MINISTERUL ECONOMIEI ȘI INFRASTRUCTURII

Raport despre executarea în semestrul I 2020 a Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020

Hotărîrea Guvernului nr.811 din 29.10.2015

Chișinău, august 2020

S U M A R

INFORMAȚIE GENERALĂ

Dezvoltarea accelerată a tehnologiei informației și comunicațiilor electronice moderne care au penetrat deja toate sferele vieții sociale, economice și politice ridică la un alt nivel abordarea amenințărilor, riscurilor și vulnerabilităților într-o societate informațională.

În prezent, amenințările și riscurile, atacurile și incidentele cibernetice, precum și alte evenimente survenite în spațiul cibernetic în care nu există frontiere, se produc cu o frecvență, complexitate și o amploare din ce în ce mai mare, aducînd pagube enorme sectorului guvernamental, celui privat și cetățenilor. Acestea se materializează în spațiul cibernetic prin exploatarea vulnerabilităților de natură umană, tehnică și procedurală. Caracterul asimetric de prevenire și combatere a acestora aduc nu numai prejudicii economice semnificative, dar pot afecta și securitatea informațională a Republicii Moldova, dacă nu se vor întreprinde măsuri speciale de monitorizare a spațiului cibernetic al țării.

Problema securității cibernetice și primele măsuri de soluționare la nivel de politici guvernamentale sînt expuse în premieră în Strategia națională de dezvoltare a societății informaționale "Moldova Digitală 2020" aprobată prin Hotărîrea Guvernului nr.857 din 31.10.2013. Totodată, această problemă a fost examinată în premieră și la ședințele Consiliului Suprem de Securitate (CSS) în cadrul cărora au fost formulate un șir de recomandări, aprobate prin Decizia CSS nr.01/1-02-05 din 07.10.2014.

În contextul realizării prevederilor acestor 2 acte juridice a fost inițiată elaborarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (PNSC 2016-2020) care a fost aprobat prin Hotărîrea Guvernului nr.811 din 29.10.2015.

Obiectivul principal al PNSC 2016-2020 este „Crearea și implementarea unui sistem de management al securității cibernetice a Republicii Moldova”. Pentru asigurarea derulării eficiente a procesului de implementare a obiectivului stabilit cu finalitate în 2020 a fost elaborat Planul de acțiuni privind implementarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (PAI PNSC 2016-2020).

Acțiunile din PAI PNSC 2016-2020, realizarea cărora au o complexitate interdependentă, sînt repartizate în 7 compartimente conform obiectivelor specifice ale PNSC 2016-2020:

1. procesarea, stocarea și accesarea în siguranță a datelor, inclusiv a datelor de interes public;
2. securitatea și integritatea rețelelor și serviciilor de comunicații electronice;
3. dezvoltarea capacităților de prevenire și reacție urgentă la nivel național (crearea rețelei de CERT-uri naționale);
4. prevenirea și combaterea criminalității informatice;
5. consolidarea capacităților de apărare cibernetică;
6. educația, formarea și informarea continuă în domeniul securității cibernetice;
7. cooperarea și interacțiunea internațională în sferele ce țin de securitatea cibernetică.

Totodată, la realizarea acțiunilor din PAI PNSC 2016-2020 se va ține cont și de prevederile ce țin de securitatea cibernetică expuse în Strategia securității informaționale a Republicii Moldova pentru anii 2019-2024 (SSI 2019-2024) aprobată prin Hotărîrea Parlamentului nr. 257/2018, Strategia națională de apărare pentru anii 2018–2022 (SNA 2018-2022) aprobată prin Hotărîrea Parlamentului nr. 134/2018, cît și Strategia de securitate națională, aprobată prin Hotărîrea Parlamentului nr. 153 din 15.07.2011.

Potrivit prevederilor Hotărîrii Guvernului nr. 811 din 29.10.2015, în sarcina Ministerului Economiei și Infrastructurii (MEI) este pusă responsabilitatea de monitorizare și coordonare a procesului de realizare a PNSC 2016-2020. În contextul exercitării acestei

sarcini, MEI a recepționat de la ministere și alte autorități administrative centrale informația privind executarea în semestrul I 2020 a PNSC 2016-2020, conform responsabilităților stabilite pentru aceste instituții în PAI PNSC 2016-2020.

În majoritatea cazurilor în semestrul I 2020 a fost continuată executarea acțiunilor din PAI PNSC 2016-2020 inițiate în semestrul II 2019.

Responsabilii principali de executarea acțiunilor din PAI PNSC 2016-2020 sînt identificați în conformitate cu prevederile pct.30 din PNSC 2016-2020 și urmează să prezinte informația în conformitate cu prevederile pct. 30, 41 și 42 din PNSC 2016-2020.

În prezentul Raport n-au fost incluse informațiile care:

- argumentează necesitatea executării acțiunilor și care de fapt nu se referă la executarea propriu zisă a acestora;
- nu se referă la conținutul semantic al denumirii acțiunii;
- dublează aceleași rezultate și pentru alte acțiuni;
- se referă la evaluarea intermediară (anuală), deoarece principalele instituții responsabile (responsabilii principali) de executarea acțiunilor n-au transmis în adresa MEI, inclusiv informația de raportare a monitorizării și evaluare privind realizarea acțiunii concrete.

I. OBIECTIVUL SPECIFIC „PROCESAREA, STOCAREA ȘI ACCESAREA ÎN SIGURANȚĂ A DATELOR, INCLUSIV A DATELOR DE INTERES PUBLIC”

Implementarea acestui obiectiv specific se realizează prin executarea a 11 acțiuni din PAI PNSC 2016-2020.

Pînă în semestrul I 2020 inclusiv, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, au fost realizate 8 acțiuni, au fost continuate activitățile de realizare a 3 acțiuni inițiate în anul 2018 și 2 acțiuni inițiate în 2019, rezultatele executării cărora se expun după cum urmează mai jos.

Acțiunea 1.1 „Asigurarea ajustării cadrului normativ-legislativ privind securitatea cibernetică a Republicii Moldova care va prevedea: a) definirea termenilor (noțiunilor) din domeniul securității cibernetice; b) delimitarea pe domenii a competențelor; c) stabilirea organului cu funcții de monitorizare a respectării cerințelor de securitate cibernetică; d) desemnarea organului responsabil de controlul implementării rezultatelor auditului de securitate cibernetică; e) obligațiile deținătorilor sistemelor informaționale de stat privind efectuarea periodică a auditului acestor sisteme, cu stabilirea periodicității, nivelelor, obligațiilor de prezentare a raportului către organul competent; f) sancțiuni pentru nerespectarea deciziei auditului privind conformitatea cu cerințele minime obligatorii de securitate cibernetică; g) responsabilitatea personală pentru asigurarea securității cibernetice; h) introducerea în autoritățile publice a funcției de coordonator de securitate cibernetică, inclusiv atribuțiile principale ale acestuia; i) formarea Consiliului intersectorial de securitate cibernetică (cu funcție de coordonare a activităților de securitate cibernetică)”

Termen de realizare: 2016-2017.

Responsabil principal este Ministerul Economiei și Infrastructurii (MEI).

În contextul executării acestei acțiuni, MEI a continuat studierea cadrului legislativ-normativ și instituțional al altor state, inclusiv și celui european referitor la securitatea cibernetică.

Astfel, pentru realizarea acestei acțiuni a fost elaborată și aprobată Hotărîrea Guvernului nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică.

Totodată, în scopul stabilirii instituției responsabile de efectuarea auditului și evaluarea conformității acestuia, a fost elaborată și aprobată HG 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat. De asemenea, această Hotărîre prevede desemnarea instituțiilor publice: Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) și Agenția de Guvernare Electronică (AGE) cu noi atribuții în domeniul securității cibernetice.

Concomitent, a fost elaborată și aprobată Concepția securității informaționale a Republicii Moldova prin Legea nr. 299 din 21.12.2017, ulterior publicată în Monitorul Oficial nr. 48-57/122 din 16.02.2018.

În conformitate cu art. 3 din Concepția securității informaționale, Serviciul de Informații și Securitate (SIS) a elaborat și a definitivat de comun cu autoritățile naționale competente proiectul Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și Planul de acțiuni pentru implementarea acesteia, ulterior aprobată prin Hotărîrea Parlamentului nr. 257 din 22.11.2018.

Astfel, în scopul realizării HP 257/2018 SIS a inițiat procedura de creare a Consiliului Coordonator pentru asigurarea securității informaționale, care va avea atribuții inclusiv în domeniul securității cibernetice. În acest sens, SIS a elaborat și a remis în adresa instituțiilor/organizațiilor competente proiectul Hotărîrii de Guvern „Cu privire la crearea Consiliului coordonator pentru asigurarea securității informaționale". Ulterior au avut loc ședințe de lucru cu instituțiile guvernamentale, companii private TIC (reprezentate de Moldova IT Park și ATIC), reprezentanți ai societății civile și ai instituțiilor media. Ulterior, după recepționarea tuturor sugestiilor instituțiilor/organizațiilor implicate, SIS va definitiva și va înainta spre promovare proiectul de Hotărîre de Guvern.

În aceeași ordine de idei, ținem să comunicăm că MEI a inițiat procedura de elaborare a proiectului de lege de transpunere în legislația națională a Directivei UE 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. În prezent, se examinează cele mai bune practici în domeniul securității rețelelor și sistemelor informaționale pentru a fi incluse în proiect. Prin Ordinul MEI nr. 54 din 04.03.2019 a fost creat grupul de lucru pentru elaborarea proiectului de lege privind securitatea rețelelor și sistemelor informaționale.

De asemenea, MEI este în dialog permanent cu partenerii de dezvoltare la subiectul lansării unui proiect de asistență consultativă în dezvoltarea legislației naționale în domeniul securității rețelelor și sistemelor informaționale. În acest sens, avem un acord prealabil din partea partenerilor americani și în scurt timp va fi asigurată expertiză necesară de cea mai înaltă calitate.

Concomitent, Corporația MITRE (SUA) elaborează un raport de pre-evaluare a capacității cibernetice naționale, ce va fi utilizat la elaborarea legii. Totodată, în I trimestru 2020, Comisia Europeană lansează proiectul EU4Cyber, un obiectiv al căruia va fi asistarea țărilor Parteneriatului Estic în transpunerea Directivei NIS.

În același context, STISC a inițiat procedura de avizare a proiectului hotărîrii de Guvern „privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental" care prevede desemnarea Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică" în calitate de Centru guvernamental de reacție la incidente de securitate cibernetică (CERT guvernamental) și aprobarea regulamentului CERT

guvernamental.

Acțiunile 1.3, 1.4 și 2.3

Termen de realizare: 2016-2017.

Responsabil principal este MEI.

Executarea acestor acțiuni urma să fie realizată în cadrul a două comitete tehnice de standardizare: CT 28 "Tehnologia informației" și CT 29 "Comunicații electronice", conducerea cărora era exercitată de către reprezentanții MEI.

Prin Hotărîrea nr. 57 din 14.03.2016 a Institutului Național de Standardizare aceste două comitete tehnice de standardizare au fost desființate, instituindu-se un nou comitet tehnic de standardizare CT 48 "Tehnologia informației și comunicații electronice". Comitetul tehnic CT 48 și-a pus scopul de a participa la lucrările de standardizare europeană și internațională, în special prin examinarea proiectelor de standarde elaborate de comitetul tehnic ISO/IEC JTC 1/SC 6. CT 48 este membru participant la comitetul internațional ISO/IEC JTC 1 ceea ce înseamnă că membrii CT pot vota proiecte de standarde, precum și pot veni cu comentarii de îmbunătățire.

În vederea armonizării reglementărilor din domeniul TIC cu standardele europene și internaționale a fost remisă Institutului de Standardizare solicitarea (nr. 01/305 din 15.03.2017) de adoptare a standardelor ETSI prioritare. Astfel, reieșind din importanța și numărul lor, au fost aprobate ca standarde moldovene 15 standarde ETSI din categoria "Cyber Security".

De asemenea, anterior au fost adoptate 22 standarde ISO ca standarde moldovenești.

Institutul de Standardizare din Moldova este în proces de implementare a sistemului de management a securității informației, conform standardului SM EN ISO/IEC 27001:2017 „Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe". În acest context sînt implementate: proceduri de operare documentate, sistem de management al parolelor, restricționarea accesului la informație, securitatea fizică și a mediului de lucru, utilizarea informației secrete de autentificare și a semnăturilor digitale, înregistrarea evenimentelor și generarea dovezilor, managementul accesului utilizatorului și controlul accesului și alte aspecte de securitate cibernetică internă.

În total au fost adoptate ca standarde moldovenești 214 standarde internaționale și europene privind procesarea, stocarea, accesarea sigură a datelor, securitatea sistemelor informaționale, a sistemelor de comunicații electronice etc.

Totodată, MAI comunică că în contextul evaluării vulnerabilităților sistemelor informaționale din cadrul acestuia, în temeiul contractului nr. 84/15 din 21.12.2015 încheiat cu "Info-Trust Consulting" SRL, se află la etapa finală de realizare Proiectul implementării sistemului de management al securității informației (etapa-1) și definirea modelului operațional al Serviciului Tehnologii Informaționale (STI) conform principiilor IT Service Management (ITSM). Unul din rezultatele Proiectului are drept scop asigurarea unui spațiu informațional unic protejat și securizat al sectorului TIC din cadrul MAI și în mod special a segmentelor ce țin de "Sistemul Informațional integrat ale autorităților administrative și instituțiilor subordonate ale MAI", implicate în detectarea și prevenirea criminalității. După realizarea etapelor de evaluare a vulnerabilităților sistemelor informaționale și de implementare a clasificării informației în cadrul MAI, acesta ar putea înainta propuneri suplimentare de aplicare a standardelor europene și internaționale ce țin de procesarea, stocarea și accesarea în siguranță a datelor.

Acțiunea 1.5 „Elaborarea cerințelor minime obligatorii de securitate cibernetică”

Termen de realizare: 2016-2018.

Responsabil principal este MEI.

În contextul executării acestor acțiuni, MEI a elaborat proiectul Hotărîrii Guvernului privind aprobarea "Cerințelor minime de securitate cibernetică" care a fost aprobat prin Hotărîrea Guvernului nr. 201 din 28.03.2017.

Acțiunea 1.6 „Certificarea specialiștilor reieșind din standardele și metodologia identificate și cerințele minime obligatorii de securitate cibernetică aprobate”

Termen de realizare: 2016-2018.

Responsabil principal este MEI.

Conform informației prezentate în ianuarie 2019, 28 specialiști din sectorul public au fost certificați reieșind din standardele internaționale și cerințele minime obligatorii de securitate cibernetică, cu următoarele modele de certificate: „Eset NOD 32 Technical Specialist” Nr. 239488; Certificate of the completion of trhe computer security incident response team training, Chișinău, 21.10.2016; CompTIASecurity+; CompTIA PenTest+; Security Development Lifecycle and Web Application Security; auditor intern pentru sisteme de Management Calitate, conform standardului ISO 9001:2017; Anti-Mita, conform standardului ISO 37001:2016 și Ghidului ISO 19011:2011 și auditor conform standardului ISO SM ISO/IEC 27001:2013.

Acțiunea 1.8 „Efectuarea unui audit în autoritățile administrației publice centrale și locale, în alte entități deținătoare de sisteme informaționale de stat, cu scopul identificării vulnerabilităților și corespunderii la cerințele minime obligatorii de securitate cibernetică”

Termen de realizare: 2017-2020.

Responsabili principali: Autoritățile administrației publice centrale și locale, deținători ai sistemelor informaționale de stat.

Prin HG 414/2018 s-a stabilit că AGE este responsabilă de efectuarea auditului de securitate cibernetică a infrastructurilor de tehnologie a informației și a Sistemului de telecomunicații al autorităților administrației publice, precum și a altor infrastructuri cibernetice de interes național, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora. De asemenea, AGE este responsabilă de efectuarea și evaluarea conformității auditului de securitate cibernetică și monitorizarea implementării rezultatelor auditului de securitate cibernetică efectuate în autoritățile publice în conformitate cu cerințele minime obligatorii de securitate cibernetică, aprobate de Guvern.

Astfel, în semestrul I 2019 a fost elaborat Graficul de desfășurare a auditului de securitate cibernetică în autoritățile și instituțiile publice subordonate Guvernului. În perioada 15.07– 15.11.2019 a fost realizat auditul cibernetic în 13 instituții. Ulterior, AGE a emis și expediat instituțiilor audiate rapoartele de audit, cu identificarea disfuncțiilor, vulnerabilităților și furnizarea soluțiilor de remediere a acestora.

De asemenea, întru respectarea cadrului normativ în cadrul MAI a fost efectuat auditul intern de securitate cibernetică pentru anul 2018, în baza Ordinului STI nr.45 din 14.11.2018, finalizat în ianuarie 2019. Scopul și obiectivele acțiunii de audit au urmărit confirmarea respectării prevederilor HG nr. 201 din 28.03.2017, identificarea vulnerabilităților existente, a obiectivelor politicilor de securitate ale MAI și STI, precum și conformarea cu standardele internaționale de securitate în domeniul TIC.

Prin Raportul de audit intern de securitate s-au stabilit unele neajunsuri, au fost evaluate riscurile reziduale întru respectarea cerințelor minime obligatorii de securitate cibernetică, fiind înaintate recomandări care urmează a fi implementate conform Planului calendaristic în scopul conformării standardelor de securitate și respectării de către persoanele responsabile din cadrul STI implicate în domeniul de activitate specifice instituției.

În anul 2018 în cadrul MEI au fost derulate misiuni de audit ale Curții de Conturi în domeniul performanței evidenței resurselor și sistemelor informaționale deținute de minister (06.06.2018), în domeniul tehnologiilor informaționale din cadrul ministerului, inclusiv evaluarea situațiilor financiare consolidate (29.03.2018) și în domeniul gestionării Serviciului Guvernamental de Plăți Electronice MPay (06.04.2018).

De asemenea, în 2019, Serviciul audit intern al IGPF al MAI, a inițiat misiunea de audit intern cu titlul „Evaluarea conformității sistemului IT din cadrul IGPF la cerințele minime de securitate cibernetică", care va avea loc în perioada lunilor iulie-septembrie 2019.

În conformitate cu Ordinul Ministerului Educației, Culturii și Cercetării (MECC) nr. 319/2019 „Cu privire la realizarea auditul intern a tehnologiilor informaționale (TI)", în semestrul I 2019, Serviciul audit intern și Serviciul Tehnologiei informației și comunicațiilor din cadrul MECC au inițiat misiunea de audit intern. Această misiune a fost efectuată în cadrul aparatului central și în 2 instituții din subordinea MECC, în vederea identificării registrelor, serviciilor și proceselor interne de interes sporit, evaluării modului de aplicare a tehnologiilor informaționale pentru activităților aferente în domeniul educației, precum și localizarea zonelor sensibile și problematice a sistemelor informaționale din cadrul MECC.

Acțiunea 1.9 „Elaborarea planului de înlăturare a vulnerabilităților conform recomandărilor auditului și executarea acestuia prin responsabilitate personalizată în cadrul autorităților administrației publice centrale și locale, altor entități deținătoare de sisteme informaționale de stat"

Termen de realizare: 2016-2018.

Responsabil principal este orice autoritate a administrației publice centrale sau locale care, potrivit normelor legale, deține sisteme informaționale de stat.

Activitățile de elaborare a planurilor de înlăturare a vulnerabilităților, conform recomandărilor auditului, urmează a fi efectuate după realizarea acțiunii de la pct. 1.8 din PAI PNSC 2016-2020.

Prin Ordinul MAI nr. 374 din 12.12.2017 au fost aprobate procedurile de raportare a incidentelor, analiza și evaluarea riscurilor de securitate a informației în cadrul MAI. Aceste proceduri conțin reglementări privind modul de elaborare și realizare a planului de înlăturare a vulnerabilităților de către deținătorii sistemelor informaționale din cadrul MAI.

De asemenea, urmare a auditului intern de securitate cibernetică efectuat pentru anul 2018 (finalizat în ianuarie 2019), în baza Ordinului STI nr. 45 din 14.11.2018, au fost identificate unele neajunsuri, au fost evaluate riscurile reziduale întru respectarea cerințelor minime de securitate cibernetică, fiind înaintate recomandări care urmează a fi implementate conform Planului calendaristic în scopul conformării standardelor de securitate și respectării de către persoanele responsabile din cadrul STI implicate în domeniul de activitate specifice instituției.

Acțiunea 1.10 „Elaborarea și implementarea metodologiei de marcare a informației furnizate prin sistemul care conține date cu caracter personal cu utilizarea mărcii temporale"

Termen de realizare: 2016-2019.

Responsabil principal este Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDCP).

CNPDCP informează că pentru elaborarea metodologiei de marcare a informației furnizate prin sistemul care conține date cu caracter personal cu utilizarea mărcii temporare urmează să fie implicați specialiști în tehnologia/securitatea informațională, cu cunoștințe ce ține de mecanismul de creare/utilizare a semnăturii electronice. Reieșind din faptul, că instituția nu dispune de asemenea specialiști și nici de competențe de reglementare în domeniul semnăturii electronice, serviciilor de marcare temporală, etc., fapt care pune sub întrebare desemnarea CNPDCP ca instituție responsabilă pentru această acțiune, CNPDCP propune examinarea posibilității desemnării unei alte instituții responsabile pentru această acțiune.

Acțiunea 1.11 „Elaborarea și implementarea actelor legislative necesare pentru introducerea măsurilor de securitate și standardelor obligatorii în companiile din domeniul tehnologiei informației și comunicațiilor, cu stabilirea unor cerințe minime de securitate a sistemelor informaționale de stat și a informațiilor din aceste sisteme"

Termen de realizare: 2017

Responsabil principal este MEI.

Informația este expusă la acțiunea 2.1.

II. OBIECTIVUL SPECIFIC „SECURITATEA ȘI INTEGRITATEA REȚELELOR ȘI SERVICIILOR DE COMUNICAȚII ELECTRONICE"

În semestrul I 2019, în conformitate cu termenele stabilite pentru realizarea acestui obiectiv, au fost continuate activitățile de realizare a acestora inițiate în anul 2018, rezultatele executării cărora se expun după cum urmează.

Acțiunea 2.1 „Armonizarea legislației din domeniul comunicațiilor electronice la directivele-cadru UE din domeniu"

Termen de realizare: 2016.

Responsabil principal este MEI.

MEI a elaborat proiectul de lege pentru modificarea și completarea Legii comunicațiilor electronice nr. 241-XVI din 15.11.2007, armonizat la prevederile directivelor-cadru UE din domeniul comunicațiilor electronice prevăzute în Acordul de Asociere „Republica Moldova – Uniunea Europeană". Proiectul propune completarea Legii în cauză cu 2 articole noi (art. 20^1 și art. 20^2), care se referă la securitatea și integritatea rețelelor și serviciilor. Prin aceste completări, legislația națională a fost armonizată cu prevederile capitolului III-A „Securitatea și integritatea rețelelor și serviciilor" din Directiva 2002/21/CE, astfel cum aceasta a fost modificată prin Directiva 2009/140/CE.

Proiectul de lege vizat a fost aprobat prin Legea nr. 185 din 21.09.2017 pentru modificarea și completarea unor acte legislative.

După republicarea Legii comunicațiilor electronice nr.241-XVI din 15.11.2007 în Monitorul Oficial al Republicii Moldova nr. 399-410 din 17.11.2017, art.679, prevederile respective se regăsesc în art. 21 și art. 22 din această Lege.

SIS, în calitate de instituție partener, în limita competențelor acordă suportul necesar instituțiilor de profil. În acest context, a fost aprobat Regulamentul privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora, prin Hotărîrea Guvernului nr. 1141 din 20.12.2017 și Regulamentul privind activitatea prestatorilor de

servicii de certificare în domeniul aplicării semnăturii electronice, prin Hotărîrea Guvernului nr. 1140 din 20.12.2017.

Acțiunea 2.2 „Stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității, non-repudierii și integrității rețelelor și/sau serviciilor de comunicații electronice și raportarea incidentelor cu impact semnificativ asupra acestora"

Termen de realizare: 2016-2017.

Responsabil principal este Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI).

ANRCETI a elaborat proiectul Măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității și integrității rețelelor și serviciilor publice de comunicații electronice și raportarea incidentelor cu impact semnificativ asupra acestora. De asemenea, a fost elaborată Analiza Impactului de Reglementare la proiect. Proiectul menționat, va fi supus examinării și aprobării de către Consiliul de Administrație al ANRCETI în modul stabilit de legislație.

Totodată, în contextul armonizării legislației naționale cu cadrul de reglementare al Uniunii Europene pentru comunicațiile electronice, a fost adoptată Legea nr. 185/2017.

Prin armonizarea menționată, în art. 21-22 din Legea comunicațiilor electronice nr. 241/2007 (republicată), deja (la nivel de act legislativ) se reglementează măsurile tehnice și organizatorice necesare pentru a gestiona în mod corespunzător riscurile legate de securitatea rețelelor și serviciilor sau pentru a asigura integritatea rețelelor, pe care, întreprinderile ce furnizează rețele publice de comunicații sau servicii de comunicații electronice accesibile publicului, au obligația de a le realiza.

Art. 22 alin. (2) din Legea nr. 241/2007 dispune că intervenția ANRCETI prin reglementarea modalităților/ măsurilor care să contribuie la nivelul sporit de securitate a comunicațiilor electronice este condiționată de verificarea și evaluarea prealabilă a măsurilor stabilite de furnizori.

Prin urmare, înainte de adoptarea unor măsuri specifice în domeniul securității cibernetice, ANRCETI, prin lege, are atribuția de a obține în prealabil informații suficiente pentru a fi în măsură să evalueze nivelul de securitate a rețelelor sau serviciilor, precum și de a obține date complete și certe referitoare la incidentele reale.

În această ordine de idei, ANRCETI a inițiat, în temeiul art. 22 alin. (1) lit. a) din Legea nr. 241/2007, un proces de colectare de la furnizorii de rețele publice de comunicații electronice și/sau servicii de comunicații electronice accesibile publicului informații necesare evaluării securității și integrității rețelelor și serviciilor, inclusiv a politicilor interne de securitate aplicabile, pentru a constata stabilirea unor reglementări în acest sens.

Acest studiu a demonstrat că companiile din domeniu au elaborat politici (instrucțiuni, ghiduri, practici, etc.) care includ măsuri tehnice și organizatorice necesare pentru asigurarea unui nivel de securitate corespunzător riscului identificat și prevenirea sau minimalizarea impactului incidentelor de securitate asupra utilizatorilor rețelelor interconectate. Concomitent, pentru fiecare procedură standard de operare în rețea și/sau servicii, companiile dispun de reglementări interne separate, care descriu acțiunile necesare sa fie întreprinse pentru a asigura implementarea eficientă a procedurii.

Acțiunea 2.4 „Efectuarea unui studiu cu privire la modificarea legislației în domeniul comunicațiilor electronice în vederea eliminării sau diminuării numărului abonaților serviciilor de comunicații electronice depersonalizați”

Termen de realizare: 2016-2017.

Responsabil principal este SIS.

SIS a studiat practica țărilor europene în domeniu și înaintează propuneri de modificare a cadrului legislativ național.

Astfel, în contextul diminuării numărului abonaților serviciilor de comunicații electronice depersonalizați, SIS a elaborat proiectul legii de modificare a Legii comunicațiilor electronice nr. 241/2007 și l-a remis în adresa MEI spre promovare. MEI nu a susținut promovarea proiectului de lege, invocînd faptul că la nivelul UE nu există o legislație unitară în materie.

În scopul identificării soluției optime pentru promovarea proiectului au fost solicitate date de la autorități (MEI, ANRCETI, MAI) privind utilizarea cartelelor SIM preplătite și a fost elaborată Analiza impactului de Reglementare a proiectului de lege pentru modificarea art. 64 din Legea comunicațiilor electronice nr. 241 din 15.11.2007. Astfel, luînd în calcul refuzul MEI de a promova proiectul de lege menționat, tot setul de acte necesare (proiectul de lege, analiza impactului de reglementare, nota informativă) a fost remis în adresa MAI spre promovare**.**

Acțiunea 2.5 ”Dezvoltarea în continuare a rețelei de comunicații speciale a autorităților administrației publice pe întreg teritoriul Republicii Moldova”

Termen de realizare: conform Planului aprobat de Guvern.

Responsabil principal este Cancelaria de Stat (CS).

Pentru semestrul I 2020, SIS informează despre inițierea a unei serii de acțiuni în scopul modernizării infrastructurilor de transport a rețelei speciale de comunicații guvernamentale în mun. Chișinău.

STISC raportează că în prezent instituțiile statale sunt conectate la o rețea de fibră optică cu lungimea totală de circa 150 km, care acoperă doar mun. Chișinău. Din lipsa de resurse financiare alocate, rețeaua de comunicații speciale nu a fost extinsă. Pentru transportul de date în alte localități ale țării se utilizează rețelele agenților privați, ceea ce constituie o vulnerabilitate semnificativă. Proiectul de dezvoltare a rețelei de comunicații speciale a autorităților administrației publice pe întreg teritoriul Republicii Moldova este elaborat și în prezent se lucrează asupra etapelor de implementare, cu suportul partenerilor externi. Se poartă discuții cu compania Huawei referitor la implementarea proiectului de extindere a Sistemului de telecomunicații al autorităților publice la nivel național (rețeaua de comunicații speciale a autorităților publice).

MAI raportează, că în scopul executării acțiunii prenotate, dar și în conformitate cu Dispoziția MAI nr. 8/4-5024 din 19.07.2016, a fost aprobată lista punctelor de prezență ale MAI incluse în Proiectul privind modernizarea rețelei corporative (WAN) a MAI. Astfel, la moment, în baza Contractului nr. 49/16 din 03.06.2016 dintre STISC și STI MAI s-a inițiat procesul de achiziționare a serviciilor de transfer date între punctele de prezență a MAI, precum și serviciilor de creare și mentenanță a sistemului WAN MAI, prin care MAI beneficiază de o rețea securizată în toate Inspectoratele de Poliție de pe întreg teritoriul Republicii Moldova.

În scopul asigurării unui schimb securizat de date între subdiviziunile subordonate acestuia, precum și cu alte autorități ale administrației publice locale, MAI a încheiat cu STISC un Contract de achiziționare a serviciilor de transport date între punctele de prezență ale MAI, precum și a serviciilor de creare și mentenanță a sistemului WAN MAI.

Urmare încheierii acestui Contract, MAI și-a asigurat serviciile de arendă a canalelor transfer date/servicii, transfer date (comunicații electronice securizate) pentru o perioadă de 24 luni (01.06.2016 - 31.05.2018). Acest transfer de date și servicii transfer date este asigurat între sediile Aparatului Central al MAI, STI, SPIA precum și 94 puncte de prezență ale MAI (subdiviziunile teritoriale IGP, BMA și SPCSE), inclusiv a derulat crearea/modernizarea infrastructurii de acces pentru 24 puncte de prezență WAN MAI.

De asemenea, MAI raportează că în semestrul I 2019 se află în proces de implementare Proiectul „Asigurarea unui sistem de comunicații fiabil și eficient pentru scopuri operaționale în cadrul Poliției", prevăzut în Matricea de politici anexă a Acordului de finanțare CRIS:ENI/2015/038-144 „Suport pentru dezvoltarea Poliției" și a Strategiei de dezvoltare a Poliției 2016-2020, aprobată prin Hotărîrea Guvernului nr. 587 din 12 mai 2016 care are ca obiectiv principal crearea platformei comune de radiocomunicații securizate în standard TETRA.

Conform proiectului, pînă la finele anului 2020 urmează să fie instalate 66 stații de bază TETRA pe întreg teritoriul Republicii Moldova, pentru o acoperire de circa 94% la nivel de terminal mobil. Totodată, se finalizează lucrările de instalare și punere în funcțiune a 35 stații de bază TETRA în mai multe locații din țară.

În aceeași ordine de idei, în anul 2019 urmau a fi instalate încă 16 stații de bază TETRA, astfel să fie atinsă o acoperire în proporții de 80% a centrelor raionale și 65% din drumurile naționale, la nivel de terminal mobil.

III. OBIECTIVUL SPECIFIC „DEZVOLTAREA CAPACITĂȚILOR DE PREVENIRE ȘI REACȚIE URGENTĂ LA NIVEL NAȚIONAL (REȚEAUA CERT NAȚIONALĂ)"

Atingerea acestui obiectiv specific se va realiza prin executarea a 8 acțiuni din PAI PNSC 2016-2020.

În semestrul I 2019, în conformitate cu termenele stabilite pentru realizarea acestui obiectiv, au fost continuate activitățile de realizare a acestora inițiate în anul 2018, rezultatele executării cărora se expun după cum urmează.

Acțiunea 3.1 „Crearea Centrului național de reacție la incidentele de securitate cibernetică (CERT)"

Termen de realizare: 2016.

Responsabil principal este CS.

Dezvoltarea capacităților de prevenire și reacție urgentă la nivel național (rețeaua CERT națională) prevede crearea Centrului național de reacție la incidentele de securitate cibernetică (CERT-național), a centrelor departamentale în autoritățile publice centrale, autoritățile publice locale, alte entități ce dețin sisteme informaționale de stat, stabilirea obligațiilor de raportare și evidență operativă obligatorie a incidentelor de securitate cibernetică pentru autoritățile administrației publice centrale și locale și mediul de afaceri din domeniul tehnologiei informației și comunicațiilor.

Cu referire la evoluția dezvoltării capacităților de prevenire și reacție urgentă la incidentele de securitate cibernetică în Republica Moldova, menționăm că inițial, în vederea executării prevederilor HG nr. 746/2010 „Cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului Republica Moldova - NATO actualizat", în cadrul Î.S. „Centrul de Telecomunicații Speciale" (ulterior reorganizată prin transformare în I.P. STISC) a fost creat Centrul pentru Securitatea Cibernetică CERT-GOV-MD, misiunea căruia era de a asista beneficiarii în utilizarea sistemelor informaționale și de telecomunicații al autorităților

administrației publice în implementarea măsurilor proactive și reactive în vederea reducerii riscurilor de incidente ale securității TI și acordarea asistenței în reacționarea la incidente.

Ulterior, în conformitate cu prevederile Strategiei securității informaționale a Republicii Moldova 2019-2024 (HP 257/2018), HG 482 din 08.07.2020 „Privind aprobarea unor măsuri necesare privind asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărîrii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat" I.P. STISC este desemnată în calitate de Centru guvernamental de reacție la incidentele de securitate cibernetică (CERT-Gov). CERT-Gov constituie punctul unic de contact și de raportare a incidentelor de securitate cibernetică pentru structurile de tip CERT departamentale și dispune de capacitatea necesară pentru prevenirea, analiza, identificarea și reacția la incidentele cibernetice la nivel guvernamental. În acest context, HG 482/2020 delimitează competențele și responsabilitățile entităților publice în domeniul securității cibernetice, inclusiv măsurile și mecanismele necesare implementării, în scopul menținerii unui spațiu cibernetic securizat la nivel guvernamental.

Totodată, pe parcursul anului 2019 au fost purtate discuții cu parteneri strategici (SUA și UE) în vederea oferirii unui suport pentru consolidarea securității cibernetice a Republicii Moldova printr-un proiect de asistență de transpunere în legislația națională a Directivei NIS, cu ulterioara asistență în crearea Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT).

Totodată, în scopul acordării asistenței țărilor Parteneriatului Estic pentru sporirea securității cibernetice și pregătirea împotriva atacurilor cibernetice, Uniunea Europeană a lansat, în ianuarie 2020, „Programul EU4Digital: Îmbunătățirea rezilienței cibernetice în țările Parteneriatului Estic". Perioada de realizare - 36 luni. În cadrul acestui Program, Republica Moldova va beneficia de expertiză la dezvoltarea cadrului legal și instituțional pentru asigurarea unui nivel înalt de securitate a rețelelor și a sistemelor informatice la nivel național, în conformitate cu standardele UE.

Astfel, proiectul de Lege va prevedea stabilirea cadrului normativ și instituțional la nivel național și cadrului național de cooperare în asigurarea securității rețelelor și sistemelor informatice prin desemnarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică ca autoritate națională cu atribuții de reglementare, supraveghere și control și care va îndeplini și funcția de Punct Unic de Contact la nivel național, cât și funcția de echipă CSIRT națională (echipă de răspuns la incidente de securitate informatică la nivel național și de participare la răspunsul comun la nivel european), precum și delimitarea clară a atribuțiilor actorilor implicați, cerințelor de notificare a incidentelor, măsurilor și cerințelor pentru asigurarea securității cibernetice a sistemelor informatice utilizate în gestionarea obiectivelor și serviciilor de infrastructură critică.

În acest sens, la începutul anului 2020, au avut loc primele întrevederi și discuții de documentare a experților proiectului, iar în toamna acestui an se preconizează a fi prezentat raportul pe țară cu ulterioarele propuneri de activități.

Actualmente, în lipsa unei structuri de tip CERT cu competențe naționale, CERT-Gov exercită atribuții de răspuns la incidentele de securitate, la nivel de Guvern, pentru sistemele informatice ale autorităților și instituțiilor publice centrale, aflate în administrarea tehnică a STISC. Ulterior, CERT-Gov a preluat o parte din prerogativele unui CERT național, respectiv: asigurarea Punctului național de Contact pentru incidente de securitate cibernetică, diseminarea alertelor de securitate primite de la partenerii internaționali către toți operatorii de rețele și sisteme informatice, coordonarea campaniilor de conștientizare a utilizatorilor de

internet asupra pericolelor existente în mediul online, etc. Cu toate eforturile depuse reușesc să acopere doar sectorul public, de nivel central, respectiv în cadrul celorlalte instituții ale statului, care nu sînt în subordinea Guvernului, cum ar fi autoritățile și instituțiile din cadrul Administrației Publice Locale, nu se pot derula activități de asigurare a securității cibernetice pentru mediul privat.

Reieșind din cele expuse și urmare a aprobării PAI SSI 2019-2024, crearea/desemnarea entității care va exercita rolul centrului de reacție la incidente cibernetice la nivel național este obiectiv prioritar, care implică alocații bugetare considerabile și ca precondiție acțiunea de elaborare și promovare a cadrului normativ relevant, fapt pentru care au fost stabilite noi termene de realizare: 2019–2021.

STI, în calitate de autoritate administrativă a MAI, în baza Proiectului de consultanță privind implementarea sistemului de management al securității informației (etapa 1) și definirea modelului operațional al STI conform principiilor ITSM, a planificat ca necesar, constituirea la nivel de MAI a unui CERT instituțional de reacționare la incidentele cibernetice ce pot surveni în cadrul infrastructurilor critice gestionate. Astfel, constituirea acestuia în cadrul MAI este în proces de realizare.

Acțiunea 3.2 „Crearea unui sistem național de alerte și informare în timp real despre incidentele de securitate cibernetică”

Termen de realizare: 2016-2017.

Responsabil principal este CS.

Instrumentul principal de lucru al CERT Gov cu funcții de CERT național va fi Sistemul național de alerte și de informare în timp real despre incidentele de securitate cibernetică, crearea căruia este preconizată.

Sistemul trebuie să asigure gestionarea incidentelor de securitate cibernetică în timp real prin recepționarea automatizată a alertelor de securitate de la partenerii interni și/sau internaționali și transmiterea operativă a acestora către operatorii/deținătorii /administratorii sistemelor informatice suspectate de derularea unor activități malițioase în internet. Aceste date vor proveni din 3 surse: sursele proprii, prin instalarea unor senzori în rețele, sursele partenerii internaționali care monitorizează acțiunile malițioase din internet și datele utilizatorilor de internet care reclamă apariția unor incidente de securitate cibernetică. Prin aceste activități se vor diminua riscurile și se va îmbunătăți climatului național de securitate cibernetică. Astfel, Sistemul va asigura un mecanism unitar de reacție și răspuns la incidentele de securitate cibernetice.

În contextul celor expuse, I.P. Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) a elaborat Studiul de fezabilitate pentru acest Sistem și urmează să fie identificate resursele financiare pentru implementarea acestuia.

În aceeași ordine de idei, potrivit informației prezentate de STISC, a fost elaborat Conceptul și caietul de sarcini pentru crearea unui Sistem care va emite alerte și informație privind incidente de securitate a informației, ghiduri care ar ajuta funcționarii de a nu fi expuși riscurilor și noilor amenințări, care devin tot mai complexe. Standardizarea mai rapidă a formatului schimburilor de date la nivel național ar duce cu rapiditate la scăderea timpului de răspuns și creștere a compatibilității sistemelor tehnologice utilizate de diverse instituții.

Totodată, furnizarea periodică a unor rapoarte care să conțină pe lîngă componenta tehnică (pe care sînt orientate majoritatea platformelor și furnizorilor actuali) și analize, evaluări profesionale cu privire la evoluția de perspectivă a mediului de securitate online, în vederea consolidării componentei de prevenție și susținerii informaționale a actului de decizie (atît în mediul public, cît și privat), ar fi necesară.

Odată cu aprobarea HG 482/2020 privind aprobarea unor măsuri necesare privind asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărîrii Guvernului nr. 414/2018, STISC, în calitate de CERT Gov, urmează să întreprindă toate acțiunile pentru crearea Sistemul național de alerte și de informare în timp real despre incidentele de securitate cibernetică în termenul stabilit.

Acțiunea 3.3 „Crearea centrelor de reacție la incidentele de securitate cibernetică departamentale în autoritățile administrației publice centrale și locale, în alte entități deținătoare de sisteme informaționale de stat"

Termen de realizare: 2016-2017.

Responsabil principal este orice autoritate a administrației publice centrale sau locale, precum și orice altă entitate, care potrivit normelor legale, deține sisteme informaționale de stat.

Este necesar de menționat că în Planul de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 (PAI SSI 2019-2024), este prevăzută acțiunea de elaborare a mecanismelor de creare și consolidare a centrelor departamentale de reacție la incidente de securitate cibernetică și informațională, atît de drept public, cît și de drept privat, cu termene de realizare 2021–2023.

În contextul realizării acestei acțiuni, în cadrul MAI în baza Proiectului de consultanță privind implementarea sistemului de management al securității informației (etapa 1) și definirea modelului operațional al STI conform principiilor ITSM, a planificat constituirea unui CERT instituțional de reacționare la incidente cibernetice ce pot surveni în cadrul infrastructurilor critice gestionate de MAI. Acesta urmează a fi constituit în urma aprobării noii structuri funcționale a STI MAI.

În prezent se identifică resursele bugetare și resursele partenerilor de dezvoltare pentru finanțarea lucrărilor de creare a CERT-ului instituțional al MAI. Totodată, este cazul de menționat și faptul că realizarea acestei acțiuni este dependentă în mare măsură de crearea CERT-național.

MA raportează că actualmente este în derulare crearea CERT-ului militar cu suportul oficiului SPS NATO în cadrul proiectului „Dezvoltarea capacităților de apărare cibernetică a Forțelor Armate", termenul de implementare fiind august 2020.

SIS informează că a inițiat procesul de extindere a capacităților sale instituționale în acest context.

CNPDCP informează că deține un Centru departamental de reacție la incidentele de securitate cibernetică. Or, potrivit pct. 90 din Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal (Cerințe), aprobate prin Hotărîrea Guvernului nr. 1123 din 14.12.2010, CNPDCP recepționează anual, de la deținătorii (operatorii) de date cu caracter personal, rapoarte generalizate despre incidentele de securitate a sistemelor informaționale de date cu caracter personal. În baza acestor rapoarte, CNPDCP întreprinde măsurile ce se impun de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

În cadrul CNPDCP a fost elaborat un set de legi (privind Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova, inclusiv pentru modificarea și completarea unor acte legislative), potrivit căruia:

- în cazul în care are loc o încălcare a securității datelor personale, operatorul va informa despre acest lucru CNPDCP, fără întîrzieri, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice;

- va fi creat în cadrul CNPDCP o subdiviziune specializată, cu atribuții de reacție la incidentele de securitate cibernetică.

Acțiunea 3.4 „Stabilirea obligațiilor pentru autoritățile administrației publice centrale și locale și mediul de afaceri din domeniul tehnologiei informației și comunicațiilor privind raportarea operativă obligatorie a incidentelor de securitate cibernetică în baza unui mecanism de schimb de date și rolurile bine definite"

Termen de realizare: 2016-2017.

Responsabil principal este CS.

Acțiunea în cauză urmează a fi desfășurată după realizarea acțiunii de la pct.3.2 din PAI PNSC 2016-2020.

Totodată, în vederea executării prevederilor Hotărîrii Guvernului nr. 746 din 18.08.2010 „Cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului Republica Moldova – NATO actualizat", în cadrul STISC a fost creat Centrul pentru Securitatea Cibernetică - CERT-GOV-MD.

Autoritățile administrației publice centrale și locale și mediul de afaceri din domeniul tehnologiei informației și comunicațiilor urmează să realizeze raportarea incidentelor de securitate cibernetică către Centrul pentru Securitatea Cibernetică - CERT-GOV-MD.

În aceeași ordine de idei, este necesar de menționat că în PAI SSI 2019-2024 este prevăzută acțiunea de determinare a politicii privind modalitatea de raportare, de stocare și de prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale, cu termene de realizare 2021–2022, responsabil STISC.

În conformitate cu HG 482/2020 privind aprobarea unor măsuri necesare privind asigurarea securității cibernetice la nivel guvernamental și modificarea hotărârii Guvernului nr. 414/2018, prin care a fost reglementată activitatea CERT Gov, STISC întreprinde toate măsurile pentru crearea și asigurarea funcționării platformei de management a incidentelor și schimbului de informații cu CERT-urile departamentale. De asemenea, în conformitate cu Măsurile necesare pentru asigurarea securității cibernetice la nivel guvernamental ale prezentei hotărâri, în temeiul punctului 7, subpct 1) a prezentei hotărâri, în vederea exercitării rolului de Centre departamentale de reacție la incidente de securitate cibernetică (CERT Departamental) entitățile publice au atribuția de a desemna, prin act normativ, persoana (subdiviziunea) responsabilă de punerea în aplicare în cadrul entității publice a măsurilor necesare asigurării securității cibernetice.

În acest context, se urmărește stabilirea unui dialog eficient între CERT Gov și CERT-urile departamentale privind modalitatea de raportare, stocare și prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale.

La nivel de MAI, obligațiile privind raportarea operativă obligatorie a incidentelor de securitate cibernetică au fost aprobate prin Ordinul MAI nr. 374 din 12 decembrie 2017 privind aprobarea procedurilor de raportare a incidentelor, analiză și evaluare a riscurilor de securitate a informației în cadrul MAI.

Acțiunea 3.5 „Organizarea unei baze de date cu acces al autorităților responsabile privind amenințările, vulnerabilitățile și incidentele de securitate cibernetică identificate sau raportate, tehnicile și tehnologiile folosite pentru atacuri, bunele practici pentru protecția domeniului tehnologiei informației și comunicațiilor"

Termen de realizare: permanent.

Responsabil principal este CS.

Acțiunea în cauză urmează a fi desfășurată după aprobarea concepției Sistemului prevăzut a fi creat la pct.3.2 din PAI PNSC 2016-2020.

Totodată, crearea și funcționarea Centrului guvernamental de reacție la incidente de securitate cibernetică în conformitate cu prevederile SSI 2019-2024, va prevedea cadrul legal necesar pentru crearea bazei de date cu acces al autorităților responsabile privind amenințările, vulnerabilitățile și incidentele de securitate cibernetică identificate sau raportate, tehnicile și tehnologiile folosite pentru atacuri, bunele practici pentru protecția domeniului tehnologiei informației și comunicațiilor.

În PAI SSI 2019-2024 pentru obiectivul Dezvoltarea capacităților instituționale în combaterea criminalității informatice este prevăzută acțiunea de creare a unei baze de date naționale privind evoluția fenomenului criminalității informatice, cu termene de realizare 2021–2022.

Conform prevederilor HG 482/2020 privind aprobarea unor măsuri necesare privind asigurarea securității cibernetice la nivel guvernamental și modificarea hotărârii Guvernului nr. 414/2018, în temeiul punctului 4, STISC în termen de 9 luni de la data aprobării, creează și pune în aplicare Registrul de Stat al incidentelor de securitate cibernetică, care va cuprinde o bază de date cu acces al autorităților responsabile privind amenințările, vulnerabilitățile și incidentele de securitate cibernetică identificare sau raportate, tehnicile și tehnologiile folosite pentru atacuri, bunele practici pentru protecția domeniului tehnologiei informației și comunicațiilor.

MAI informează că implementează funcția „Service Desk”, urmare implementării căreia va fi creat un singur punct de contact pentru serviciile de tehnologii informaționale ale MAI, cu restabilirea funcționalității acestora în cel mai scurt timp posibil în cazul unor situații de urgență. Implementarea funcției „Service Desk” va permite acumularea solicitărilor și propunerilor, informațiile despre incidentele de securitate și problemele tehnice transmise de utilizatorii tehnologiilor informaționale. Datele astfel acumulate sînt transmise prestatorilor de servicii spre analiză și identificarea soluțiilor. Soluțiile identificate se remit beneficiarului. În acest mod va fi creată o bază de date de evidență a tuturor incidentelor de securitate din cadrul MAI.

Acțiunea 3.6 „Desfășurarea exercițiilor și antrenamentelor comune de consolidare a capacităților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate”

Termen de realizare: permanent.

Responsabil principal este CS.

În vederea consolidării capacităților de reacție la atacuri cibernetice au fost organizate o serie de evenimente:

1. STISC a organizat mai multe exerciții de securitate cibernetică la care au participat atît funcționari din sectorul public, cît și privat, precum și mediul academic. În luna octombrie 2017, cu suportul Ambasadei Statelor Unite ale Americii în Moldova și partenerilor naționali, s-a organizat Conferința “CyberSec 2017". Acest eveniment face parte din Luna Europeană a Securității Cibernetice (ECSM), o campanie de conștientizare la nivel european, cu scopul de a promova securitatea cibernetică în rîndul cetățenilor și de a schimba percepția asupra amenințărilor informatice, prin intermediul promovării conceptului de securitate a datelor și a informațiilor, prin educație, schimbul de bune practici și competiții. În cadrul Campaniei din acest an au fost discutate tematici precum securitatea cibernetică la locul de muncă și acasă, guvernanță și protecția vieții private, a datelor și a dezvoltării competențelor specifice domeniului.

2. STISC, la inițiativa Uniunii Internaționale a Telecomunicațiilor (UIT) în parteneriat cu Ministerul Economiei și Infrastructurii al RM, Asociația Națională a Companiilor din Domeniul TIC (ATIC), a organizat un exercițiul regional de testare a abilităților de protecție împotriva atacurilor cibernetice, eveniment ce se încadrează în inițiativa "Joint Cyber Drill ITU - ALERT pentru Europa și regiunile CSI".

Peste 170 de participanți din 25 țări din CSI și UE, precum România, Luxemburg, Belgia, Lituania, Serbia, Macedonia, Albania, Cipru, Tadjikistan, Ucraina, Muntenegru, Bosnia și Herțegovina ș.a., s-au întrunit în cadrul acestui eveniment. Echipele s-au antrenat să răspundă operativ la atacuri cibernetice de diferite tipuri, în baza a 8 scenarii de lucru, pe care le-au aflat doar în momentul exercițiilor. Acestea au primit sarcinile în regim interactiv și au avut la dispoziție un timp limitat pentru a veni cu o soluție. Aproape 30 de experți și traineri din țările UE și CSI au antrenat și au jurizat echipele participante la ALLERT Cyber Drill 2017.

3. Organizarea celui de-al 2-lea Exercițiu Regional de Cooperare privind Criminalitatea Cibernetică de către Oficiul Programului Cybercrime al Consiliului Europei, în cadrul proiectelor Cybecrime@EAP 2018, întru sprijinirea eforturile comune ale CERT-GOV-MD (Centrul pentru Securitatea Cibernetică din cadrul STISC, Moldova) și CERT-RO. Circa 50 de participanți din regiunea Parteneriatului Estic (Armenia, Azerbaidjan, Belarus, Georgia, Moldova și Ucraina), precum și participanți din Ghana, Mauritius, Filipine, Sri Lanka și Tonga vor participa la exercițiul condus de echipa de experți din Moldova, România și Marea Britanie. Prin acest exercițiu s-a demonstrat importanța și necesitatea consolidării parteneriatului public-privat în domeniul criminalității și securității cibernetice, atît din perspectiva accesării datelor deținute de companiile private, cît și pentru încurajarea folosirii unor abordări și metode comune de prelucrare a dovezilor electronice în cazul incidentelor cibernetice și a investigațiilor penale / financiare, aplicînd standardele internaționale din domeniu, cum ar fi Convenția Consiliului Europei privind Criminalitatea Cibernetică.

4. În perioada 29.10-02.11.2018 STISC sub patronatul Guvernului a organizat evenimentul regional Moldova Cyber Week 2018, alăturîndu-se astfel campaniei europene de conștientizare #CyberSecMonth. În contextul acestui eveniment și întru consolidarea capacităților de reacție la atacurile cibernetice, inclusiv de blocare a atacurilor cibernetice simulate, în perioada 30-31.10.2018 au fost organizate exerciții și antrenamente în format Cyber Drill. Sub ghidarea unor experți de renume s-a reușit testarea capacităților de răspuns și a nivelului de pregătire tehnică a 100 de participanți, reprezentanți ai sectorului public, privat și mediul academic atît din Republica Moldova, cît și din alte țări din Europa și spațiul CSI.

5. STISC a planificat pentru perioada octombrie - noiembrie 2019 desfășurarea unei noi ediții a evenimentului "*Moldova Cyber Week",* eveniment conceput pentru reprezentanții sectorului public, privat și academic, care va include conferință, workshop-uri, exerciții și antrenamente comune de consolidare a capacităților de reacție la atacuri cibernetice. Ca de fiecare dată la eveniment se va alătura campaniei europene de conștientizare #CyberSecMonth, aducînd în prim plan subiectul Securității Cibernetice.

SIS, în calitate de instituție co-responsabilă, în limita competențelor, acordă suportul necesar instituțiilor de profil. În acest context, s-a participat la:

- Atelierul de lucru „Dezvoltarea Sistemului de management al securității informaționale în Republica Moldova" în cadrul MEI, organizat cu suportul experților coreeni din cadrul Misiunii de consultanță în domeniul securității cibernetice;

- Cursul „Network vulnerability assessment and risk mitigation” oferit de școala post navală Oberamergau.

De asemenea, a fost organizat exercițiul internațional antiterorist „Bucovina - 2018” la care au fost aplicate și elemente de securitate cibernetică.

MAI raportează că angajații din cadrul STI al MAI, pe parcursul anului 2016, au participat la diverse ședințe de instruire a specialiștilor IT, desfășurate de către companii prestatoare de servicii de asigurare a securității informaționale. În special, urmează de a menționa participarea la evenimentul ce a avut loc la 30 martie curent, cînd reprezentanții MAI, de comun cu 20 specialiștii IT din cele mai mari companii din Moldova, au testat cunoștințele sale în domeniul securității informaționale, participînd la business joc „Security Games 2017”, organizat de companiile „DAAC System Integrator” și „Cisco”. Subiectele analizate se referă la patru situații de prevenire a scurgerii de date. Participanții au fost repartizați în echipele ce au jucat rolul de furnizor al serviciilor de Internet și rolul de instituție financiară.

În perioada 21-23 noiembrie 2017 a fost organizat la Chișinău un exercițiu ALERT Cyber Drill 2017. La exercițiu pe lîngă reprezentanții din Republica Moldova au participat și experți din statele CSI și UE, unde au testat, dezvoltat și fortificat abilitățile de protecție împotriva atacurilor cibernetice. Peste 170 de participanți din 25 țări din CSI și UE, precum România, Luxemburg, Belgia, Lituania, Serbia, Macedonia, Albania, Cipru, Tadjikistan, Ucraina, Muntenegru, Bosnia și Herțegovina ș.a., s-au întrunit în cadrul ALLERT Cyber Drill.

Ziua de 21.11.2017 a fost dedicată prezentărilor și discuțiilor publice pe tema ultimelor evoluții și amenințări din spațiul cibernetic. Zilele de 22 și 23 noiembrie 2017 au fost destinate în exclusivitate exercițiilor practice, timp în care echipele participante și-au putut îmbunătăți capacitatea de comunicare și de răspuns la incidente survenite în adresa lor prin simularea unor scenarii de atacuri cibernetice, în formatul Cyber Drill ALERT unde misiunea principală a fost de a găsi în timp potrivit cele mai corecte soluții de răspuns la incidente sau situații de criză.

Acțiunea 3.7 „Consolidarea capacităților echipei Centrului național de reacție la incidentele de securitate cibernetică pentru a asigura analiza strategică a incidentelor de securitate și coordonarea acțiunilor de răspuns la incidente de securitate în sectorul public, privat și academic, inclusiv prin organizarea trening-urilor de către experți calificați”

Termen de realizare: 2016-2018.

Responsabil principal este CS.

Consolidarea și fortificarea capacităților CERT-GOV-MD este un proces continuu axat pe preluarea celor mai bune practici și schimb de experiență. În acest sens, CERT-GOV-MD menține un dialog deschis și manifestă o implicare directă în relație cu cele mai notorii instituții la nivel internațional în domeniul vizat. Respectiv STISC a participat la:

1. Centrul de Răspuns la Incidente Cibernetice CERT-GOV-MD din cadrul STISC a participat în calitate de membru acreditat FIRST la cea de-a 30-a Conferință Anuală a Forumului de Reacție la Incidente și Echipele de Securitate (FIRST) și cea de-a 13-a Conferință NatCSIRT 2018, organizată de Institutul de Inginerie Software (SEI), Universitatea Carnegie Mellon. Ambele conferințe, atît FIRST cît și NatCSIRT 2018, reprezintă o platformă eficientă de dialog prin împărtășirea obiectivelor, ideilor și informațiilor în vederea îmbunătățirii securității informatice la nivel mondial. Evenimentele au fost concepute pentru a crea o conexiune globală, oferind o mulțime de oportunități pentru

ca oamenii să comunice între ei și să se conecteze în cadrul tuturor sesiunilor și atelierelor organizate.

2. Seminarul Regional ITU cu genericul „Aspecte esențiale ale securității cibernetice în contextul Internet of Things", eveniment organizat în cadrul ICT Week2017 (The week of Information and Communication Technologies) în orașul Taşkent, Uzbekistan. La seminar au participat reprezentanți ai ministerelor și agențiilor, ai mediului academic, cît și a echipelor CERT din țările membre și asociate ITU, operatori de telecomunicații, dezvoltatori de software și alte organizații din domeniul tehnologiilor informaționale.

3. În cadrul Lunii securității cibernetice, STISC în calitate de organizator al evenimentului „Moldova Cyber Week 2018" a participat activ în cadrul Conferinței privind securitatea cibernetică, care a reunit de altfel peste 60 de experți care și-au prezentat cercetările și o serie de prezentări informative pe parcursul a 8 paneluri informative și sesiuni plenare, abordînd subiecte de interes precum:

- tendințe emergente în securitatea informatică;
- inovația ca soluție pentru securitatea informatică;
- sisteme de control industriale pentru asigurarea infrastructurii companiei SCADA;
- schimbul de informații și parteneriatele public-privat;
- cerințe de implementare și de funcționare a CERT-urilor;
- criminalitatea informatică și aplicarea legii;
- GDPR: elemente indispensabile;
- Bazele Bitcoin, Blockchain și Contracte Smart.

4. Cea de-a 5-a ediție a Conferinței GISD (Geneva Information Security Day) privind securitatea informatică a furnizorilor care a avut loc pe data de 12.10.2018. În cadrul acestui eveniment s-au reunit liderii comunității elvețiene și europene de securitate cibernetică în cadrul unui dialog deschis, constructiv și axat pe discuții eficiente și schimb de cunoștințe despre ultimele tendințe din industrie. Totodată, la acest eveniment s-au discutat care sînt probleme principale la nivel național în domeniul securității cibernetice și care ar fi soluțiile după evaluarea riscurilor în lupta cu crimele cibernetice și cum de creat o strategie de securitate cibernetică la nivel național.

5. La Summitul regional „7th Regional Cybersecurity Summit" desfășurat în or. Kuweit în perioada 21-22.10.2018 au participat peste 250 de experți din Orientul Mijlociu, SUA, Europa, fiind astfel puse în discuție subiecte precum problemele, tendințele și provocările curente, ultimele progrese tehnologice care pot ajuta în lupta împotriva amenințările cibernetice. Pe parcursul summit-ului s-a reușit:

- prezentarea unor sisteme de management al securității informatice de ultimă oră pentru a preveni riscurile, amenințările și pierderile de informații;
- prezentarea celor mai recente descoperi metodologice inovatoare pentru a menține organizația în siguranță împotriva criminalității informatice și a furtului de date;
- prezentarea unor studii de caz și povești de succes care demonstrează modul în care organizațiile au depășit cu succes atacurile cibernetice și criminalitatea informatică;
- discuții despre cadrul legislativ și politici în domeniul protecției datelor. Integrarea sistemelor de avertizare timpurie pentru a identifica amenințările potențiale și a optimiza monitorizarea eficientă a acestora.

Totodată se impune necesitatea fortificării activității CERT-GOV-MD, prin elaborarea unui proiect de lege, care va stabili anumite reguli în ceea ce privește raportarea și răspunsul în cadrul unor incidente de securitate. Se implementează platforma de informare pentru CERT (baze de date, sistem de raportare a incidentelor), care va sprijini activitatea CERT, în

colectarea, analiza rapoartelor despre incidente curente sau amenințări, crearea unei analize a amenințărilor pentru o bună înțelegere a situației și luarea măsurilor de apărare cibernetică, fapt ce va contribui la facilitarea cooperării și coordonării la nivel național și internațional.

Pe perioada semestrului I 2019, reprezentanții STISC au participat la evenimente dedicate consolidării și fortificării capacităților de răspuns la provocările spațiului cibernetic, după cum urmează:

1. Vizita de studiu TAIEX privind schimbul de experiență în domeniul securității cibernetice, în calitate de instrument de asistenta tehnică și schimb de informații gestionat de către Comisia Europeană. Scopul acestei vizite a fost extinderea relațiilor de cooperare în vederea consolidării capacităților operaționale a Centrului de răspuns la incidente cibernetice din cadrul STISC în conformitate cu obiectivele Programului de dezvoltare strategică a instituției pentru perioada 2019-2021. Astfel de vizite de studiu sînt foarte utile datorită componentei practice, care facilitează atît implementarea unei platforme eficiente la nivel național de schimb de informații și experiență, cît și crearea CERT-ului național.

În cadrul vizitei a fost examinată posibilitatea de implementare la nivel național a două sisteme de analiză a riscurilor care fac parte din procesul de asigurare a securității informațiilor, și anume:

- MONARH - metoda de analiză optimizată a riscului care permite gestionarea precisă și repetabilă a riscurilor și platforma de partajare a amenințărilor;
- MISP – software-ul care realizează distribuirea informațiilor despre amenințări și indicatori de securitate cibernetică.

De asemenea a fost semnat un Acord de colaborare între Serviciul Tehnologia Informației și Securitate Cibernetică și Centrul de răspuns la incidente informatice din Luxemburg. Părțile se obligă pe viitor să conlucreze prin schimb de experiență și bune practici, contribuind nemijlocit la ridicarea nivelului de cultură în domeniul TIC.

2. Conferința internațională RSA 2019, în cadrul căreria au fost prezentate și discutate cele mai optime soluții de securitate, precum și noile tendințe pe care dezvoltatorii de tehnologie încearcă să le anticipe.

Conferința RSA 2019 este o platformă inovativă pentru cele mai noi tehnologii și oportunități educaționale care îi ajută pe profesioniștii din industrie să descopere modul în care își pot face companiile mai sigure în domeniul securității cibernetice.

Printre aspectele principale care au fost discutate și care vor influenta activitatea pe parcursul anului 2019 a fost „*inteligența artificială”* care este unul dintre factorii care propulsează multe industrii, în special, domeniul supravegherii video. Soluții de deep-learning sînt deja utilizate pentru aplicații de analiză video, dar, pentru viitor este preconizată utilizarea pe scară mai largă în aplicații și produse tot mai variate, procesare la nivel cloud și edge. Conceptul de „*cloud computing”* a căpătat amploare în ultimii ani și este la ora actuală un adevărat fenomen, fiind folosit pe scară largă în toate domeniile.

Un alt subiect la ordinea de zi a fost menținerea echilibrului între personalizarea soluțiilor furnizate clienților și confidențialitate, prin intermediul impunerii unui nou set de reguli pentru protecția datelor la nivelul Uniunii Europene. Confidențialitatea prevalează atunci cînd producătorii trebuie să personalizeze soluțiile furnizate clienților, pentru a răspunde cel mai bine nevoilor acestora. Stabilirea unei relații de încredere între o companie și clienții săi poate fi puternic influențată de nivelul insuficient de securitate cibernetică care poate duce la degradarea iremediabilă a relațiilor părților.

Acțiunea 3.8 „Elaborarea mecanismelor (modelelor) de prevenire timpurie a incidentelor de securitate cibernetică în Republica Moldova, inclusiv în baza parteneriatelor public-private”

Termen de realizare: 2016-2018.

Responsabil principal este CS.

În contextul elaborării mecanismelor (modelelor) de prevenire timpurie a incidentelor de securitate cibernetică, STISC informează că una din problemele esențiale atît în sectorul public, cît și în cel privat o constituie analfabetismul tehnic.

Este important ca organizațiile să sesizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze pozitiv acest subiect prin conștientizare în rîndul angajaților și înțelegerea tipologiei amenințărilor și vulnerabilităților specifice mediilor informatizate și aplicarea practicilor de control.

Dat fiind faptul că majoritatea datelor prelucrate și stocate de către instituțiile de stat reprezintă informații confidențiale, angajații din domeniul public sînt responsabili să asigure gestionarea datelor și informațiilor sensibile, cunoscînd și respectînd cerințele minime obligatorii de securitate cibernetică.

În acest sens, CERT-GOV-MD din cadrul Serviciului Tehnologia Informației și Securitate Cibernetică oferă cursuri de instruire în domeniile de competență, avînd drept obiectiv implementarea măsurilor proactive și reactive în vederea reducerii riscurilor de incidente ale securității TI și acordarea asistenței în reacționarea la incidente. În acest sens se menționează elaborarea și publicarea Ghidul de bune practici pentru securitatea cibernetică, care a fost expediat către toate instituțiile publice și care este publicat pe pagina web a Centrului de răspuns la incidente cibernetice www.cert-stisc.gov.md.

Prevenirea timpurie a incidentelor de securitate cibernetică în Republica Moldova este posibilă prin educarea unui comportament corect în raport cu gestionarea riscurilor și a eventualelor incidente de securitate cibernetică. Respectiv, informarea, comunicarea și schimbul de experiență sînt esențiale în asigurarea acestui proces. Împreună cu alte instituții publice, STISC a organizat campanii publice de conștientizare a amenințărilor cibernetice adresate unui public specializat, prin diverse evenimente la nivel de Guvern, cît și mediul academic.

Un accent aparte este pus pe promovarea și sprijinirea tinerelor specialiști prin oferirea posibilităților de instruire în cadrul Laboratoarelor de securitate cibernetică și participare la exercițiile și workshop-urile organizate, care au ca scop identificarea tinerelor talente în cadrul seminarelor tematice organizate în cadrul Laboratorului de securitate cibernetică, sprijinirea tinerilor în formarea carierei profesionale în domeniul securității cibernetice, motivarea tinerilor specialiști să lucreze în cadrul instituțiilor publice, precum și potențialul de creștere a specialiștilor pe acest sector.

IV. OBIECTIVUL SPECIFIC „PREVENIREA ȘI COMBATEREA CRIMINALITĂȚII INFORMATICE„

Atingerea acestui obiectiv specific se va realiza prin executarea a 7 acțiuni din PAI PNSC 2016-2020.

Conform termenelor stabilite, în semestrul I 2020 au fost continuate activitățile inițiate în semestrul II 2019, rezultatele executării cărora se expun după cum urmează.

Acțiunea 4.1 „Elaborarea proiectului de lege privind modificarea și completarea legislației penale și contravenționale pentru prevenirea și combaterea crimelor informatice în scopul armonizării continue a acesteia la prevederile Convenției Europene privind criminalitatea informatică și la deciziile Comitetului acestei Convenții”

Termen de realizare: 2016.

Responsabil principal este MAI.

În scopul reglementării procesului de examinare a unui sistem informatic sau a unui suport de stocare a datelor informatice și excluderii unui șir de bariere de ordin legislativ în procesul de asigurare a securității informaționale de către organele abilitate, a fost elaborată și aprobată Legea nr. 294 din 22.12.2016 privind modificarea și completarea art.118 din Codul de procedură penală RM nr.122-XV din 14.03.2003.

De asemenea, a fost elaborat și prezentat Parlamentului spre adoptare proiectul de Lege pentru modificarea și completarea unor acte legislative (înregistrat cu nr.161 din 13.04.2016), însă aceasta nu a fost examinat în prima lectură în cadrul ședinței parlamentare, fiind declarat nul și retras.

Proiectul în cauză, elaborat de către Ministerul Afacerilor Interne, urma să modifice și să completeze Legea privind prevenirea și combaterea criminalității informatice, Legea comunicațiilor electronice, Codul Contravențional, Legea cu privire la exercitarea profesiunii de medic, Codul penal, Codul de procedură penală, Legea cu privire la asistența juridică internațională în materie penală. Proiectul în cauză a fost elaborat conform prevederilor Convenției de la Budapesta, Convenției Lanzarote, a directivelor UE și a practicii legislative din țările-membre ale UE, avizat pozitiv de către Comisia de la Veneția cu ulterioara includere a propunerilor de îmbunătățire sub aspectul garantării drepturilor persoanelor.

La 04.07.2019 MAI a inițiat procedurile de revizuire a prevederilor acestui proiect de Lege. În acest context, reieșind din faptul că procesul de promovare a proiectului de Lege elaborat anterior nu a fost finalizat în mare parte datorită complexității sale, Centrul pentru Combaterea Crimelor Informatice al MAI consideră oportună divizarea proiectului pe șase domenii, cu reinițierea procesului de elaborare și avizare a proiectelor respective. Reieșind din actualitatea și necesitatea prevederilor acestuia în procesul de prevenire și combatere a criminalității informatice, textul proiectelor în structura nouă a fost definitivat și transmis subdiviziunii specializate a IGP cu propunerile enunțate mai sus.

În aceeași ordine de idei, MAI menționează că, în scopul reglementării procesului de examinare a unui sistem informatic sau a unui suport de stocare a datelor informatice, a fost elaborată și aprobată Legea nr. 294 din 22.12.2016 pentru completarea articolului 118 din Codul de procedură penală al Republicii Moldova nr. 122-XV din 14 martie 2003. La 03.02.2017 Legea dată a fost publicată în Monitorul Oficial nr. 30-39, art. 67.

Ținem să menționăm că aprobarea modificărilor propuse au drept scop efectuarea examinării de către organul de urmărire penală a sistemelor informatice sau a suporturilor de stocare a datelor informatice cu consimțământul și în prezența persoanei care deține sau are sub control aceste obiecte, ceea ce ar da o explicație mai clară în cazul acumulării mijloacelor de probe și prezentării acestora în instanța de judecată.

Totodată, la 06.04.2020, IGP al MAI a transmis spre avizare către Procuratura pentru Combaterea Criminalității Organizate și Cauze Speciale (PCCOCS) propuneri de modificare a Codului penal și codului de procedură penală sub aspectul infracțiunilor informaționale. La moment, Procuratura Generală urmează să inițieze elaborarea proiectului de lege privind modificarea și completarea legislației penale și contravenționale pentru prevenirea și

combaterea crimelor informatice în scopul organizării continue a acesteia la prevederile Convenției Europene privind criminalitatea informatică, cît și la deciziile Comitetului Convenției.

Acțiunea 4.2 „Instruirea angajaților organelor de drept, specialiștilor certificați în domeniul securității cibernetice privind: a) depistarea, investigarea, urmărirea penală și judecarea infracțiunilor informatice; b) legătura dintre criminalitatea informatică, crima organizată, infracțiunile economice și alte categorii de infracțiuni"

Termen de realizare: 2016-2020.

Responsabil principal este Institutul Național de Justiție (INJ).

MAI raportează, că în 2019, 13 angajați din cadrul STI au participat la 3 cursuri de instruire în domeniul securității cibernetice, iar angajații CCCI au participat la 32 evenimente, dintre care 8 cursuri la nivel național și 24 cursuri la nivel internațional, fiind instruiți 38 angajați.

Pe parcursul semestrului I al anului 2019, în cadrul INJ au fost realizate 7 activități de formare în domeniu, în cadrul cărora au fost instruiți 184 beneficiari, după cum urmează:

- două seminare cu tematica „Metodici și tactici de identificare, investigare și judecare a infracțiunilor săvîrșite asupra copiilor cu utilizarea tehnologiilor informaționale" (04.04.2019 și 04-05.06.2019), fiind instruiți 54 angajați.
- două seminare cu tematica „Particularitățile urmăririi penale și judecării cauzelor privind infracțiunile în domeniul informaticii și telecomunicațiilor" (05.03.2019 și 03.06.2019), fiind instruiți 54 angajați.
- seminarul „Securitatea informațională și implementarea cerințelor față de asigurarea securității datelor cu caracter personal " (06.03.2019), au fost instruiți 27 angajați.
- seminarul „Specificul activității speciale de investigație la cercetarea infracțiunilor din domeniul informaticii " (09.04.2019). Au fost instruiți 27 angajați.
- cursul „Criminalitatea informatică, crima organizată, infracțiunile economice și alte categorii de infracțiuni: aspect relaționale" (06-07.06.2019). Au fost instruiți 17 angajați.

MAI raportează, că în semestrul I 2020, au fost organizate 21 evenimente la care la care au participat 71 angajați IGP al MAI.

Pe parcursul semestrului I 2020, INJ a efectuat 7 activități de formare în domeniul, fiind instruiți 202 angajați, după cum urmează:

- seminarul online: „Specificul activității speciale de investigație la cercetarea infracțiunilor din domeniul informaticii" 07.05.2020). Au fost instruiți 17 angajați.
- seminarul online: ‚Metodici și tactici de identificare, investigare și judecare a infracțiunilor săvîrșite asupra copiilor cu utilizarea tehnologiilor informaționale" (08-09.06. 2020). Au fost instruiți 26 angajați.
- cursul de instruire „Particularitățile urmăririi penale și judecării cauzelor privind infracțiunile în domeniului informaticii și telecomunicațiilor" (10.06.2020) Au fost instruiți 24 angajați.
- seminarul online: ‚Securitatea informațională și implementarea cerințelor față de asigurarea securității datelor cu caracter personal" (17.06.2020). Au fost instruiți 32 angajați.

Acțiunea 4.3 „Implementarea recomandărilor Consiliului Europei, în special ale proiectului EAP privind instruirea personalului organelor de drept"

Termen de realizare: 2016.

Responsabil principal este INJ.

Academia „Ștefan cel Mare” a MAI a elaborat curriculumul „Securitatea cibernetică și criminalitatea informatică”.

În baza acestui curriculum a implementat programele de studii:

1. programul „Securitatea informațională”, în cadrul căruia au fost informați și instruiți, în perioada 01.01.2016-31.03.2016, 275 de audienți (studenți la an. I, an. II, facultatea de drept și SCOP);

2. programul „Investigarea infracțiunilor informatice prin ASI”, în cadrul căruia au fost efectuate 2 instruiri:

- în perioada 26.01.2016-24.02.2016 au fost instruiți 16 audienți (an.I, ciclul 2, Masterat, Drept Penal);
- în perioada 25.02.2016-15.03.2016 au fost instruiți 21 studenți (an.I, ciclul 2, drept penal);

3. programul „Instrumentarea cazurilor penale privind infracțiunile informatice”, desfășurat în perioada 04.04.2016-08.04.2016, în cadrul căruia au fost instruiți 21 angajați ai MAI;

4. programul „Tactica documentării și investigării infracțiunilor cibernetice” la care au participat, în perioada 04.04.2016-08.04.2016, 21 angajați ai MAI;

5. programul „Infracțiuni informatice: frauda și falsul informatic, accesul neautorizat la serviciile și rețelele de telecomunicații. Analiza juridică a acestora și aspecte privind metodica cercetării”, în cadrul căruia, în perioada 19.09.2016-21.09.2016, au fost instruiți 30 ofițeri de urmărire penală;

6. programul „Utilizarea avansată a softului EnCase în examinarea probelor electronice, inclusiv în cazurile de utilizare a virușilor în statică și dinamică”, în cadrul căruia, în perioada 24.10.2016-28.10.2016, au fost instruiți 35 ofițeri de investigații;

7. programul „Utilizarea softului FTK în examinarea mijloacelor de comunicare mobilă”, în cadrul căruia, în perioada 24.10.2016-28.10.2016, au fost instruiți 35 ofițeri de investigații.

Totodată, pe parcursul anului 2017, 5 angajați ai Centrului pentru combaterea crimelor informatice (CCCI) al IGP al MAI au participat în cadrul a 6 evenimente: 2 la nivel național și 4 la nivel internațional, după cum urmează:

- 25.02-02.03.2017, un angajat al Centrului a participat la atelierul de lucru în cadrul proiectului „The Cybercrime@EAP II project" al Consiliului Europei, în or. Singapore, Republica Singapore;
- 03-06.04.2017, 5 angajați ai Centrului au participat la Programul de training în domeniul cooperării internaționale, inclusiv companii multinaționale prestatoare de servicii internet, pentru regiunea Parteneriatului Estic, eveniment organizat sub egida Consiliului Europei, prin intermediul Oficiului Cybercrime Programme Office (C-PROC) cu sediul la București, România, în mun. Chișinău;
- 06.06-10.06.2017, un angajat al Centrului a participat la ședința planetară a Comitetului Convenției privind criminalitatea informatică (T-CY), eveniment organizat în cadrul proiectul „The CyberCrime@EAP II project" de Consiliul Europei, în or. Strasbourg, Franța;
- 14-17.06.2017, un angajat al Centrului a participat la atelierul de lucru privind strategiile de instruire pentru organele de forță și accesul la materialele Grupului European de formare și instruire în domeniul combaterii criminalității cibernetice, eveniment organizat în cadrul proiectului „The CyberCrimc@EAP II project" de Consiliul Europei, în or. Bruxelles, Belgia;

- 11.09.2017, doi angajați ai CCCI au participat la cea de a 4-a întrunire Regională privind legislația, garanții și cooperare cu ISP, eveniment desfășurat în cadrul programului Cybercrime@EAP III, în RM;
- în perioada 08-12.10.2017, șeful Centrului și un angajat au participat la Conferința regională dedicată combaterii criminalității informatice, eveniment organizat în cadrul proiectului CyberCrime@EAP II, în or. Baku, Republica Azerbaidjan.

Acțiunea 4.4 „Elaborarea și aprobarea proiectului de lege privind ratificarea protocolului adițional la Convenția Consiliului Europei privind criminalitatea informatică"

Termen de realizare: 2016.

Responsabil principal este MAI.

În scopul implementării prevederilor „Protocolului Adițional la Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă și xenofobă săvîrșite prin intermediul sistemelor informatice" adoptat la Strasbourg la 28.01.2003, MAI a elaborat proiectul de Lege pentru ratificarea Protocolului dat.

La 13.01.2017, în Monitorul Oficial a fost publicată Legea nr. 302 din 22.12.2017 pentru ratificarea Protocolului adițional la Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă și xenofobă comise prin intermediul sistemelor informatice.

Acțiunea 4.5 „Ajustarea legislației naționale la prevederile Convenției Consiliului Europei pentru protecția copiilor împotriva exploatării și abuzurilor sexuale și a Protocolului adițional la Convenție (Lanzarote, 25 octombrie 2007)"

Termen de realizare: 2016-2017.

Responsabil principal este MAI.

A fost elaborat proiectul de lege pentru modificarea și completarea unor acte legislative, înregistrat în Parlamentul RM cu nr. 161 din 13.04.2017, care prevedea modificarea și completarea mai multor norme, în vederea ajustării acestora la cadrul juridic internațional. Însă, aceasta nu a fost examinat în prima lectură în cadrul ședinței parlamentare, fiind declarat nul și retras.

Astfel, în urma celor discutate în cadrul ședinței MAEIE a venit cu următoarele propuneri în soluționarea acestei probleme:
- clarificarea competențelor instituționale pentru implementarea Convenției de la Lanzarote, întrucît instrumentul nu se limitează doar la competența funcțională a MAI;
- includerea Convenției de la Lanzarote în competența Consiliului național pentru protecția drepturilor copilului;
- ajustarea mecanismului existent/crearea unui mecanism nou (similar abordării naționale a problematicii vizînd traficul de ființe umane) de interacțiune „modus operandi" dintre autoritățile publice centrale-locale-societatea civilă pentru domeniul protecției drepturilor copilului la general.

În semestrul II 2018 a fost inițiată procedura de elaborare în comun cu Direcția cooperare internațională (DCI) a MAI și cu participarea CI „LaStrada" a mecanismului național de monitorizare a implementării Convenției Lanzarote. Ulterior, la 14.12.2018 a fost elaborat și transmis, în adresa DCI a MAI, proiectul Dispoziției Guvernului privind aprobarea mecanismului național de monitorizare a implementării Convenției Lanzarote. Cu toate acestea, Cancelaria de Stat și MAI nu au ajuns la un numitor comun privind organul principal care urmează să monitorizeze această Convenție.

În perioada 08-09.04.2019 la Strasbourg, Republica Franceză a avut loc Conferința internațională cu genericul „Consolidarea participării societății civile în implementarea și monitorizarea Convenției Consiliului Europei privind protecția copiilor împotriva exploatării și abuzului sexual - Convenția de la Lanzarote”.

La demersul MAEIE din 09.01.2020, MAI a avizat pozitiv proiectul de act normativ elaborat în anul 2018 care vine să reglementeze mecanismul național de monitorizare și raportare a implementării Convenției Lanzarote, promovarea actului fiind preluată de către MAEIE. Totodată, în componența Consiliului Național de coordonare a implementării Convenției Lanzarote au fost desemnați 3 angajați ai MAI și s-a reconfirmat calitatea de expert titular a reprezentantului IGP al MAI.

Acțiunea 4.6 „Efectuarea unui studiu pentru perfecționarea cadrului normativ în domeniul prevenirii și combaterii crimelor informatice”

Termen de realizare: 2016.

Responsabil principal este Procuratura Generală (PG).

În contextul realizării studiului în cauză, PG a efectuat o analiză a situației în domeniul prevenirii și combaterii crimelor informatice și a examinat legislația procesual-penală, măsurile speciale de investigații, a pregătit propuneri de ajustare a legislației naționale la cea internațională.

Toate modificările și completările legislației naționale în principal urmăresc următoarele scopuri:

- adaptarea prevederilor Codului Penal în scopul asigurării realizării politicii penale, reieșind din prevederile Protocolului facultativ la Convenția ONU cu privire la drepturile copilului referitoare la vînzarea de copii, prostituția și pornografia infantilă, ratificat la 22.02.2007, a Convenției Consiliului Europei pentru protecția copiilor împotriva exploatării sexuale și a abuzurilor sexuale, ratificată la 19.12.2011;
- implementarea prevederilor Convenției Consiliului Europei privind criminalitatea informatică, conservarea rapidă a datelor informatice și interceptarea datelor informatice;
- implementarea Convenției Consiliului Europei privind criminalitatea informatică și a Consiliului Europei pentru protecția copiilor împotriva exploatării sexuale și abuzurilor sexuale (Lanzarote 2007), sub aspectul garantării cercetării și urmăririi eficiente a infracțiunilor prevăzute de Convenție;
- implementarea Directivei 2011/92/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile.

Acțiunea 4.7 „Consolidarea în cadrul Procuraturii Generale, Serviciului de Informații și Securitate și Inspectoratului General al Poliției al Ministerului Afacerilor Interne a capacităților pentru prevenirea și combaterea criminalității informatice și, după caz, formularea unor propuneri de modificare a cadrului normativ și crearea unui laborator de testare și expertiză”

Termen de realizare: 2016-2019.

Responsabil principal este MAI.

În scopul consolidării capacităților de prevenire și combatere a criminalității informatice, MAI a întreprins măsuri de perfecționare a cadrelor și de înzestrare cu soft-hardul respectiv a unităților structurale de profil.

Astfel, în perioada de raportare, cu titlu de viitori formatori: 2 persoane au urmat cursuri de instruire în utilizarea softurilor ce țin de criminalistică , iar alta - cursuri de studiere a programului XRY.

A fost procurat echipament pentru examinarea DVR, au fost reînnoite licențele la mai multe produse criminalistice, a fost procurat echipament și soft pentru examinarea sistemelor informatice.

În cadrul Centrului pentru combaterea crimelor informatice (CCCI) a fost creat Serviciul Suport Operațional care a fost dotat cu tehnica necesară pentru examinarea sistemelor informatice și dispozitive de stocare a informației.

Ofițerii de investigații ai CCCI acordă asistență tehnică subdiviziunilor INI ale IGP la investigarea infracțiunilor comise prin utilizarea sistemelor informatice și a mijloacelor tehnice moderne (Dispoziția INI a IGP nr. 9/7478 din 16.08.2016).

Procuratura Generală a întreprins următoarele măsuri:

1. a analizat informația statistică a hotărîrilor adoptate pe cauzele penale de investigare a infracțiunilor informatice și conexe acestora, fiind expediate în teritoriu solicitări de actualizare a datelor statistice;
2. a efectuat studiul statistic al stării de fapt în domeniul investigării infracțiunilor de pornografie infantilă pentru anii 2013-2017;
3. a efectuat studiul situației în domeniul prevenirii și combaterii criminalității informatice pentru anul 2017;
4. a elaborat propuneri cu privire la necesitățile material-tehnice ale Procuraturii ce țin de consolidarea securității informaționale;
5. a elaborat propuneri cu privire la necesitățile material-tehnice ale Procuraturii ce țin de implementarea Sistemului Informațional Automatizat Integrat „Urmărire penală: E-Dosar”;
6. a achiziționat bunurile și tehnica necesară pentru implementarea Sistemului;
7. începînd cu 01.07.2017, prin Ordinul Procurorului General a fost pus în aplicare sistemul, cu introducerea zilnică de către procurori, consultanții acestora și specialiști a informației privind activitatea efectuată în cadrul cauzelor penale;
8. în acest sens, a elaborat Ghidul utilizatorului privind Sistemul.
9. Secția Tehnologii Informaționale și combaterea crimelor cibernetice din cadrul Direcției Urmărire penală și criminalistică a Procuraturii Generale este responsabilă de administrarea Sistemului, asigurarea accesului la sistem și monitorizarea completării bazei de date, acordarea asistenței metodologice, practice privind modul de utilizare a sistemului. În perioada 24.05.2017-30.06.2017 au fost petrecute instruiri cu toți procurorii, consultanții acestora și specialiștii din cadrul Procuraturii Generale, precum și din cadrul procuraturilor teritoriale și specializate, referitor la completarea și utilizarea sistemului, monitorizarea veridicității și plenitudinii datelor introduse în Sistem, precum și operarea corectărilor în cazul introducerii datelor eronate. Pînă la data de 31.07.2017, în Sistem au fost introduse de către procurori, consultanții acestora și specialiști circa 2520 cauze penale și soluțiile adoptate, precum și prejudiciul stabilit;
10. a acumulat și generalizat informația cu privire la respectarea prelucrării datelor cu caracter personal în cadrul Procuraturii pentru anul 2016, urmare accesării procurorilor a bazelor de date ale Î.S. "CRIS-"Registru", Serviciului Vamal și Î.S. "Cadastru";
11. a verificat registrele de accesare a acestor baze de date, ținute de către procurori;
12. a acumulat și actualizat datele statistice cu privire la investigarea infracțiunilor cibernetice și celor conexe acestora de către organele procuraturii;

13. a adoptat și implementat ordinul Procurorului General cu privire la aprobarea modelului Registrului accesărilor bazelor de date ale instituțiilor publice și regulile de ținere a acestuia;

14. a desemnat procurori din procuraturile teritoriale și specializate responsabili (specializați) în domeniul bazelor de date și investigării infracțiunilor cibernetice;

15. a fost elaborat Raportul național privind riscurile în cadrul criminalității cibernetice, potrivit prevederilor Ordinului comun nr. 75/01/342/10/19/9 din 12.03.2016 cu privire la aprobarea „Concepției pentru analiza riscurilor în domeniul combaterii criminalității cibernetice";

16. s-a implicat în proiectul Uniunii Europene „Suport pentru asigurarea respectării drepturilor de proprietate intelectuală", obiectivul căruia este îmbunătățirea modului de aplicare a cadrului legal și de reglementare în domeniul protecției drepturilor de proprietate intelectuală în Republica Moldova. Unul din scopuri constă în eficientizarea comunicării și coordonării autorităților naționale responsabile de implementarea legislației cu privire la DPI.

17. s-a implicat în proiectul "No more ransom", solicitat de Centrul de Cooperare Polițienească Internațională (INTERPOL).

În vederea asigurării conectării sistemelor informaționale ale Procuraturii Generale la platforma de interoperabilitate MConnect, pentru efectuarea schimbului de date și metadate dintre diferiți beneficiari, a fost semnat Acordul de colaborare dintre Agenția de Guvernare Electronică și Procuratura Generală privind utilizarea platformei de interoperabilitate (MConnect) nr. 3009-108.

Această platformă va asigura interconectarea securizată a Sistemului informațional automatizat „E-Dosar" la sistemele informatice ale altor autorități publice centrale ale Ministerului Afacerilor Interne, Ministerului Justiției, Centrului Național Anticorupție și ale altor instituții.

V. OBIECTIVUL SPECIFIC „CONSOLIDAREA CAPACITĂȚILOR DE APĂRARE CIBERNETICĂ"

Implementarea acestui obiectiv specific se va realiza prin executarea a 6 acțiuni din PAI PNSC 2016-2020.

În semestrul I 2020, în conformitate cu termenele stabilite pentru realizarea acestui obiectiv, au fost continuate activitățile de realizare a acestora inițiate în a semestrul II 2019, rezultatele executării cărora se expun după cum urmează.

Acțiunea 5.1 „Elaborarea compartimentului de apărare cibernetică a Republicii Moldova, ca parte componentă a Strategiei securității informaționale a Republicii Moldova"

Termen de realizare: 2016.

Responsabil principal este SIS.

În Hotărîrea Parlamentului 257/2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia este inclus compartimentul de apărare cibernetică.

Acțiunea 5.2 „Stabilirea autorităților responsabile și cooperarea reciprocă pe timp de pace, în situații de criză, asediu și război în cadrul spațiului cibernetic"

Termen de realizare: 2016-2017.

Responsabil principal este SIS.

În conformitate cu prevederile SSI și PAI 2019-2024 se creează Consiliul coordonator pentru asigurarea securității informaționale, entitatea cu competențe de promovare și coordonare a politicilor de securitate informațională.

Acțiunea 5.3 „Valorificarea oportunităților spațiului cibernetic pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic"

Termen de realizare: 2016-2018.

Responsabil principal este SIS.

SIS comunică că a inițiat procesul de executare a acestei acțiuni. Astfel, în calitate de instituție responsabilă, a studiat practica țărilor europene pe domeniul dat. Ca urmare, în Strategia securității informaționale a Republicii Moldova și în Planul de acțiuni pentru implementarea acesteia a fost introdus obiectivul privind crearea rețelei de CERT-uri, misiunea căreia rezidă în asigurarea unui spațiu cibernetic protejat la nivel național. În acest sens, odată cu crearea Consiliului coordonator pentru asigurarea securității informaționale, se va lansa o platformă de comunicare destinată diseminării comunicatelor, alertelor, recomandărilor și altor informații utile pentru mediul public/privat și societatea civilă, competență care în mare parte revine și CERT-ului național.

Totodată pentru valorificarea oportunităților spațiului cibernetic, SIS se află în proces de transpunere în legislația națională a cadrului normativ UE, și anume, a Regulamentului 910/2014, ceea ce în rezultata va impulsiona dezvoltarea serviciilor digitale de încredere aferente semnăturii electronice.

Acțiunea 5.4 „Dezvoltarea capabilităților militare de protecție a infrastructurii și serviciilor critice destinate apărării naționale"

Termen de realizare: 2016-2017.

Responsabil principal este Ministerul Apărării (MA).

MA a identificat un șir de riscuri și vulnerabilități care au fost incluse în Strategia națională de apărare pentru anii 2018–2022, aprobată prin Hotărîrea Parlamentului nr. 134 din 19.07.2018 și în Strategia securității informaționale a Republicii Moldova pentru anii 2019–2024, aprobată prin Hotărîrea Parlamentului nr. 257 din 22.11.2018

Conceptul de dezvoltare a capabilităților de apărare cibernetică în cadrul Armatei Naționale a fost elaborat și aprobat prin act normativ intern, de asemenea, a fost elaborat și aprobat Planul de acțiuni, ca parte componentă a Proiectului de creare a Centrului de Reacție și Răspuns la Incidente Cibernetice a Forțelor Armate cu suportul Programului NATO „Știință pentru Pace", vizat de Ministrul Apărării și aprobat de către Consiliul NATO la data de 03.04.2017, termenul implementării fiind august 2020.

Concomitent, în cadrul structurilor Armatei Naționale sînt întreprinse măsuri organizatorice și tehnice pentru dezvoltarea capabilităților de apărare cibernetică prin crearea, instruirea și dezvoltarea unei echipe CERT cu rol de detectare, prevenire și reacție rapidă împotriva incidentelor cibernetice.

În același timp MA menționează că, acțiunea 5.4 se regăsește în Planul de acțiuni pentru implementarea Strategia Securității Informaționale și va fi realizată în conformitate cu noile termene.

În aceeași ordine de idei, SIS, în calitate de instituție partener, a efectuat un studiu a Directivei 2008/114/CE a Consiliului din 02.12.2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, precum și cadrul legislativ în domeniul infrastructurii critice a altor state, în vederea

elaborării proiectului de lege privind identificarea și desemnarea infrastructurii critice naționale. La moment, proiectul se află în procesul de elaborare.

Acțiunea 5.5 „Stabilirea programelor de conștientizare și educare a personalului destinat securității și apărării naționale în domeniul securității cibernetice”

Termen de realizare: 2016-2017.

Responsabil principal este SIS.

În scopul stabilirii programelor de conștientizare și educare a personalului destinat securității și apărării naționale în domeniul securității cibernetice, MAI a asigurat participarea angajaților subdiviziunilor MAI la un șir de cursuri de instruire și evenimente ce țin de securitatea cibernetică:

1. „Gestionarea incidentelor și managementul restabilirii”, desfășurat în perioada 28.11.2016-02.12.2016 în cadrul Ministerului Apărării, curs ce a cuprins lecții de securitate cibernetică atît teoretice, cît și practice;

2. „Educația și Conștientizarea Securității Cibernetice”, desfășurat în perioada 12.12.2016-16.12.2016 în cadrul Ministerului Apărării, curs care a cuprins atît lecții teoretice, cît și practice în vederea evaluării, gestionării și aplicării programului de management al riscurilor bazat pe principii, practici și concepte de securitate cibernetică;

3. „Securitatea digitală și spionajul mobil”, workshop destinat specialiștilor IT și de securitate informațională, organizat de STISC în comun cu Proiectul de Îmbunătățire a Securității Cibernetice;

4. Evenimentul organizat de „RSD Day – innovate with us”, ediția a 7-a și realizat în parteneriat cu „StarNet”, sesiune de securitate în cadrul căreia au fost discutate soluții de securitate informațională, prezentate de către reprezentanții companiilor Bitdefender, McAfee, CoSoSyS, IBM, Digital Guardian, TITUS, Netwrix;

5. Lansarea în cadrul Universității Tehnice a Moldovei a Laboratorului de securitate cibernetică, creat și implementat în cadrul proiectelor partenerilor internaționali NATO, Ambasada Statelor Unite ale Americii și Ambasada Estoniei.

Totodată, angajații din cadrul STI al MAI pe parcursul anului 2017 conform solicitărilor parvenite, au participat la data de 27.10.2017 la Conferința „CyberSec 2017„ eveniment organizat în cadrul Lunii Europene a Securității Cibernetice 2017: Uniți împotriva amenințărilor cibernetice, organizată de STISC în parteneriat cu A.O Centrul pentru Securitate Juridică a Informației, Asociația Națională a Companiilor Private din Domeniul TIC și Ambasada Statelor Unite ale Americii.

Ulterior, la data de 21-23 noiembrie 2017 s-a participat la Exercițiul regional Cyber Drill ALERT 2017, organizat de către STISC din cadrul Cancelariei de stat, în parteneriat cu Uniunea Internațională a Telecomunicațiilor, ce a avut drept scop îmbunătățirea capacității de comunicare și de răspuns a participanților la incidente cibernetice și însușirea bunelor practici oferite de experți internaționali și reprezentați ai echipelor CSIRT(Computer security incident response teams).

SIS informează despre participarea la ședințe cu reprezentanții Ministerului Apărării, IGP, CNA, AGE, ASP și CNPDCP pentru acordarea ajutorului metodic în implementarea "Măsurilor de protecție tehnică și criptografică a secretului de stat", în scopul creării cerințelor specifice de securitate a sistemelor informaționale în cadrul cărora va fi prelucrată informația atribuită la secretul de stat.

În informațiile prezentate nu sînt careva referințe la programele respective de conștientizare și educare stabilite, identificate sau aprobate.

Angajații Ministerului Apărării participă anual în cadrul pregătirii profesionale a efectivului din organele de conducere a Armatei Naționale și în cadrul exercițiilor și antrenamentelor pe domeniul comunicații și informatică.

Acțiunea 5.6 „Stabilirea relațiilor de cooperare cu instituțiile naționale și cele internaționale din domeniu"

Termen de realizare: 2016-2018.

Responsabil principal este SIS.

SIS asigură permanent schimbul de informații privind amenințările și incidentele de securitate informațională cu serviciile speciale partenere.

PG, în cadrul unor cauze penale cu privire la investigarea infracțiunilor transnaționale, inclusiv în domeniul informaticii, a încheiat acorduri cu privire la crearea echipelor comune de investigații împreună cu autoritățile competente ale altor state, EUROPOL și EUROJUST.

Ministerul Apărării a inițiat relații de cooperare în domeniul apărării cibernetice cu România.

VI. OBIECTIVUL SPECIFIC „EDUCAȚIA, FORMAREA ȘI INFORMAREA CONTINUĂ ÎN DOMENIUL SECURITĂȚII CIBERNETICE"

Implementarea acestui obiectiv specific se va realiza prin executarea a 6 acțiuni din PAI PNSC 2016-2020.

În sem. II 2019, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, au fost continuate activitățile de realizare a acestora inițiate în sem. I 2019, rezultatele executării cărora se expun după cum urmează mai jos.

Acțiunea 6.1 „Elaborarea conceptului campaniilor de informare și conștientizare despre riscurile spațiului cibernetic"

Termen de realizare: 2016-2017.

Responsabil principal este CS.

În 2018, STISC raportează despre elaborarea Caietului de sarcini privind organizarea unei campanii de informare și conștientizare despre riscurile spațiului cibernetic. La data de 01.02.2019, prin Procesul verbal nr. 1 al Consiliului, a fost aprobată Strategia de comunicare a STISC care trasează obiective bine determinate pentru o comunicare eficientă, planifică acțiunile de comunicare și explică prin proceduri standardizate implementarea acestora. Scopul strategiei este de a răspunde necesităților de informare a autorităților administrației publice și a cetățenilor cu privire la activitățile și reformele din domeniul tehnologiei informaționale și securitate cibernetică.

Potrivit informațiilor prezentate, CNPDCP informează continuu societatea (prin prisma domeniului protecției datelor cu caracter personal) despre riscurile spațiului cibernetic, măsurile minime de securitate, cazurile de rezonanță social sporită în domeniu, date statistice relevante etc.

Acțiunea 6.2 „Completarea curriculumului de învățământ în domeniul securității cibernetice"

Termen de realizare: 2016-2018.

Responsabil principal este Ministerul Educației, Culturii și Cercetării (MECC).

Ministerul Educației, Culturii și Cercetării este în proces de revizuire a Curriculumului Național, care presupune și dezvoltarea curriculara pe discipline școlare, respectiv vor fi actualizate și completate conținuturile cu privire la securitatea cibernetică în curriculum școlar.

Conform Planului de activitate al MECC, pentru noiembrie 2017 au fost planificate 2 activități, și anume:

- implicarea cadrelor didactice în activități de informare și sensibilizare ale copiilor și adolescenților în cadrul „Lunii securității cibernetice”, zilei „Siguranța în Internet”;
- revizuirea și implementarea modulelor „Siguranța în mediul online a copiilor/elevilor” în curricula specialităților pedagogice (formare inițială și continuă).

De asemenea, potrivit informației prezentate de Academia de Administrare Publică, pe perioada raportării, a fost creat Modulul de instruire Guvernarea Electronică (total 24 de ore) cu elementele:

- modernizarea Tehnologică a guvernării;
- E-servicii;
- elemente de management al schimbării;
- managementul proiectelor TI;
- interoperabilitatea serviciilor publice;
- securitatea informațională;
- politici de securitate;
- tehnologii Cloud computing și securitatea cibernetică;
- comunicare eficientă în spațiul virtual informațional.

AGE, a inclus module cu elemente de securitate cibernetică sau totalmente dedicate Securității Cibernetice în cadrul a 3 cursuri:

- pentru funcționarii publici începători în cursul "Introducerea în Funcția Publică", inclusiv Modulul de e-Transformare - 3 zile;
- pentru funcționarii publici cu experiență în cursurile de consolidare a capacităților, inclusiv modulul de 1 zi privind Agenda de e-Transformare a Guvernării;
- masteratul in TI, inclusiv Modulul Securitate Cibernetică.

Conform datelor de care dispune AGE, pînă la 30.12.2016, în cadrul cursurilor respective, organizate la AAP, au fost instruiți peste 1300 funcționarii publici.

Potrivit opiniei prezentate de STISC, educația în domeniul tehnologiei informației și comunicațiilor în Moldova este o problemă recunoscută la nivel național. În pofida unui număr mare de absolvenți, se observă fenomenul că cei mai mulți dintre ei nu dețin abilități practice adecvate pentru a lucra in domeniul TIC și, în mod special, în domeniul securității cibernetice. Printre cauzele principale ale acestui fenomen sînt deficitul de profesori calificați, lipsa unui curriculum și a unei baze educaționale care să satisfacă cerințelor actualului nivel de dezvoltare TIC. Toate acestea, împreună cu un nivel scăzut de alfabetizare digitală a populației, au făcut sectorul public și cel privat să fie o țintă ușoară pentru infractorii cibernetici.

Acțiunea 6.3 „Crearea unui portal cu anunțarea operativă a pericolelor din spațiul cibernetic (digital)”

Termen de realizare: 2016-2018.

Responsabil principal este CS.

STISC relatează că în octombrie 2018 a fost lansat portalul www.stisc-cert.gov.md destinat înștiințării publicului larg despre pericolele din spațiul cibernetic. Portalul este unul ușor navigabil și pune la dispoziția utilizatorului informații pe dimensiunea securității cibernetice despre cele mai recente avertizări și amenințări, instrucțiuni și instrumente de securitate cibernetică. De asemenea, portalul prevede un modul pentru raportarea incidentelor cibernetice, iar pentru informare sînt publicate ghiduri de securitate cibernetică, recomandări

de securitate și cele mai actuale alerte. La moment, pe pagina web este publicată lista alertelor de securitate și instrumentele necesare de securitate.

Acțiunea 6.4 „Stabilirea cerințelor de competență în domeniul securității cibernetice pentru personalul din sectorul public și privat, precum și organizarea procesului de instruire, evaluare și certificare a specialiștilor pentru acest domeniu”

Termen de realizare: 2016-2018.

Responsabil principal este MEI.

Prin Hotărîrea Guvernului nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, a fost modificată HG 100/2017, transferîndu-se atribuțiile de implementare a politicii statului în domeniul securității cibernetice Serviciului Tehnologia Informației și Securitate Cibernetică și Agenției de Guvernare Electronică.

Asigurarea securității cibernetice prin fortificarea capacităților instituționale în domeniul respectării cerințelor minime obligatorii de securitate cibernetică reprezintă o acțiune prioritară în activitatea STISC, astfel CERT-GOV-MD oferă, la solicitare, cursuri de instruire în domeniile de competență ale Serviciului în vederea reducerii riscurilor de incidente ale securității TI și acordarea asistenței în reacționarea la acestea din urmă. Prin urmare, este important ca organizațiile să sesizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze pozitiv acest subiect printr-o conștientizare în rîndul angajaților, înțelegerea tipologiei amenințărilor și vulnerabilităților specifice mediilor informatizate și aplicarea practicilor de control.

Domeniile de competență ale AGE includ, ca funcție de bază, organizarea cursurilor de instruire privind implementarea cerințelor minime de securitate cibernetică și sporirea competențelor în securitate cibernetică pentru coordonatorii de securitate cibernetică din autoritățile publice.

Totodată, alte cerințele de competență generală a personalului în cauză au fost incluse în proiectele elaborate în cadrul acțiunilor prevăzute la pct. 1.5 și pct. 2.2 din PAI PNSC 2016-2020.

Acțiunea 6.5 „Organizarea și efectuarea trainingurilor și workshopurilor în domeniul securității cibernetice pentru personalul din sectorul public și privat, deținătorii de elemente de infrastructură critică”

Termen de realizare: permanent.

Responsabil principal este MEI.

În cadrul Săptămînii Securității Cibernetice, eveniment planificat pentru perioada octombrie - noiembrie 2019, STISC va organiza trening-uri și workshop-uri în domeniul securității cibernetice pentru personalul din sectorul public și privat deținătorii de elemente de infrastructură critică.

Ministerul Apărării (MA) raportează că, în semestrul I 2019 au fost instruiți 24 specialiști în cadrul cursului de Management al incidentelor cibernetice cu suportul programelor de asistență externă NATO School Oberammergau, Germania.

La 12 iulie 2019 Agenția de Guvernare Electronică a organizat un seminar de inițiere a auditului de securitate cibernetică în autoritățile publice întru implementarea HG nr.201/2017 „Privind aprobarea Cerințelor minime obligatorii de securitate cibernetică”, în cadrul căruia au fost discutate următoarele subiecte:

1. contextul si obiectivele auditului de securitate cibernetică;
2. modalitatea de organizare și efectuare a auditului;

3. constrîngerile, limitările și riscurile în procesul de audit;
4. linii de comunicare și aspectele logistice în cadrul misiunilor de audit;
5. comunicarea și validarea rezultatelor auditului.

Un eveniment important, care se desfășoară anual în sectorul public, este Luna Securității Cibernetice (luna octombrie). În cadrul acestui eveniment, Ministerul Economiei și Infrastructurii, Ministerul Afacerilor Interne, Ministerul Apărării, Serviciul de Informații și Securitate, Agenția de Guvernare Electronică, STISC în comun cu parteneri internaționali, organizează un șir de evenimente de informare, discuții și instruire în formatul training sau workshop pe diverse subiecte ce țin de Securitate Cibernetică și Securitatea informației în Guvern.

Circa 300-350 de funcționari publici, reprezentanți ai mediului academic și sectorului privat participă anual la acest eveniment.

În vederea dezvoltării competențelor și abilităților de reacție a personalului la apariția unor incidente de securitate, la data de 26.07.2018 75 de angajați ai MEI au participat la sesiunea de instruire cu privire la amenințările cibernetice organizate de STISC.

AGE anual distribuie funcționarilor publici din autoritățile APC și APL materiale informative diseminate în format electronic și pe suport de hîrtie (calendare cu regulile securității informației – 1000-1500 anual, buclete, reflectorizante etc.). În contextul implementării Hotărîrii Guvernului nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică, întru sporirea competențelor în securitate cibernetică pentru coordonatorii de securitate cibernetică din autoritățile publice, la data de 17.12.2018 AGE a organizat un seminar cu tema „Organizarea sistemului intern de securitate cibernetică”.

STISC organizează mai multe exerciții de securitate cibernetică la care participă atît funcționari din sectorul public, cît și privat, precum și mediul academic. Necesitatea pentru un răspuns rapid și eficient în caz de incidente cibernetice, cunoașterea procedurilor și a fluxurilor de informații este esențială și participanții au fost instruiți în acest sens. Aceste exerciții sînt un reper important pentru construirea încrederii, pentru mai bună înțelegere a mecanismelor de cooperare cibernetică existente la nivel de instituții și pentru consolidarea gestionării la nivel de Guvern a incidentelor cibernetice.

STISC a fost solidar campaniei de conștientizare privind amenințările cibernetice la nivelul UE și a organizat la data de 27.10.2017, Chișinău, Conferința “CyberSec 2017". Acest eveniment face parte din Luna Europeană a Securității Cibernetice (ECSM), o campanie de conștientizare la nivel european. În cadrul Campaniei din acest an, au fost discutate tematici precum securitatea cibernetică la locul de muncă și acasă, guvernanță și protecția vieții private, a datelor și a dezvoltării competențelor specifice domeniului.

În luna martie 2018, la inițiativa STISC, un grup de experți din cadrul Departamentului de Stat al Statelor Unite și Institutului de Inginerie Software (SEI), Universitatea Carnegie Mellon, au efectuat o vizită de lucru în Moldova. În cadrul vizitei, experții au purtat discuții atît cu reprezentanți din sectorul public/privat cît și mediul academic, cu scopul de a identifica și aprecia capabilitățile instituționale cibernetice, precum și care ar fi mecanismele necesare (instituționale, legale, tehnice și resurse umane) pentru a fi ulterior dezvoltate în proiecte și implementate.

În cadrul acestei vizite s-a organizat și un Workshop tematic “Crearea/Gestionarea unui CSIRT”, în cadrul căruia, experții din cadrul Institutului de Inginerie Software au oferit o prezentare generală privind aspectele cheie în crearea și gestionarea unui CSIRT, inclusiv și instrumentele necesare pentru a răspunde eficient incidentelor survenite din spațiul

cibernetic. Conform programului, vor fi puse în discuție subiecte precum: modul în care CSIRT-ul interacționează cu factorul de decizie politică; rolul și responsabilitățile unui CSIRT; nevoile și obiectivele strategice ale Republicii Moldova, etc.

În luna iunie 2018, Centrului de excelență Tekwill, „Reliable Solutions Distributor" în parteneriat cu STISC și "Universitatea Tehnică a Moldovei", au organizat un eveniment important pentru industria de securitate cibernetică din Republica Moldova –"BitDefender Day". Spionajul cibernetic, criptarea datelor cu pierderea lor, furtul de date și expunerea lor publică, spargerea rețelei și preluarea accesului asupra acesteia, precum și vulnerabilitatea din lipsa de securitate informațională este cauza cea mai frecvent întîlnită în situațiile de atacuri cibernetice și furturi de date. Consecințele sînt și mai grave din moment ce o mare parte din sistemele de apărare cibernetică folosite de operatorii de infrastructură critică din Moldova continuă a fi depășite și ineficiente. Experții Bitdefender Romania au prezentat cele mai actuale tendințe ale atacurilor cibernetice și riscurile atacurilor de tip hacking, precum și cele mai inovatoare soluții de securitate, contribuind direct la ridicarea nivelului de informare și cunoaștere a domeniului de securitate informațională, ridicînd astfel Moldova la nivelul țărilor cu securitate informațională înaltă și performantă.

În luna iulie 2018 un grup de experți din cadrul Departamentului de Stat al Statelor Unite ale Americii și Pacific Northwest National Laboratory (PNNL), cu asistența organizatorică acordată din partea Serviciului Tehnologia Informației și Securitate Cibernetică (STISC), au întreprins o vizită de lucru în Republica Moldova cu scopul de a consulta și dialoga cu reprezentanții sectorului guvernamental, TIC, financiar și energetic pe tema "Infrastructuri critice naționale – situația la zi și măsuri de protecție". Reprezentanții delegației au apreciat viziunea și acțiunile întreprinse de STISC în vederea cunoașterii, anticipării, prevenirii și contracarării amenințărilor la adresa infrastructurilor critice, ținînd neapărat să reitereze rolul acestor acțiuni în pregătirea organizațiilor guvernamentale, pentru a face față amenințărilor de tip atac terorist, dezastre naturale, epidemii și atacuri cibernetice.

De asemenea, pe 26.07.2018 Centrul de Răspuns la Incidente Cibernetice CERT-GOV-MD din cadrul STISC a organizat prima rundă de instruiri a funcționarilor publici privind respectarea cerințelor minime obligatorii de securitate cibernetică. Angajații au fost familiarizați cu provocările și riscurile parvenite din mediul cibernetic și nu în ultimul rînd cu educarea unor deprinderi minim necesare și obligatorii pentru siguranța online atît în cadrul instituției cît și în mediul privat.

În perioada 29.10–02.11.2018 STISC a organizat un eveniment regional dedicat securității cibernetice – Moldova Cyber Week 2018, alăturîndu-se astfel campaniei europene de conștientizare #CyberSecMonth, aducînd în prim plan subiectul Securității Cibernetice.

În cadrul Săptămînii Securității Cibernetice, pentru personalul din sectorul public și privat, deținătorii de elemente de infrastructură critică, STISC a organizat pe parcursul perioadei de 31.10 – 02.11.2018, o serie variată de Workshop-uri:

1. Workshop-uri despre cele mai inovatoare soluții de securitate:
- „Gestionarea mobilității moderne a securității";
- „Asigurarea protecției înalte a datelor pe rețelele hibride";
- „Microsoft 365 Intelligent Security";
- „Veeam Backup", Back-up și replicare în Veam; Veeam Backup pentru Microsoft Office 365;
- „Bitdefender - Platforma de infrastructură securizată".
- Cisco Networking Academy course: CCNACyberOps;
2. Workshop „Ce înseamnă GDPR pentru companiile din Moldova";

3. Workshop „Safe Kids”.

În contextul realizării acestei acțiuni MAI comunică, că angajații din cadrul STI al MAI, pe parcursul anilor 2016-2017, au participat la diverse ședințe de instruire a specialiștilor IT, desfășurate de către companii prestatoare de servicii de asigurare a securității informaționale și de instituțiile publice:

- Conferința informativă, desfășurată de către compania "BitDefender", în cadrul căreia au fost prezentate soluții de asigurare a securității informaționale a stațiilor de muncă, de asigurare a necesităților cu hardware și software de protecție; seminarul organizat de MEI cu suportul reprezentanților IT din afara hotarelor țării (Moldova – GCCD Cybersecurity Joint Seminar);
- Workshop-ul "Securitatea digitală și spionajul mobil" (sesiune specială pentru specialiști-IT și de securitate informațională), organizat de STISC cu suportul Proiectului de Îmbunătățire a Securității Cibernetice.

Acțiunea 6.6 „Crearea unui laborator de securitate cibernetică”

Termen de realizare: 2016-2018.

Responsabil principal este STISC.

La inițiativa STISC, în cadrul Programului NATO „Știință pentru pace și securitate”, cu suportul Ambasadei SUA și Ambasadei Estoniei din RM a fost creat *Laboratorul de cercetare și instruire în domeniul securității cibernetice*. Scopul creării acestui laborator a fost crearea capacităților de răspuns la problemele complexe de securitate cibernetică. Laboratorul organizează cursuri de instruire ce țin de securitatea cibernetică, exerciții de securitate cibernetica, training-uri, experimente, activități de cercetare pentru funcționari publici și studenți. Ulterior acești studenți vor fi atrași în cîmpul muncii din cadrul instituțiilor publice. Laboratorul a fost lansat oficial în luna octombrie 2016.

În martie 2018, cu suportul financiar din partea Bitdefender, a fost creat un *nou Laborator de securitate cibernetică* în cadrul Universității tehnice din Moldova. Crearea acestui laborator reprezintă un pas important și tangibil în vederea fortificării capacităților de lucru a specialiștilor atît de necesari la ziua de azi, pentru a administra eficient și în condiții de maximă siguranță infrastructurile IT, fiind capabili în același timp să remedieze vulnerabilitățile și să contracareze amenințările de securitate.

VII. OBIECTIVUL SPECIFIC „COOPERAREA ȘI INTERACȚIUNEA INTERNAȚIONALĂ ÎN SFERELE CE ȚIN DE SECURITATEA CIBERNETICĂ”

Implementarea acestui obiectiv specific se va realiza prin executarea a 7 acțiuni din PAI PNSC 2016-2020.

În sem. II 2019, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, au fost continuate activitățile de realizare a acestora inițiate în sem. I 2019, rezultatele executării cărora se expun după cum urmează mai jos.

Acțiunea 7.1 „Încheierea acordurilor de cooperare cu alte echipe naționale de răspuns la incidentele legate de securitatea cibernetică (CERT), precum și US–CERT, europene și nord-atlantice (NATO NCERT)”

Termen de realizare: 2016-2018.

Responsabil principal este CS.

Centrul de răspuns la incidente cibernetice CERT-GOV-MD este acreditat și recunoscut ca membru al comunității internaționale Trusted-Introducer (TI) din ianuarie 2014, comunitate care a fost înființată în Europa în anul 2000 pentru a facilita colaborarea între echipele de răspuns și, prin urmare, pentru a crește nivelul de securitate prin răspunsul mai

rapid la atacurile în desfășurare și a amenințărilor de tip nou. Comunitatea TI asigură o bază de încredere, cu servicii adiționale specializate pentru toate echipele de răspuns la incidente de securitate. De asemenea, TI administrează o bază de date cu informații despre astfel de echipe existente și oferă o imagine de ansamblu actualizată asupra nivelului lor demonstrat de maturitate și abilitate.

Echipa CERT-GOV-MD ajută utilizatorii să reacționeze la atacurile îndreptate asupra echipamentelor IT, indiferent de tehnologia utilizată sau din ce organizație face parte utilizatorul respectiv.

Din iunie 2018 CERT-GOV-MD din cadrul STISC este primul și unicul CERT din Moldova acreditat de comunitatea FIRST (Forumul de reacție la incidente și echipele de securitate), care include peste 420 de echipe CERT/CSIRT din 87 de țări. Comunitatea FIRST are ca obiectiv coordonarea și cooperarea pentru prevenirea incidentelor și stimularea reacțiilor rapide, împreună cu facilitarea transferului de informații/cunoștințe/practici între membri. Fiecare echipă de răspuns la incidente de securitate poate asista comunitatea locală și, respectiv, coordona răspunsul adecvat cu alte echipe pentru a oferi o soluție globală la problemele identificate.

Calitatea de membru FIRST, permite CERT-GOV-MD să-și fortifice capacitățile de răspuns la incidentele de securitate cibernetică, cît și să aplice cele mai bune metodologii și practici de prevenire și combatere a crimelor cibernetice, utilizînd cunoștințe, abilități și experiențe obținute în urma colaborării cu membrii comunității internaționale.

În cadrul acestor două comunități: Trusted-Introducer și FIRST sînt echipe CERT din toată lumea, ceea ce prezintă o platformă profesională de colaborare și cooperare la nivel internațional. STISC a semnat acorduri de cooperare cu echipe de tip CERT din Europa, Asia Centrală, sectorul privat.

Totodată, conform prevederilor Strategiei de securitate a informației și odată cu aprobarea cadrului legal care va reglementa activitatea CERT Gov, STISC va întreprinde măsurile necesare pentru crearea mecanismelor de cooperare cu subdiviziunile de tip Centre departamentale de reacție la incidente de securitate cibernetică (CERT-departamental), care urmează a fi desemnate în cadrul tuturor entităților publice ce dețin sisteme informaționale de stat, în scopul stabilirii unui dialog eficient între CERT Gov și subdiviziunile de tip Centre departamentale de reacție la incidente de securitate cibernetică în scopul stabilirii modalității de raportare, stocare și prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale.

Acțiunea 7.2 „Elaborarea unei platforme de coordonare și consultare în ceea ce privește evaluarea amenințărilor cibernetice și identificarea soluțiilor”

Termen de realizare: 2016-2018.

Responsabil principal este CS.

Evaluarea amenințărilor cibernetice și identificarea soluțiilor potrivite este un proces sistemic în activitatea STISC, bazat pe surse de date colectate de la parteneri (Shadowserver Foundation, Computer Emergency Response Team for federal agencies, Network Security Research Lab at 360), care includ diverse informații culese din surse publice sau restricționate, cum ar fi sistemele de detectare, precum IPSS, firewall-urile, site-urile web specializate etc. O altă categorie de alerte primite sînt cele prin intermediul sistemelor de detecție automate. Aceste tipuri de alerte sînt trimise doar de organizații specializate, cum ar fi de exemplu CSIRT-urile internaționale sau alte companii de securitate, care dețin în posesia lor sisteme de detectare a incidentelor de securitate cibernetică.

Acțiunea 7.3 „Dezvoltarea cooperării cu sectorul privat (identificarea unor aplicații necesare implementării măsurilor de securitate; înființarea de puncte de contact în vederea asigurării solicitării unor date și informații conform prevederilor legale și stabilirea unui sistem modern de transmitere a solicitărilor; realizarea de întruniri periodice în cadrul unor forumuri de dezbateri pentru cunoașterea mai bună a situației operative și pentru înțelegerea nevoilor fiecărei instituții)"

Termen de realizare: 2016-2019.

Responsabil principal este CS.

În vederea asigurării securității cibernetice la nivel național, parteneriatele public-private sînt indispensabile. Protejarea spațiului virtual reprezintă o responsabilitate partajată și care poate fi eficient realizată prin colaborarea dintre Guvern și sectorul privat.

STISC pune accent pe intensificarea eforturilor de colaborare cu alte țări precum și organizații internaționale pe subiectul dezvoltarea proiectelor în domeniul securității cibernetice, pentru a pregăti specialiști care să răspundă noilor amenințări cibernetice precum și care ar fi cele mai bune practici tehnici de remediere în caz că instituția a fost atacată, dezvoltînd și planuri de cooperare bilaterală cu alte state pentru asigurarea securității cibernetice.

În acest sens, a fost organizată Săptămîna Securității Cibernetice 29.10.2019 – 02.10.2019, eveniment realizat în parteneriat cu peste 25 de reprezentanți din sectorul privat din Republica Moldova, România, Ucraina, Marea Britania, Estonia etc. Pentru cunoașterea situației operative în domeniu au fost organizate exerciții practice și work-shop-uri axate pe simulare de atacuri cibernetice, la care participanții au identificat scenarii de gestionare a situațiilor de criză.

STISC raportează organizarea **Workshop-ului "Gestiunea Incidentelor Cibernetice",** în parteneriat cu I.P. „Agenția de Guvernare Electronică" și „Academia de e-Guvernare" din Estonia în perioada 17-18 februarie 2020, pentru specialiștii TI și responsabilii de securitate cibernetică și/sau informațională din cadrul instituțiilor publice și private. Workshop-ul a fost condus de către trei experți din partea Academiei de e-Guvernare din Estonia, și a avut drept scop, analiza tendințelor, amenințărilor și vulnerabilităților prezente în spațiul cibernetic. Sub ghidarea experților, participanții au examinat taxonomii comune pentru descrierea incidentelor și cele mai bune metode de identificare și investigare a acestora, inclusiv tehnici de contracarare și răspuns, practici operaționale, precum și alte aspecte organizatorice și juridice.

Serviciul de Informații și Securitate, în calitate de instituție partener, în mod constant atenționează și acordă asistență inițiativelor parvenite din mediul privat în domeniile securității cibernetice, prevenirii și combaterii crimelor informatice.

Acțiunea 7.4 „Promovarea intereselor naționale de securitate cibernetică în formatele internaționale de cooperare la care participă Republica Moldova"

Termen de realizare: permanent.

Responsabil principal este MEI.

În perioada 12-13.06.2019, MEI a găzduit cel de-al 4-lea Atelier de lucru „EU4Digital: Trust & Security" al Panelului pentru Armonizarea Pieței Digitale din cadrul Parteneriatului Estic. În cadrul evenimentului au participat reprezentații guvernelor din regiune, agențiilor de implementare și sectorului asociativ ale țărilor Parteneriatului Estic, precum și implementatorul proiectului – Compania de consultanță Ernst&Young. Obiectivele acestui instrument regional de cooperare, creat de Comisia Europeană și implementat prin DG Conect, sînt promovarea principalelor domenii ale economiei digitale în regiunea

Parteneriatului Estic și implementarea unor proiecte comune de cooperare, în conformitate cu normele și cele mai bune practici ale UE, pe următoarele direcții: legislația în comunicații electronice, securitatea cibernetică, eComerț, inovație digitală, educație digitală și eSănătate.

Potrivit informației prezentate, SIS realizează această acțiune prin participarea permanentă la executarea obiectivelor stabilite în cadrul: Procesului de Revizuire și Planificare a Parteneriatului (PARP); Planului Individual de Acțiuni al Parteneriatului (IPAP) Republica Moldova – NATO; Comisiei pe Securitate Informațională pe lîngă Consiliul Conducătorilor Organelor de Securitate și Serviciilor Speciale ale țărilor membre CSI; Comisiei pe Securitate Cibernetică pe lîngă Consiliul Conducătorilor Autorităților Naționale de Securitate din țările Europei de Sud-est, membre ale Consiliului de Cooperare Regională (CCR) - (SEENSA); ședințelor Organelor de Securitate și Serviciilor Speciale ale țărilor Europei Centrale (MEC) și de Sud-Est (SEEIC) pe problemele securității cibernetice.

Potrivit informației prezentate de STISC, cooperarea pe plan național, cît și pe plan internațional a fost intensificată în ultima perioadă în vederea asigurării unor răspunsuri adecvate la amenințările provenite din mediul virtual. Colaborarea cu alte organizații internaționale, precum Uniunea Internațională a Telecomunicațiilor (UIT), Departamentul de Stat al Statelor Unite ale Americii și Pacific Northwest National Laboratory (PNNL), Institutului de Inginerie Software (SEI), Universitatea Carnegie Mellon, OSCE (Capacity Building Measures), FIRST, George C. Marshall Center, North Atlantic Treaty Organization (NATO) oferă posibilitatea de a prelua cele mai bune practici, de a organiza în comun conferințe, workshop-uri, exerciții, vizite de lucru. Rezultatele acestor colaborări ulterior pot fi implementate și utilizate cu succes și în Republica Moldova.

Din ce în ce mai mult, a fost pus accent pe intensificarea eforturilor de colaborare cu alte țări, precum și organizații internaționale în domeniul dezvoltării proiectelor în domeniul securității cibernetice, în special pregătirea specialiștilor pentru a răspunde noilor amenințări cibernetice, precum și care ar fi cele mai bune practici tehnici de remediere în caz că instituția a fost atacată, dezvoltînd și planuri de cooperare bilaterală cu alte state pentru asigurarea securității cibernetice. În acest sens, au fost semnate acorduri de colaborare bilaterale și dezvoltarea proiectelor naționale.

Pe parcursul semestrului I 2019 angajații CCCI al MAI au participat și au reprezentat interesele naționale în cadrul următoarelor evenimente:

- în perioada 04-07.03.2019 un angajat al CCCI a participat la Reuniunea Comitetului Părților la Convenția CoE pentru protecția copiilor împotriva exploatării sexuale și a abuzurilor sexuale (Convenția Lanzarote), ședința de lansare a proiectului internațional ,,End OCSEA@Europe”, eveniment desfășurat sub egida CoE, în or. Strasbourg, Republica Franceză;
- la 29.05.2019 și respectiv la 31.05.2019 un angajat al CCCI a participat în calitate de expert la 2 ateliere de lucru, în contextul misiunii de evaluare a experților Consiliului Europei privind efectuarea Studiului de cercetare a problemelor sistemice care afectează răspunsul sistemului de protecție a copilului la exploatarea și abuzul sexual asupra copiilor și implementarea Convenției Lanzarote, în cadrul căreia au fost discutate rezultatele misiunii și etapele de efectuare a cercetării;
- în perioada 03-07.06.2019 un angajat al CCCI a participat la cea de-a 24-a Reuniune a Comitetului Părților la Convenția Consiliului Europei pentru protecția copiilor împotriva exploatării sexuale (Comitetul Lanzarote), or. Strasbourg, Franța;
- în perioada 22-23.01.2019 un angajat al CCCI a participat la ce-a de-a 8-a Reuniune a Grupului de lucru GUAM în domeniul securității cibernetice, în cadrul căreia a fost abordat

subiectul semnării un memorandum de cooperare în domeniul securității cibernetice, precum și organizarea mai multor acțiuni de schimb informațional, eveniment desfășurat în or. Kiev, Ucraina;

- în perioada 08-09.04.2019 un angajat al CCCI a participat la cea de-a 19-a sesiune a Alianței împotriva traficului de persoane cu genericul ,,Utilizarea tehnologiei în combaterea traficului de ființe umane: Transformarea responsabilității în avantaj", în or. Viena, Austria;
- în perioada 09-11.04.2019 un angajat al CCCI a participat la Reuniunea EMMA 5 European Money Mule Action, eveniment organizat de către Oficiul European de Poliție (Europol), în or. Haga, Regatul Țărilor de Jos, în scopul combaterii fraudei online, inclusiv prin cărțile de plată, contribuind la îmbunătățirea unui parteneriat eficient dintre poliție, procuratură și sectorul bancar, atît la nivel național, cît și la nivel internațional;
- în perioada 06-08.05.2019 un angajat al CCCI a participat la ședința operațională "Operation ShredIT" în domeniul proprietății intelectuale privind investigarea noilor tendințe în domeniul PI, în or. Haga, Regatul Țărilor de Jos;
- în perioada 12-25.05.2019 un angajat al CCCI a participat la grupul de lucru aferent exploatării sexuale prin intermediul internetului a minorilor, cu genericul: ,,6th Victim Identification Task Force" (VIDTF), organizat sub egida Punctului Focal Europol Twins (EUROPOL SOC-AP) din Haga, Regatul Țărilor de Jos;
- în perioada 16-17.05.2019 un angajat al CCCI a participat la Conferința regională în scopul consolidării cooperării la nivel național în domeniul contracarării fenomenului de exploatare și abuz sexual asupra copiilor în Internet, în or. Strasbourg, Franța. La eveniment au fost invitați și reprezentanții instituțiilor naționale relevante cum ar fi: MECC, MSM și PS, MEI, PG, INJ, MAEIE, Oficiul Avocatului Poporului, participarea cărora urmărește scopul implicării active în procesul implementării proiectului în cadrul instituției reprezentante;
- în perioada 23-24.05.2019 doi angajați ai CCCI au participat la cel de-al 2-lea seminar privind securitatea cibernetică/ICT. Evenimentul a fost organizat sub egida Organizației pentru Securitate și Cooperare în Europa (OSCE), desfășurat în or. Sarajevo, Bosnia și Herțegovina;
- la 12.06.2019 un angajat al CCCI a participat la conferința cu genericul,, Prevenirea victimizării minorilor – online și offline", organizată în contextul Președinției rotative a Consiliului Uniunii Europene, sub egida Rețelei Europene de Prevenire a Criminalității (EUCPN), organizată de Inspectoratul General al Poliției Române (IGPR) prin institutul de Cercetare și Prevenire a Criminalității (ICPC), în or. București, România;
- în perioada 18-19.06.2019 un angajat al CCCI la ce-a de-a 3-a Ședință Europol în domeniul proprietății intelectuale privind investigarea noilor tendințe în domeniul PI, în or. Malaga, Spania.

De asemenea, pe parcursul semestrului I 2019, angajații CCCI au participat la următoarele operațiuni:

- în perioada 22-23.01.2019, un angajat al CCCI a participat la ședința operațională IOS X kick-off meeting, eveniment desfășurat în contextul continuității Operațiunii cu genericul Operation In Our Sites IOS X, cu privire la comercializarea prin intermediul internetului a bunurilor contrafăcute, la invitația Punctului Focal Europol Copy;
- în perioada 15-16.05.2019, ofițerii de investigații ai CCCI au participat la ședința operațională privind o operațiune internațională desfășurată sub egida Oficiului European de Poliție EUROPOL, la care au participat și organele de drept din Bulgaria, Georgia, Ucraina, Statele Unite ale Americii, dar și din Republica Moldova. Astfel, Oficiul European de Poliție

EUROPOL a investigat activitatea unei grupări de infractori cibernetici, care a activat pe teritoriul mai multor țări, inclusiv în Republica Moldova;

- în semestrul II 2019 angajații CCCI au participat la Operațiunea PANGEA, care reprezintă conlucrarea a 153 țări membre OIPS sub coordonarea INTERPOL, care are drept scop contractarea vînzătorilor online a produselor farmaceutice contrafăcute.

Acțiunea 7.5 „Promovarea cooperării dintre universitățile din Moldova și liderii mondiali în instruirea și certificarea în domeniul securității cibernetice, cum ar fi (ISC) 2, ISACA, SANS"

Termen de realizare: permanent.

Responsabil principal este MECC.

Ministerul Educației, Culturii și Cercetării informează că pe parcursul anului de studiu universitățile realizează întruniri cu companii și parteneri externi, care oferă prelegeri teoretice și susținerea exercițiilor practice în domeniul securității cibernetice. În rezultatul întrunirilor sînt încheiate acorduri de colaborare, datorită cărora are loc schimbul activ de experiență între instituții în domeniul vizat.

Astfel, în perioada 15.10.2016-14.10.2019 este implementat proiectul de dezvoltare a capacității și colaborare instituțională Erasmus+ LMPI „Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam".

În Republica Moldova proiectul este implementat la patru instituții de învățămînt superior: Universitatea de Stat din Moldova, Universitatea Tehnică a Moldovei, Academia de Studii Economice a Moldovei și Universitatea de Stat Alecu Russo din Bălți, avînd ca parteneri Ministerul Educației, Culturii și Cercetării, Centrul pentru Combaterea Crimelor Informatice și STISC. Activitățile preconizate în cadrul proiectului sînt realizate cu participarea a 9 parteneri europeni, printre care: UNINETTUNO (Italia), JEEP FIPAG (Franța), CESIE (Italia), University of West Attica (Grecia).

În semestru II 2019, Universitatea de Stat din Moldova a realizat următoarele activități:

1. Au fost admiși la Programul de master Informatică aplicată, care conține trasul Securitatea informației – 32 de studenți. În program sînt incluse următoarele cursuri: Managementul și Audit al Securității Informației; Securitatea tranzacțiilor electronice și Securitatea informației întreprinderii.
2. A fost organizat ciclul de cursuri în securitatea informației pe următoarele cursuri:
   - Iot Security;
   - BlockchainTechлologies;
   - Cyber Security Terms,
   - Protocols and standards;
   - Informationsecurity;
   - Network Security.
3. Trei cadre didactice de la Facultatea de Matematică și Informatică au absolvit cursul Audit intern pentru sisteme de management al calității SM EN ISO 9001:2015, organizat de Institutul de Standardizare din Moldova;
4. Studenții de la Facultatea de Matematică și Informatică au participat la lecția Securitatea în mediul on-line;
5. A fost organizat ciclul de cursuri în Securitatea Informației:

- Международное-европейское правовое регулирование защиты данных и информационной безопасности;

- Fintech – совершенствование, защита и автоматизация данных при оказании финансовых услуг.

6. A fost organizat ciclul de lecții „Tehnologia blockchain și criptovalută: istorie, bune practici, perspective”.

În semestrul I 2019, Universitatea de Stat din Moldova:

- a organizat seminarul de formare „Aspecte de management și audit al securității informației” ghidat de compania BSD Management SRL, la care au participat 11 cadre didactice ale facultății de Matematică și Informatică;
- a fost procurat standardul ISO Securității Informatice, care vor fi utilizate în procesul de studii;
- a fost semnat Acordul de diplomă dublă în Securitatea Informației, la nivel de master cu Universitatea West Attica, Grecia;
- în perioada 2018-2019, au fost admiși la studii și instruiți aproximativ 70 de studenți la discipline ce țin de Securitatea Informației, dintre care 20 au absolvit programul de studii de licență în anul 2019.

În perioada 2018-2019, în cadrul Universității de Stat din Tiraspol, Facultatea de Fizică, Matematică și Tehnologii Informaționale, au fost realizate cercetări științifice în cadrul a 2 proiecte internaționale axate pe securitatea teritorială, care, la rîndul său, include și securitatea cibernetică:

- NATO SPS G5381 MIDAS – Control of Team of Mini-UAVs to support Counter-Terrorism Missions;
- NATO SPS G5437 WITNESS – Wide Integration of Sensor Networks to Enable Smart Surveillance.

La data de 19.04.2019 profesorii din cadrul Universității de Stat din Tiraspol au participat în cadrul prezentării Polului de Excelență în Securitate Cibernetică, dezvoltat de UTM și echipat cu suportul financiar al UE în cadrul proiectului LMPI (Licence, Master Professionnel en Protection Informatique).

Acțiunea 7.6 „Stabilirea și dezvoltarea relațiilor cu comunitatea internațională de cercetare în domeniile specifice care stau la baza securității cibernetice”

Termen de realizare: 2016-2019.

Responsabil principal este MECC.

Ministerul Educației, Culturii și Cercetării este la etapa de colaborare și stabilire a relațiilor cu partenerii externi, care realizează cercetări în domeniile specifice care stau la baza securității cibernetice. Astfel, pentru semestrul II 2019, I.P. Institutul Național de Cercetări Juridice, Politice și Sociologice (ICJPS) raportează stabilirea relațiilor de comunicare internațională de cercetare în cadrul Programul COST (Cooperarea Europeană în domeniul Științei și Tehnologiei) care contribuie la consolidarea capacităților de cercetare și inovare din Europa, participînd în cadrul următoarelor acțiuni COST:

1. CA l5207 - Professionalization and Social Impact of European Political Science (ProSEPS);
2. CA |62l| - Reappraising Intellectual Debates on Civic Rights and Democracy in Europe;
3. CA 16233 - Drylands facing change:interdisciplinary research on climate change, food
4. insecurity, political instability;
5. CA 17102 - Police Stops;
6. CA 171 14 , Transdisciplinary solutions to cross sectoral disadvantage in youth (YOUNG-IN);
7. CA l823б - Multi-disciplinary innovation for social change.

În perioada noiembrie-decembrie 2018, în cadrul colaborării UTM cu Universitatea Alexandru Ioan Cuza în domeniul Securității informaționale, ambele universități avînd programe la licență și master Securitate informațională, Laboratoare identice Bitdefender etc., expertul în criptanaliză, prof. Ferucio Laurențiu Țiplea, de la Universitatea Alexandru Ioan Cuza, Iași, a ținut un de curs masteranzilor de la Securitate.

La Institutul de Dezvoltare a Societății Informaționale (IDSI) a fost realizată cercetarea "A bibliometric analysis of cybersecurity research papers in Eastern Europe: case study from the RM", care urmează să fie comunicată în 2019 (Central and Eastern European e-Dem and e-Gov Days).

Academia de Științe a Moldovei raportează că Institutul de Dezvoltare a Societății Informaționale (IDSI) a fost coorganizator și a participat la conferința CEE e-Dem and e-Gov Days 2019 - Cyber Security and e-Government, Proceeding of the Central and Eastern European e-Dem and e-Gov Days 2019, 02-03.05.2019, Budapest. Totodată, IDSI, fiind deținător al certificatului de conformitate cu cerințele standardului internațional ISO/IEC 27001:2013 „Sisteme de management al securității informației", colaborează cu Organismul Româno-Italian de certificare RINA SIMTEX acreditat la nivel internațional. În semestrul I al anului 2019, sistemul de management al IDSI a fost reevaluat de organismul susnumit, fiind constatată menținerea și îmbunătățirea sistemului de management al securității informației în cadrul IDSI.

Acțiunea 7.7 „Stabilirea și dezvoltarea relațiilor cu liderii mondiali în domeniul securității cibernetice pentru a crea un Centru de excelență pentru cercetare și dezvoltare în Republica Moldova"

Termen de realizare: 2016-2018.

Responsabil principal este MECC.

Ministerul Educației, Culturii și Cercetării informează, că în prezent are loc stabilirea cadrului normativ în domeniul cercetărilor, după care va fi inițiată realizarea acestei acțiuni.