digitale, cu impact semnificativ asupra guvernării și societății, în ansamblu.

3. Cycon-2023 „Meeting Reality” la care au fost discutate aspectele de politici, strategii, cadrul legal și ultimele inovații tehnologice, cele precum Inteligența Artificială, care vin să schimbe considerabil evoluția conflictelor din spațiul cibernetic, părțile implicate și tacticile utilizate.

4. „Area of Cybersecurity and Workforce Development Programs”, cu scopul realizării schimbului de experiență privind bunele practici în domeniul securității cibernetice, abordarea priorităților și nevoilor Republicii Moldova în acest sens, prezentarea strategiei de viitor asupra securității cibernetice și discutarea subiectelor concentrate pe programele educaționale în domeniul securității cibernetice.

5. Noiembrie 2023 STISC a participat la conferința cu genericul „Ziua Securității Cibernetice: Reziliența Cibernetică, baza securității Regionale și Naționale” (Cyber Defence Day: Cyber Resilience, the keystone of Regional and National Security)”, ce a avut loc la Ministerul Apărării.

6. 5 decembrie 2023, directorul STISC a participat la reuniunea anuală a punctelor naționale de contact ale Inițiativei Consolidării Capacităților de Apărare (DCBI) din cadrul NATO.

Potrivit PG, instruirea adresată angajaților cu atribuții de investigare și urmărire penală, procurorilor, judecătorilor, s-a realizat conform Planului de activitate la formare inițială și continuă pentru procurori și judecători în cadrul Institutului Național de Justiție.

Tematicile care țin de securitatea informației și combaterea crimelor cibernetice sunt incluse în planurile modulare ale Institutului Național de Justiție de formare continuă a procurorilor și judecătorilor. Mai este întocmit și planul modular de formare a consultanților procurorilor, care, la fel sunt beneficiari ai instruirii în cadrul Institutului Național de Justiție.

În luna iulie, a fost inițiată crearea platformei de coordonare interinstituțională cu privire la cooperare cu Misiunea EUPM. Scopul platformei este de a asigura eficient și calitativ schimbul de informații dintre EUPM și instituțiile naționale – APRM/Centrul pentru Comunicare Strategică și Combatere a Dezinformării, MAEIE, MAI, SIS, MDED, STISC. Prima reuniune a platformei a avut loc la data de 6 septembrie 2023, iar a doua reuniune – la data de 23 noiembrie 2023.

Ofițerii SIS au participat la:

- *3 ședințe ale Grupului de lucru pentru securitatea cibernetică a infrastructurilor critice din Moldova (CICWG), organizate cu suportul USAID;*
- *evenimentul privind implementarea cadrului de cooperare interinstituțională pe domeniul apărării cibernetice organizat în cadrul MA al RM;*
- *cursul de instruire privind taxonomia și gestionarea incidentelor cibernetice și a criminalității cibernetice, organizat în cadrul proiectului comun al Uniunii Europene și al Consiliului Europei, „CyberEast”.*

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 Dezvoltării Economice și Digitalizării, Serviciul Tehnologia Informației și Securitate Cibernetică, Procuratura Generală, Ministerul Afacerilor Interne.*

În anul de raportare, Ministreul apărării a realizat următoarele acțiuni:

- Participarea la ședința de lucru cu echipa de experți NATO pe proiectul Defence Capability Building Initiative *(DCBI)* „Antidronă” și „Punctele de comandă mobile”;
- Participarea la vizita de lucru a echipei de experți EPF;
- S-a realizat aderarea Centrului de Reacții la Incidente Cibernetice, la platforma Trusted Introducer.

MAEIE este parte a procesului de negociere și pregătire pentru semnarea Acordului dintre RM și UE privind statutul misiunii de parteneriat a UE în Moldova *(EUPM Moldova).* Misiunea EUPM are drept obiectiv consolidarea rezilienței sectorului de securitate al RM în domeniul gestionării crizelor și al amenințărilor hibride, inclusiv în ceea ce privește securitatea cibernetică și contracararea acțiunilor străine de manipulare a informațiilor și a ingerințelor străine.

Prin Hotărârea Guvernului nr. 857 din 08.11.2023 a fost dispusă inițierea negocierilor asupra proiectului Acordului dintre Ministerul Apărării al Republicii Moldova şi Ministerul Apărării al Republicii Franceze cu privire la cooperarea în domeniul apărării, nivelul căruia a fost ridicat ulterior

În toamna 2023, EUPM a elaborat o listă de 18 proiecte și activități *(de tip train&equip, workshops, study trips, scenario exercises, etc.),* care a fost aprobată la Bruxelles și care urmează a fi implementate de către EUPM în parteneriat cu instituțiile beneficiare.

Experții din cadrul Resilience Advisory Support Team (RAST) NATO au distribuit raportul elaborat cu recomandări în 8 domenii critice, inclusiv securitate cibernetică. Acesta a fost distribuit ministerelor și instituțiilor naționale și transmis UEpentru examinarea posibilităților de acordare a asistenței în implementare.

De asemenea, MAEIE a coordonat procesul de elaborare a Raportului național privind implementarea IPAP în anul 2023, elaborând totodată și Hotărârea Guvernului nr. 993/2023 prin care IPAP a fost extins și pentru anul 2024. Ulterior, va fi elaborat și aprobat Programul Individual al Parteneriatului (ITPP) Republica Moldova-NATO pentru anii 2025-2028.

Ofițerii SIS au participat la ședința Consiliului de coordonare al Platformei „NATO Malware Information Sharing Platform”.

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	Parțial realizat

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

În anul de referință, SIS a semnat un Acord de cooperare cu o companie internațională specializată în domeniul securității și apărării cibernetice.

SIS, de comun cu partenerii de dezvoltare, a inițiat un proiect de implementare a unui „Security Operation Center” (SOC).

Totodată, SIS a semnat un Acord de colaborare în domeniul securității cibernetice cu ÎS „Aeroportul Internațional Chișinău”.

MAEIE este parte a procesului de negociere și pregătire pentru semnare a Acordului dntre RMși UEprivind statutul misiunii de parteneriat a UE în Moldova *(EUPM Moldova).* Misiunea EUPM are drept obiectiv consolidarea rezilienței sectorului de securitate al RM în domeniul gestionării crizelor și al amenințărilor hibride, inclusiv în ceea ce privește securitatea cibernetică și contracararea acțiunilor străine de manipulare a informațiilor și a ingerințelor străine.

Semnarea Acordului SOMA EUPM a avut loc pe data 29 septembrie 2023 la Chișinău.

Prin Hotărârea Guvernului nr. 857 din 08.11.2023 a fost dispusă inițierea negocierilor asupra proiectului Acordului dintre Ministerul Apărării al Republicii Moldova şi Ministerul Apărării al Republicii Franceze cu privire la cooperarea în domeniul apărării, nivelul căruia a fost ridicat ulterior.

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	Parțial realizat

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

Întru realizarea acțiunii în perioada 28-29.11.2023, un angajat al IGP a participat la cursul de instruire „Europol Malware Analysis Solution Workshop *(EMAS)”*organizat de către OEP Europol, la București, România.

Potrivit PG, consolidarea mecanismelor de cooperare internațională între autoritățile statului cu atribuții în combaterea criminalității informatice și organismul internațional specializat EMAS *(Europol Malware Analysis Solution)* al EUROPOL urmează a fi instituite în perioada următoare.

La 24.10.2023 partea italiană a transmis proiectul Acordului dntre Guvernul Republicii Moldova şi Guvernul Republicii Italiene cu privire la cooperarea în materie de securitate, care prevede inclusiv cooperarea în domeniul combaterii criminalității cibernetice.

La 01.11.2023, în scopul demarării procedurilor interne necesare pentru inițierea negocierilor, MAI a remis spre avizare proiectul Acordului între Guvernul Republicii Moldova şi Cabinetul de Miniştri al Ucrainei privind cooperarea în domeniul combaterii criminalităţii organizate, care prevede inclusiv cooperarea în domeniul combaterii infracțiunilor informatice. MAEIE a avizat favorabil proiectul de tratat la 22.11.2023.

La 16.11.2023 MAI a remis spre avizare proiectul Acordului dntre Guvernul Republicii Moldova şi Guvernul Republicii Turkmenistan privind cooperarea în domeniul combaterii criminalității organizate, care prevede inclusiv cooperarea în domeniul combaterii infracțiunilor informatice. MAEIE a avizat favorabil proiectul de tratat la 01.12.2023.

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 2023 de către subdiviziunea CCCC al INI al IGP au fost examinate în Sistemul Informațional „Protecția Copiilor” pe c/p pornite peste 68 dispozitive de stocare a datelor, fiind depistate și excluse din circuit în rețeaua Internet peste 183 mii de imagini foto și 5 mii fișiere video cu conținut de pornografie infantilă.

Au fost examinate 767 fișiere cu imagini și video în baza de date ICSE a OIPC Interpol, pentru stabilirea apartenenței la categoria pornografiei infantile.

Mecanismul respectiv îl utilizează, conform competenței instituționale pe cauzele penale din domeniu Secția combatere trafic de ființe umane a Procuraturii Generale. La data de 14.03.2019, de către Consiliul Superior al Procurorilor a fost aprobată participarea a 2 procurori din cadrul Procuraturii Generale în cadrul grupului de lucru constituit pentru elaborarea lucrării științifice cu titlul – „Compendiu de norme juridice internaționale și naționale corespunzătoare în domeniul exploatării sexuale și abuzului sexual al copiilor cu utilizarea tehnologiilor informaționale și de comunicare *(ESACTIC)”,* dezvoltată în cadrul proiectului „Ensuring Self Sexual Assault Victims To Adequate And Social Protection”, implementat de Centrul Internațional „La Strada” în cooperare cu Biroul INL al Ambasadei SUA în Republica Moldova.

În cadrul proiectului au fost dezvoltate instrumente și metode de identificare

a victimelor, inclusiv prin utilizarea Sistemului informațional automatizat.

În anul 2023 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 Poliției), Procuratura Generală.*

Fiind punct de contact 24/7 pe Convenția privind criminalitatea informatică și G 7 24/7, subdiviziunea CCCC al INI al IGP asigură și recepționează solicitările privind asistențe imediate pentru investigațiile referitoare la infracțiunile informatice.

Astfel, pe parcursul anului 2023 au fost recepționate prin puncte de contact 24/7 pe Convenția privind criminalitatea informatică:

- cereri de conservarea datelor parvenite: 10 *(5 US Departament, 1 Canada, 2 Franța, 1 Italia, 1 Germania);*
- cereri de conservarea datelor expediate: 1 *(Armenia);*
- primite răspunsuri: 1 *(Armenia);*
- solicitări recepționate: 1 *(Ucraina);*
- transmise răspunsuri: 1 *(Ucraina);*
- transmise solicitări: 2 *(Rusia, Ucraina).*

În anul 2023, Procuratura Generală, a examinat mai multe comisii rogatorii inclusiv 22 privind infracțiunile informatice sau legate de utilizarea de sisteme informaționale, care au parvenit de la autoritățile competente din: Armenia, Austria, Cehia, Danemarca, Elveția, Germania, Italia, Lituania, SUA, Polonia, România, Federația Rusă, Slovenia.

Prin intermediul punctului de contact 24/7 au fost examinate 26 cereri de conservare a datelor informatice: SUA, Ucrainei, Franței, Germaniei, Italiei, Elveției, Marii Britanii, Cehiei, Bulgariei și Belarusului. Autoritățile Republicii Moldova pe parcursul anului 2023 au solicitat asistență prin intermediul punctului de contact 24/7 – 1 singura dată.

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.*

Întru realizarea acțiunii la 20.06.2023, un angajat al IGP a participat la workshop-ul online de prezentare a proiectului „GRACE" privind elaborarea unei soluții de interacțiune a organelor de drept la nivel european în gestionarea rapoartelor NCMEC al SUA.

Executarea punctului dat ține de competența Secției combatere trafic de ființe umane a Procuraturii Generale. Ca rezultat a Generalizării anuale a infracțiunilor în domeniul informatic și de telecomunicații, prin care sa depistat o creștere a infracțiunilor de pornografie infantilă, Procuratura Generală urmează să intensifice dezvoltarea parteneriatelor existente cu NCMEC *(Centrul Național al SUA privind Copiii Dispăruți și Exploatați)* și aderarea la alte inițiative similare.

Nr *(din Plan)*	Acțiunea	Termenul de implementare	Statut
Pilonul IV **Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale**			
26/5	Dezvoltarea unor parteneriate în scopul identificării, blocării, sechestrării şi confiscării produselor şi a instrumentelor provenite din infracţiunile transfrontaliere	Anul 2021, cu verificarea anuală a indicatorilor de progres	În proces de realizare

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

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**			
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.*

În perioada de referință angajații IGP au participat în cadrul mai multor evenimente internaționale, după cum urmează:

- în perioada 16-18.01.2023, 1 angajat a participat la evenimentul de lansare a proiectului AG-CYBER *(CPORT)* în Amsterdam, Regatul Țărilor de Jos;
- în perioada 30-31.01.2023, 2 angajați au participat la Conferința internațională despre xenofobie și rasism comise prin sisteme informatice, organizat de către Consiliul Europei în cooperare cu Președinția islandeză a Comitetului de Miniștri al Consiliului Europei;
- în perioada 30.01-03.02.2023, 1 angajat a participat la cea de-a 37-a reuniune a Comitetului Părților al Convenției Consiliului Europei privind protecția copiilor

împotriva exploatării sexuale și abuzului sexual *(Comitetul Lanzarote)* în Strasbourg, Franța;

- în perioada 31.01-01.02.2023, 12 angajat a participat la Reuniunea privind securitatea cibernetică împreună cu experții NATO, în scopul întreprinderii acțiunilor pentru implementarea Planului Individual de Acțiuni al Parteneriatului Republicii Moldova-NATO *(IPAP);*
- la 07.03.2023, 1 angajat a participat la cea de a 11-a Reuniune a Grupului de lucru INTERPOL privind combaterea criminalității financiare transnaționale, ședință pre-operațională a Operațiunii „First Light" *(online);*
- în perioada 27-29.03.2023, 1 angajat a participat la conferința cu genericul „Țările SEPCA în lupta împotriva criminalității cibernetice" organizată cu susținerea Oficiului poliției criminală al Austriei *(BK)* și proiectul iPROCEEDS-2 în Banja Luka, Bosnia și Herțegovina;
- în perioada 28-31.03.2023, 1 angajat a participat la reuniunea utilizatorilor soft-ului „Aviator" și seminarului „Peer to Peer", organizate sub egida organizației INHOPE, în Bruxelles, Regatul Belgiei;
- în perioada 17-20.04.2023, 1 angajat a participat la atelierul de lucru internațional pe segmentul prevenirii fraudelor online, care este parte componentă a acțiunii operaționale *(OA 7.1)* Prevention in Online Fraud din cadrul Planului operațional de acțiuni EMPACT, aferent schemelor de fraudă online *(OAP OFS)* în Regatul Belgiei, Bruxelles;
- la 17.05.2023, 1 angajat a participat la Conferința online privind acțiunile pregătitoare pentru organizarea celei de a 9 ediție a operațiunii internaționale European Money Mule Action *(EMMA9),* Interpol;
- în perioada 24-25.05.2023, 4 angajați au participat la Reuniunea regională privind cooperarea financiară, organizată în cadrul proiectului comun al Uniunii Europene și al Consiliului Europei, CyberEast;
- în perioada 24-26.04.2023, 1 angajat a participat la cea de-a 9-a Conferință privind valuta virtuală în Haga, Olanda;
- în perioada 25-28.04.2023, 2 angajați au participat la Conferința internațională organizată de INHOPE în Malta, Sf. Julian;
- la 14.06.2023, 1 angajat a participat la cea de-a 12 Reuniune a Grupului de lucru Interpol privind combaterea criminalității financiare transnaționale. Ședința de concluzionare a Operațiunii „First Light" 2023;
- în perioada 25.06-01.07.2023, 1 angajat a participat la Reuniunea internațională a grupului operativ privind coordonarea cazurilor de infracțiuni violente împotriva copiilor, organizată de către Biroul Federal de Investigații *(FBI)* al Departamentului de Justiție al Statelor Unite, în Portugalia, Lisabona;
- în perioada 27-28.06.2023, 1 angajat a participat la cea de-a 28-a reuniune plenară a Comitetului privind criminalitatea informatică *(T-CY)* organizată cu suportul Consiliului Europei, la Strasbourg, Franța;
- în perioada 24-29.09.2023, 1 angajat a efectuat o vizită de studiu în cadrul proiectului „Asistență rapidă în domeniul securității cibernetice din Moldova *(CRA),* la Tallinn, Estonia;

- în perioada 25-29.09.2023, 1 angajat a participat la cea de-a 39 reuniune plenară a Comitetului Lanzarote, organizată de către Consiliul Europei, la Srasbourg, Franța;
- în perioada 10-12.09.2023, 1 angajat a participat la conferința internațională cu genericul „Empact asupra crimelor cibernetice" în or. Sofia, Bulgaria și este finanțat prin Fondul pentru Securitate Internă;
- în perioada 26-29.09.2023, 1 angajat a participat la Conferința „ Aviator" și Forumul privind schimbul de date, evenimente organizate sub egida rețelei globale de combatere a abuzurilor sexuale asupra copiilor online *(INHOPE)*, Amsterdam, Olanda;
- la 16.11.2023, 1 angajat a participat la Conferința internațională cu genericul „Cyber Defence Day: Cyber Resilience, the Keystone of Regional and National Security;
- în perioada 21-23.11.2023, 1 angajat a participat la Conferința SIRUS 2023, privind accesul transfrontalier la dovezi electronice, care a avut loc online;
- în perioada 13-15.12.2023, 2 angajați au participat la Conferința de încheiere a proiectului regional comun al Consiliului Europei și Uniunii Europene „CyberEast: Acțiunea privind criminalitatea cibernetică pentru reziliența cibernetică în Regiunea Parteneriatului Estic și Conferința „Octopus: privind cooperarea împotriva criminalității cibernetice", la București, România;
- la 18.12.2023, 1 angajat a participat la Conferința cu genericul „Gestionarea amenințărilor hibride și politici de management al resurselor umane;
- în perioada 04-07.12. 2023, 1 angajat a participat la vizita de studiu privind preluarea bunelor practici de funcționare a serviciilor de raportare a materialelor ce reprezintă abuz sexual asupra copiilor în mediul online, organizată de către „INHOPE", Amsterdam, Regatul Țărilor de Jos.

Prin urmare, în contextul participării la evenimentele internaționale menționate a fost instituit în Republica Moldova mecanismului de raportare a materialelor de abuz sexual asupra copiilor și înființarea a unui instrument de tip Hotline.

De asemenea, lansarea proiectului AG-CYBER *(CPORT).* PORT prevede dezvoltarea unui portal de colaborare pentru autoritățile de aplicare a legii *(CPORT)* și pentru îmbunătățirea sistemului ICCAM *(soluție ce sprijină eliminarea materialelor cu conținut de abuz sexual asupra copiilor în mediul online, precum și asigură schimbul de rapoarte pe domeniu între diverși actori implicați)* ce ar permite și ar facilita schimbul de informații între analiștii liniilor fierbinți, INTERPOL și autoritățile de aplicare a legii.

Potrivit PG, procurorii și personalul Secției participă permanent la evenimente internaționale organizate în vederea dezvoltării sale profesionale, atât online, cât și cu prezență fizică.

În perioada 6-9 martie 2023 – vizita de documentare a reprezentanților instituțiilor naționale relevante, inclusiv MAEIE, în Regatul Țărilor de Jos și Regatul Belgiei, organizat de UE. Obiectivul vizitei a fost familiarizarea cu bunele practici internaționale, consolidarea cooperării internaționale în domeniile ce vizează

securitatea cibernetică, având loc întrevederi la Centrul Național pentru Securitate Cibernetică a Olandei, departamentul EC3 pentru combaterea crimelor cibernetice la sediul EUROPOL, întâlnire cu membrii diviziunii Cyber la EUROPOL, task Force pe Cyber al MAE olandez, SEAE, NATO, etc.

În perioada 12-16 iunie 2023, reprezentantul MAEIE a participat la instruiri oferire prin intermediul Tallinn Summer School of Syber Diplomacy, pe subiecte ce țin de digitalizare și securitate cibernetică, implementarea cadruluinormativdin domeniul securității și rezilienței cibernetice.

În iunie – reprezentantul MAEIE a participat la Berlin la instruiri și consultări tehnice în domeniul securității cibernetice, cu sprijinul proiectului UE „Moldova Rapid Cyber Security Assistance”

În august - noiembrie 2023 reprezentantul MAEIE a participat la programul de instruire online Her CyberTracks initiative, finanțat de GIZ și ITU dedicat femeilor care activează în cadrul autorităților publice centrale și locale, precum și în mediul privat cu competențe în domeniul securității cibernetice.

Prin intermediul platformelor create de Interpol, Europol și Consiliului Europei *(Proiectul CyberEast)* SIS realizează schimbul de informații pe linie de parteneriat, inclusiv are loc instruirea ofițerilor de informații pe domeniul combaterii criminalității informatice.

Ofițerii SIS au participat în cadrul a 6 evenimente:

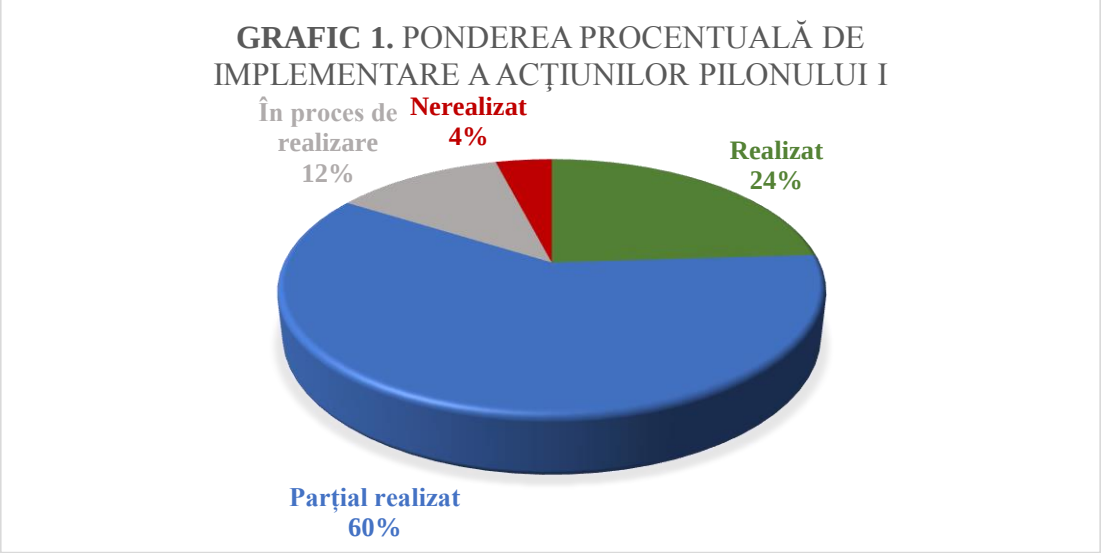
1. IP Crime Conference Webinar „Digital Safety&Online Policing” *(Interpol);*
2. Atelierul de lucru „Responsible Behaviour in Cyberspace and Cyber-hygiene” *(în cadrul Programului de dezvoltare profesională NATO - Republica Moldova (Professional Development Program NATO – RM));*
3. Webinar „Unveiling the Darknets Malware-as-a-Service model” *(Bright TALK);*
4. CyberEast „Instruirea privind taxonomia și gestionarea incidentelor cibernetice și a criminalității cibernetice”, organizat de UE și Consiliul Europei *(CoE);*
5. „7th Project Steering Committee”, CyberEast sub egida UE și CoE;
6. Întrevedere cu reprezentanții Europol pe dimensiunea proceselor de combatere a „Cybercrime”.

REFLECTAREA INDICATORILOR DE PROGRES CONFORM PRIORITĂŢILOR ŞI ACȚIUNILOR PLANIFICATE

În contextul evaluării rezultatelor de implementare a Planului SSI în anul 2023, a fost elaborată şi o prezentare grafică conform calificativelor indicatorilor de progres pe acţiunile executate de către instituţiile responsabile şi partenere reieșind din obiectivele realizabile în perioada de raportare.

În acest sens, ponderea procentuală a realizării acţiunilor este prezentată în graficile 1, 2, 3 și 4 care au fost elaborate reieșind din indicatorii de rezultat/progres întregistrate reieșind din procesul de implementare a acestora de către instituțiile responsabile.

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



Cu referință la acțiunile Pilonului I, au fost realizate – 24%, parțial realizate – 60 %, în proces de realizare – 12%, nerealizate – 3%.

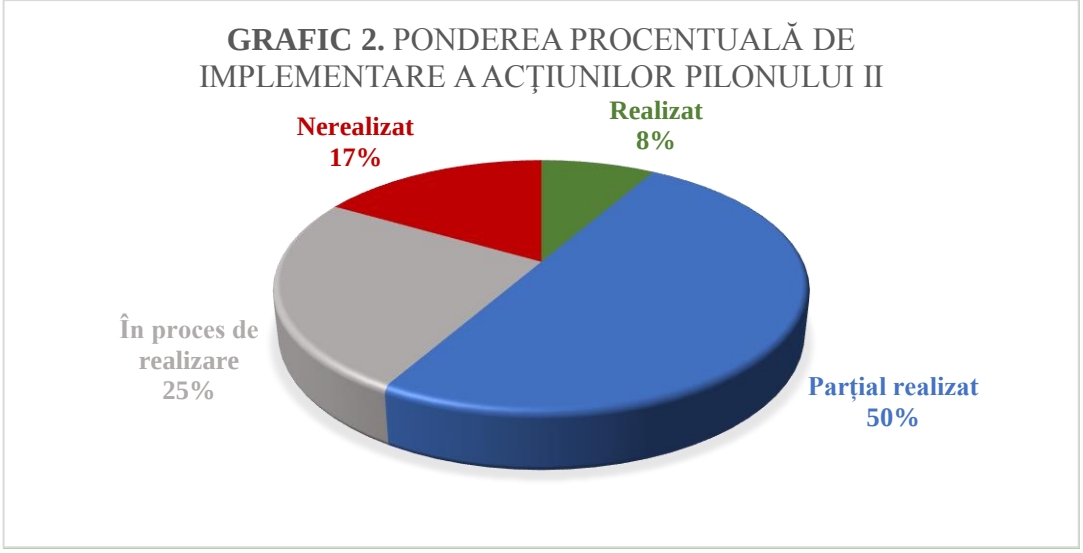
De menționat că în anul 2023, instituțiile de stat au efectuat mai multe misiuni de audit al sistemelor informaționale din gestiune, inclusiv cu participarea structurilor specializate în acest sens. În acest sens, SIS a acordat suport specializat

la crearea subdiviziunilor de securitate pentru tehnologia informației în cadrul a 22 instituții, a examinat actele interne privind organizarea și funcționarea organelor de cifrare, a remis notificări de securitate cibernetică operatorilor de comunicații naționali și a fost implicat în realizarea unor controale de audit. Totodată, SIS a emis 3 certificate de conformitate pentru mijloace de protecție tehnică și criptografică a informației, inclusiv a verificat corespunderea condițiilor de licențiere a agenților economici.

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.

În anul 2023 a fost creată Agenția pentru securitatea cibernetică *(HG nr. 1028/2023)*, autoritate care va exercita funcția Centrului de răspuns la incidentele de securitate cibernetică la nivel național *(CERT-național)*.

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 – 8%, parțial realizate – 50%, în proces de realizare – 25%, nerealizate – 17%.

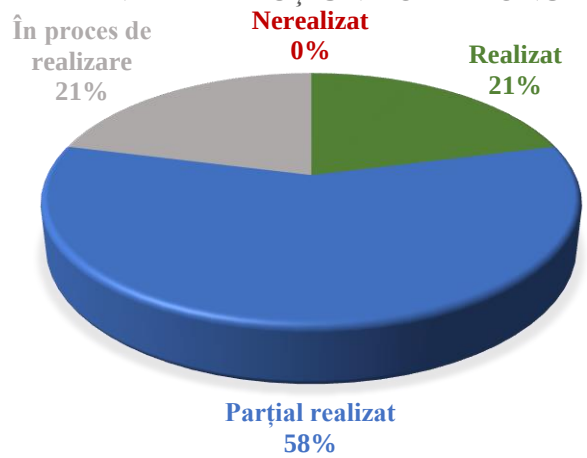
Pe parcursul anului 2023, SIS a informat Secretarul general al Guvernului RM referitor la lipsa cadrului legal național orientat spre reglementarea activității

mijloacelor de informare în masă în mediul online, inclusiv despre lipsa reglementărilor de natură să determine statutul entităților virtuale, fără persoană juridică sau identificare cu persoana fizică și lipsa mecanismelor practice de sancționare *(de blocare a resurselor web care conțin informații false, propagandistice și incitatoare)* care pot submina securitatea informațională a RM excluzând dispozițiile Comisia pentru situații Excepționale (CSE).

Procesul de implementare a acțiunilor la Pilonul II urmează să fie în continuare amplificată, în special urmare a creării la nivel național a Consiliului coordonator pentru asigurarea securității informaționale, în speță reieșind din crearea Centrului pentru Comunicare Strategică și Combaterea Dezinformării, care poate prelua poziția de platformă informațională de comunicare strategică.

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

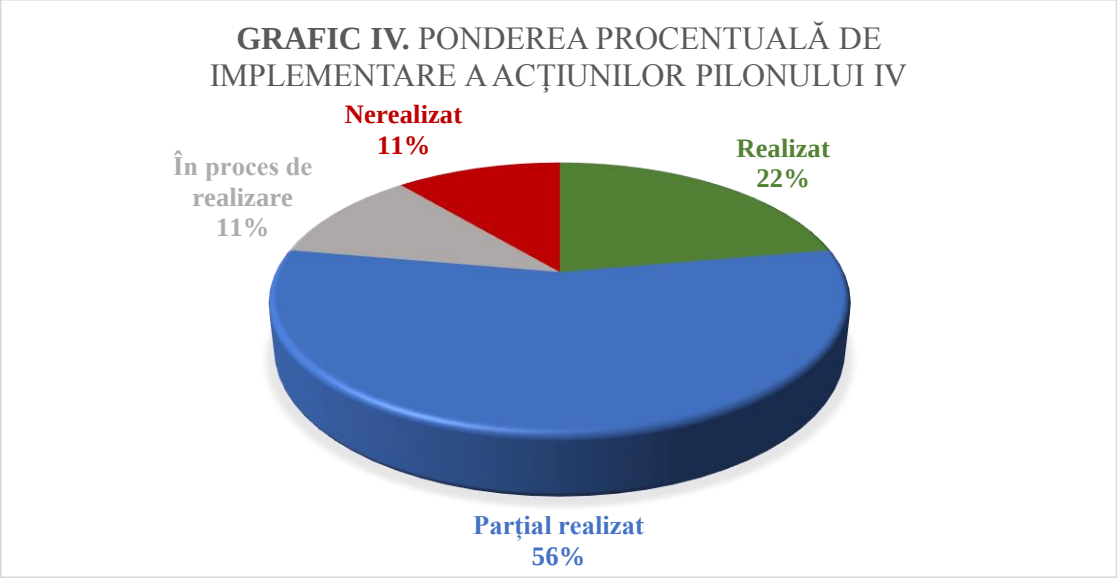
GRAFIC 3. PONDEREA PROCENTUALĂ DE IMPLEMENTARE A ACȚIUNILOR PILONULUI III



Referitor la acțiunile Pilonului III, au fost realizate – 21%, parțial realizate – 58%, în proces de realizare – 21%, nerealizate – 0%.

În cadrul Pilonului III, instituțiile statului au fost implicate în evaluarea amenințărilor hibride, prin completarea Chestionarul pe Amenințări Hibride *(AH)*, urmare a solicitării Serviciului European de Acțiuni Externe (SEAE). Pe parcursul anului 2023, instituțiile statului au fost implicate în evaluarea cadrului normativ național și adaptarea acestuia la evoluțiile de securitate regională și TIC.

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



Cu privire la acțiunile Pilonului IV, au fost realizate – 22%, parțial realizate – 56%, în proces de realizare – 11%, nerealizate – 11%.

În context, prioritățile și obiectivele Pilonului IV denotă o importanță majoră prin prisma proceselor vizate, în special în ceea ce privește 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 nominalizate.

DESCRIEREA RISCURILOR DE IMPLEMENTARE

Implementarea obiectivelor Strategiei securității informaționale a Republicii Moldova necesită o impulsionare și implicare plenară a tuturor componentelor societății informaționale în vederea transpunerii în practică a acțiunilor planificate, în special din considerentul că acestea au o configurare transectorială și comportă 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 identificare riscuri ale procesului de implementare a SSI, unele necesitând o atenție sporită și 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 2023, 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 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 securității 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: media, public și privat.

NOTĂ: În perioada următoare, 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 2023, cu elaborarea Raportului de progres pentru al cincilea an, relevă în continuare că prioritățile pe aspecte ce vizează securitatea 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 2023, în corespundere cu scopul, obiectivele şi acțiunile Strategiei, **denotă un progres parțial insuficient** în realizarea acestora.

În context, **riscurile de securitate** și **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 și 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.

De menționat că, **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 2023** fiind constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, Agenția pentru Securitate Cibernetică exercită funcția de echipă de răspuns la incidentele cibernetice la nivel național şi cea de punct național unic de contact, prin Hotărârea Guvernului Republicii Moldova nr. 1028/2023 și adoptarea legii cadru pentru implementarea SSI – 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 2023 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.