MINISTERUL TEHNOLOGIEI INFORMAŢIEI ŞI COMUNICAŢIILOR

Raport despre executarea în sem. I 2016 a Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020

Hotărîrea Guvernului nr.811 din 29.10.2015

Chişinău, august 2016

S U M A R

INFORMAŢIE GENERALĂ

Dezvoltarea accelerată a tehnologiilor informaţiei şi de comunicaţii electronice moderne, care au penetrat deja toate sferele vieții sociale, economice și politice, ridică la un alt nivel abordarea ameninţărilor, riscurilor şi vulnerabilităţilor într-o societate informaţională.

În prezent, ameninţările şi riscurile, atacurile şi incidentele cibernetice, precum şi alte evenimente survenite în spaţiul cibernetic, în care nu există frontiere, se produc cu o frecvenţă, complexitate şi o amploare din ce în ce mai mare, aducînd pagube enorme sectorului guvernamental, celui privat şi cetăţenilor. Acestea se materializează în spațiul cibernetic prin exploatarea vulnerabilităţilor de natură umană, tehnică şi 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 a acesteia, la nivel de politici guvernamentale, sunt expuse în premieră în Strategia naţională de dezvoltare a societăţii informaţionale "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 căruia 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 naţional 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 securităţii 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 naţional 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, sunt repartizate în 7 compartimente, conform obiectivelor specifice ale PNSC 2016-2020:

1) procesarea, stocarea şi accesarea în siguranţă a datelor, inclusiv a datelor de interes public;

2) securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice;

3) dezvoltarea capacităţilor de prevenire şi reacţie urgentă la nivel naţional (reţeaua CERT naţională);

4) prevenirea şi combaterea criminalităţii informatice;

5) consolidarea capacităţilor de apărare cibernetică;

6) educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice;

7) cooperarea şi interacţiunea internaţională în sferele ce ţin de securitatea cibernetică.

Totodată, la realizarea acțiunilor din PAI PNSC 2016-2020, va fi necesar de luat în vedere și prevederile ce țin de securitatea cibernetică incluse în proiectele noilor Strategii de securitate națională, de apărare națională și de securitate informațională, care în prezent sunt în proces de finalizare.

Potrivit prevederilor Hotărîrii Guvernului nr.811 din 29.10.2015, în sarcina Ministerului Tehnologiei Informaţiei şi Comunicaţiilor (MTIC) este pusă responsabilitatea de monitorizare şi coordonare a procesului de realizare a PNSC 2016-2020. În contextul exercitării acestei sarcini, MTIC a recepționat de la ministere și alte autorităţi administrative centrale informaţia privind executarea în sem. I 2016 a PNSC 2016-2020, conform responsabilităţilor stabilite pentru aceste instituții în PAI PNSC 2016-2020. Reieşind din faptul, că sem. I 2016 este primul semestru (din cele 10, pentru care se vor face raportări semestriale privind executarea PNSC 2016-2020), prezentul raport include informaţii generalizate referitoare la gradul de iniţiere a acţiunilor prevăzute pentru anul curent.

În majoritatea cazurilor, iniţierea executării acţiunilor din PAI PNSC 2016-2020 a început conform termenelor stabilite în acesta.

Responsabilii principali de executarea acţiunilor din PAI PNSC 2016-2020 sunt identificaţi în conformitate cu prevederile pct.30 din PNSC 2016-2020.

I. OBIECTIVUL SPECIFIC "Procesarea, stocarea şi accesarea în siguranţă a datelor, inclusiv a datelor de interes public"

Implementarea acestui obiectiv specific se va realiza prin executarea a 11 acţiuni din PAI PNSC 2016-2020.

În sem. I 2016, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, urmau a fi iniţiate 9 acţiuni, rezultatele executării cărora se expun după cum urmează mai jos.

Acţiunea 1.1 "Asigurarea ajustării cadrului normativ-legislativ privind securitatea cibernetică a Republicii Moldova care va prevedea: a) definirea termenilor (noţiunilor) din domeniul securităţii cibernetice; b) delimitarea pe domenii a competenţelor; c) stabilirea organului cu funcţii de monitorizare a respectării cerinţelor de securitate cibernetică; d) desemnarea organului responsabil de controlul implementării rezultatelor auditului de securitate cibernetică; e) obligaţiile deţinătorilor sistemelor informaţionale de stat privind efectuarea periodică a auditului acestor sisteme, cu stabilirea periodicităţii, nivelelor, obligaţiilor de prezentare a raportului către organul competent; f) sancţiuni pentru nerespectarea deciziei auditului privind conformitatea cu cerinţele minime obligatorii de securitate cibernetică; g) responsabilitatea personală pentru asigurarea securităţii cibernetice; h) introducerea în autorităţile publice a funcţiei de coordonator de securitate cibernetică, inclusiv atribuţiile principale ale acestuia; i) formarea Consiliului intersectorial de securitate cibernetică (cu funcţie de coordonare a activităţilor de securitate cibernetică)".

Termen de realizare: 2016-2017.

Responsabil principal este Ministerul Tehnologiei Informaţiei şi Comunicaţiilor (MTIC).

În contextul executării acestei acţiuni, MTIC a demarat activitățile de studiere a cadrului legislativ-normativ și instituțional al altor state, precum și celui european referitor la securitatea cibernetică. Totodată, MTIC a obținut asistență externă privind analiza cadrului legislativ-normativ din partea Marei Britaniei și Coreei de Sud. În acest context, experții coreeni au efectuat o vizită de studiu în perioada 22-27 august curent pentru a face cunoștință cu situația reală la acest subiect.

Acţiunea 1.2 "Clasificarea tipurilor de informaţie, cu excepţia secretului de stat".

Termen de realizare: 2016.

Responsabil principal este MTIC.

Această clasificare este elaborată și inclusă în proiectul Hotărîrii Guvernului privind aprobarea "Cerințelor minime pentru asigurarea securității cibernetice a sistemelor și resurselor informaționale, echipamentelor și produselor program".

În sem. I curent, MAI a inițiat proiectul de consultanță privind implementarea sistemului de management al securității informației (etapa 1), precum și definirea modelului operațional al Serviciului Tehnologii Informaţionale (STI) conform principiilor ITSM, care se realizează în cadrul MAI de către echipa mixtă de proiect formată din responsabilii din MAI și experți ai SC "Info-Trust Consulting" SRL. În conformitate cu prevederile și sarcinile Planului de proiect, aprobat de MAI la 18.04.2016, a demarat etapa privind clasificarea informațiilor din cadrul MA, care urmează a fi finalizată în sem. II 2016. Această clasificare se va baza pe Cerințele minime pentru asigurarea securității cibernetice a sistemelor și resurselor informaționale, echipamentelor și produselor program, aprobate de Guvern.

Acţiunea 1.3 și 1.4 "Analiza şi elaborarea propunerilor de aplicare la nivel naţional a standardelor ce ţin de procesarea, stocarea şi accesarea sigură a datelor conform clasificării tipurilor de informaţie, examinate în cadrul comitetelor tehnice de standardizare CT 28 "Tehnologia informaţiei" şi CT 29 "Comunicaţii electronice".

Termen de realizare: 2016-2017.

Responsabil principal este MTIC.

În contextul executării acestei acţiuni, MTIC a elaborat prima serie de propuneri pentru aplicarea la nivel naţional a standardelor ce ţin de procesarea, stocarea şi accesarea sigură a datelor. Aceste propuneri au fost adresate Institutului Naţional de Standardizare (INS) prin scr.nr.01/477 din 07.04.2016 care urmează a fi examinate de INS, conform procedurii stabilite (scrisoarea INS nr.02-12/263 din 26.04.2016) în sem. II 2016. Urmare acestei examinări, propunerile MTIC vor fi luate în vedere, integral sau parțial, în proiectul Programului de Standardizare Națională (PSN) pentru anul 2017 (PSN-17). Propunerile adresate INS mai includ adoptarea unor standarde, rapoarte tehnice și specificații tehnice ETSI și ISO ce țin de categoria "Cyber security". MAI urmează a formula a doua serie de propuneri (suplimentare) de

aplicare a standardelor europene și internaționale după realizarea etapei de implementare a clasificării informației în cadrul MAI, în conformitate cu prevederile proiectului de consultanță privind implementarea sistemului de management al securității informației (etapa 1) și definirea modelului operațional al STI conform principiilor ITSM. Proiectul de consultanță se implementează în cadrul MAI de către echipa mixtă de proiect, formată din responsabilii din MAI și experții SC "Info-Trust Consulting" SRL. Standardele sus numite vor fi luate în vedere la elaborarea unei metodologii pentru evaluarea vulnerabilităţilor sistemelor informaţionale de stat.

Acţiunea 1.5 "Elaborarea cerinţelor minime obligatorii de securitate cibernetică".

Termen de realizare: 2016-2017.

Responsabil principal este MTIC.

În contextul executării acestei acţiuni, MTIC a elaborat proiectul Hotărîrii Guvernului privind aprobarea "Cerințelor minime pentru asigurarea securității cibernetice a sistemelor și resurselor informaționale, echipamentelor și produselor program". Urmare avizării şi consultărilor publice, aceste Cerințe sunt în proces de finalizare în conformitate cu obiecțiile și propunerile formulate în avizele autorităților administrației publice centrale.

Totodată, la nivel departamental, în cadrul MAI, potrivit prevederilor Contractului nr. 84/15 din 21 decembrie 2015 semnat între STI și compania SC ”Info - Trust Consulting” SRL, urmează a fi definite și aprobate standarde minime de securitate (care vor include setul de cerințe minime pentru securitatea informației în cadrul MAI și setul de specificații non-funcționale-standard pentru securitatea informației, aferent aplicațiilor aplicative ale MAI). În conformitate cu aceste standarde minime de securitate, ulterior, în cadrul MAI se va efectua evaluarea fiecărui sistem informațional gestionat de acesta, inclusiv de subdiviziunile subordonate MAI. Evaluarea va stabili corespunderea sau necorespunderea sistemelor cu cerințele standardelor și existența vulnerabilităților.

Acţiunea 1.6 "Certificarea specialiştilor reieşind din standardele şi metodologia identificate şi cerinţele minime obligatorii de securitate cibernetică aprobate".

Termen de realizare: 2016-2018.

Responsabil principal este MTIC.

În scopul pregătirii specialiștilor pentru certificare, în cadrul MAI, conform Contractului nr.84/15 din 21.12.2015, experții SC "Info-Trust Consulting" SRL au derulat la 23.03.2016 o Sesiune de instruire introductivă a angajaților subdiviziunilor MAI privind Proiectul de implementare a Sistemului de management al securității informației (SMSI) și de management al serviciilor TI (ITSM). Angajații din cadrul STI al MAI au participat la diverse ședințe de instruire a specialiștilor IT: conferința organizată de compania "BitDefender" la care au fost prezentate soluții de asigurare a securității informaționale a stațiilor de lucru, mijloace hardware și software de protecție cibernetică a acestor stații de lucru; seminarul desfășurat de MTIC în comun cu experții IT de peste hotarele țării (Moldova-GCCD Cybersecurity Joint Seminar),

Workshop-ul "Securitatea digitală și spionajul mobil" pentru specialiștii IT și de securitate informațională, organizat de CTS în comun cu experții Proiectului de Îmbunătățire a Securității Cibernetice. Această modalitate de instruire este unul din elementele de bază în pregătirea profesională a specialiștilor pentru o eventuală certificare a acestora.

Acţiunea 1.7 "Identificarea şi planificarea în bugetele instituţiilor a mijloacelor financiare necesare pentru efectuarea auditului securităţii cibernetice în baza metodologiei aprobate".

Termen de realizare: 2016.

Responsabil principal este Ministerul Finanţelor (MF).

În contextul executării acestei acţiuni un şir de autorităţi ale administraţiei publice centrale, deţinătoare, potrivit prevederilor legale, de sisteme informaţionale de stat, comunică despre elaborarea propunerilor financiare respective la proiectul bugetului de stat pentru anul 2017, care sunt planificate, conform procedurilor stabilite pentru elaborarea proiectului bugetului de stat, pentru sem. II (august-septembrie) 2016.

Potrivit prevederilor pct.2 din Hotărîrea Guvernului, ministerele şi alte autorităţi administrative centrale urmau să prezinte MTIC în termenele stabilite, informaţia despre executarea PNSC 2016-2020 conform responsabilităţilor stabilite în acesta, însă MF n-a prezentat informaţia respectivă.

Acţiunea 1.8 "Efectuarea unui audit în autorităţile administraţiei publice centrale şi locale, în alte entităţi deţinătoare de sisteme informaţionale de stat, cu scopul identificării vulnerabilităţilor şi corespunderii la cerinţele minime obligatorii de securitate cibernetică".

Termen de realizare: 2017-2020.

Responsabil principal este orice autoritate a administraţiei publice centrale sau locale care potrivit normelor legale, deţine sisteme informaţionale de stat.

Activitățile de inițiere a auditului în aceste autorităţi se vor derula în sem. II 2017.

Acţiunea 1.9 "Elaborarea planului de înlăturare a vulnerabilităţilor conform recomandărilor auditului şi executarea acestuia prin responsabilitate personalizată în cadrul autorităţilor administraţiei publice centrale şi locale, altor entităţi deţinătoare de sisteme informaţionale de stat".

Termen de realizare: 2016-2018.

Responsabil principal este orice autoritate a administraţiei publice centrale sau locale care potrivit normelor legale, deţine sisteme informaţionale de stat.

Activitățile de elaborare a planurilor de înlăturare a vulnerabilităţilor, conform recomandărilor auditului, urmează a fi efectuată după realizarea acțiunilor 1.4 și 1.8 din PAI PNSC 2016-2020.

Acţiunea 1.10 "Elaborarea şi implementarea metodologiei de marcare a informaţiei furnizate prin sistemul care conţine date cu caracter personal cu utilizarea mărcii temporale".

Termen de realizare: 2016-2019.

Responsabil principal este Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (CNPDCP).

CNPDCP, în baza examinării experienței de marcare temporală a informației din cadrul STI al MAI, va iniția activitățile de elaborare și implementare a metodologiei de marcare a informației furnizate prin sistemul care conține date cu caracter personal. STI al MAI în conformitate cu prevederile Contractului nr.04/16 din 11.01.2016, încheiat cu CTS, a achiziționat deja serviciul automatizat de aplicare și verificare a semnăturii electronice avansate calificate ("ServerSignature") cu aplicarea mărcii temporale. MAI informează, că în baza "ServerSignature" este asigurată la nivelul corespunzător "marcarea temporală" a informațiilor furnizate prin sistemele ce conțin date cu caracter personal gestionate de STI.

Acţiunea 1.11 "Elaborarea şi implementarea actelor legislative necesare pentru introducerea măsurilor de securitate şi standardelor obligatorii în companiile din domeniul tehnologiei informaţiei şi comunicaţiilor, cu stabilirea unor cerinţe minime de securitate a sistemelor informaţionale de stat şi a informaţiilor din aceste sisteme".

Termen de realizare: 2017.

Responsabil principal este MTIC.

Activitățile urmează a fi desfășurate în anul 2017.

II. OBIECTIVUL SPECIFIC "Securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice"

Implementarea acestui obiectiv specific se va realiza prin executarea a 5 acţiuni din PAI PNSC 2016-2020.

În sem. I 2016 urmau a fi iniţiate toate acţiunile, rezultatele executării cărora se expun după cum urmează mai jos.

Acţiunea 2.1 "Armonizarea legislaţiei din domeniul comunicaţiilor electronice la directivele-cadru UE din domeniu".

Termen de realizare: 2016.

Responsabil principal este MTIC.

MTIC a elaborat Proiectul de lege pentru modificarea şi completarea Legii comunicaţiilor electronice nr.241-XVI din 15.11.07, elaborat și promovat în vederea executării Acordului de Asociere Republica Moldova – Uniunea Europeană. Proiectul prevede completarea Legii în cauză cu 2 articole noi (art. 20^1 şi art. 20^2), care se referă la securitatea şi integritatea rețelelor și serviciilor. Prin aceste completări, legislația națională va fi armonizată cu prevederile capitolului IIIA "Securitatea și integritatea rețelelor și serviciilor" din Directiva 2002/21/CE, astfel cum a fost modificată prin Directiva 2009/140/CE. Proiectul de lege a fost definitivat în baza avizelor autorităților publice, furnizorilor de rețele și servicii publice de comunicații electronice, care prin scr. MTIC nr. 01/719 din 02.06.2016 a fost expediat Cancelariei de Stat spre examinare. Proiectul de lege va fi coordonat suplimentar cu furnizorii de rețele și servicii publice de comunicații electronice, sub egida Consiliului Economic pe lîngă Prim-ministru al Republicii Moldova. De asemenea, în contextul armonizării actelor legislative și normative la directivele-

cadru UE din domeniu, în sem. I 2016: MTIC a elaborat și a remis spre avizare proiectul hotărîrii Guvernului "Cu privire la aprobarea Regulamentului de organizare și funcționare a structurii și efectivului-limită a Ministerului Tehnologiei Informației și Comunicațiilor"; Centrul de Guvernare Electronică (CGE) a elaborat și remis spre avizare proiectele de modificare a hotărîrilor Guvernului nr.1090 din 31.12.2013 "Privind serviciul electronic guvernamental de autentificare și control al accesului (MPass)" și nr.405 din 02.06.2014 "Privind serviciul electronic guvernamental integrat de semnătură digitală (MSign)", precum și proiectul de hotărîre a Guvernului "Cu privire la Sistemul informațional de gestiune electronică a documentelor și înregistrărilor"; Agenția Relații Funciare și Cadastru a elaborat și a remis spre avizare proiectul Legii "Privind Registrul obiectelor de infrastructură tehnico-edilitară".

Acţiunea 2.2 "Stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii, non-repudierii şi integrităţii reţelelor şi/sau serviciilor de comunicaţii electronice şi 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 efectuat "Analiza preliminară a impactului de reglementare la proiectul de Hotărâre al Consiliului de Administrație privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii şi integrităţii rețelelor și serviciilor publice de comunicaţii electronice şi raportarea incidentelor cu impact semnificativ asupra acestora", inclusiv a elaborat proiectul actului normativ aferent, care fiind supuse consultărilor publice, au fost avizate pozitiv pe data de 29 decembrie 2015 de către Grupul de lucru al Comisiei de Stat pentru reglementarea activității de întreprinzător. În conformitate cu normele transparenței decizionale, în perioada 26 ianuarie - 16 martie 2016 proiectul de hotărîre și Analiza finală a impactului de reglementare, au fost supuse unui exercițiu de consultări și dezbateri publice suplimentare. Urmare acestor consultări și dezbateri, furnizorii au solicitat adoptarea proiectului în cauză, doar după intrarea în vigoare a Legii pentru modificarea şi completarea Legii comunicaţiilor electronice nr.241-XVI din 15.11.2007, care ar permite impunerea pentru furnizori a obligației de a întreprinde măsurile tehnice și organizatorice necesare pentru garantarea securității și integrității rețelelor proprii, precum și notificarea în adresa ANRCETI despre orice încălcare a normelor de securitate sau pierdere a integrităţii, care au avut un impact semnificativ asupra funcţionării reţelelor sau a serviciilor. Totodată, în scopul preluării experienței și celor mai bune practici europene și internaționale privind asigurarea securităţii şi integrităţii reţelelor publice de comunicaţii electronice, MTIC a perfectat o scrisoarea în adresa NATO (nr.01/146 din 05.02.2016) prin care a solicitat asistența pentru organizarea unui seminar/training pentru reprezentanții furnizorilor de rețele și servicii de comunicații electronice, precum și pentru reprezentanții autorităților publice cu competență în domeniul vizat.

Acţiunea 2.3 "Analiza şi transpunerea la nivel naţional a standardelor europene şi internaţionale ce ţin de protecţia şi securitatea reţelelor de

comunicaţii electronice şi înaintarea spre adoptare către Institutul Naţional de Standardizare".

Termen de realizare: 2016-2017.

Responsabil principal este MTIC.

Urmare unei analize preliminare, MTIC a remis în noiembrie 2015 în adresa INS propunerea de a include în proiectul Programului de Standardizare Naţională pentru anul 2016 (PSN-16) a standardului ISO/IEC 27033-4 "Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways". Standardul în cauză este inclus deja în PSN-16, aprobat de directorul INS pe data de 19.02.2016. În sem. I curent, MTIC a efectuat o analiză suplimentară, urmare căreia a elaborat propunerile respective de adoptare și aplicare a unor standarde, rapoarte tehnice (Technical Report), specificații tehnice (Technical Specifications) ETSI ce țin de compartimentele specifice din domeniul TIC, inclusiv celor din categoria "Cyber security". Aceste propuneri au fost adresate Institutului Naţional de Standardizare (INS) prin scr.nr.01/477 din 07.04.2016 și după examinare, acestea vor fi luate în vedere, potrivit scrisorii INS nr.02-12/263 din 26.04.2016, la alcătuirea în septembrie curent a proiectului Programului de Standardizare Națională (PSN) pentru anul 2017.

Acţiunea 2.4 "Efectuarea unui studiu cu privire la modificarea legislaţiei în domeniul comunicaţiilor electronice în vederea eliminării sau diminuării numărului abonaţilor serviciilor de comunicaţii electronice depersonalizaţi".

Termen de realizare: 2016-2017.

Responsabil principal este SIS.

SIS a inițiat studiul respectiv. Urmare studierii problemei privind eliminarea sau diminuarea numărului abonaţilor serviciilor de comunicaţii electronice depersonalizaţi, au fost formulate următoarele concluzii:

- serviciul de comunicaţii electronice este un serviciu furnizat, de regulă, contra plată, care include în general transportul semnalelor prin reţelele de comunicaţii electronice, inclusiv serviciile de telecomunicaţii şi serviciile de transmisie prin reţelele destinate pentru difuzarea programelor audiovizuale;

- serviciul de comunicaţii electronice nu include crearea, adaptarea, stocarea, păstrarea sau ștergerea conţinutului informaţiei (contetului), nu include nici exercitarea controlului editorial asupra acestui conţinut, transmis prin intermediul reţelelor și serviciilor de comunicaţii electronice;

- serviciile societăţii informaţionale (în particular, serviciile de comerţ electronic) nu pot fi incluse în categoria serviciilor de comunicații electronice, deoarece serviciile societății informaționale nu includ transportul semnalelor prin intermediul reţelelor de comunicaţii electronice.

Acţiunea 2.5 "Dezvoltarea în continuare a reţelei de comunicaţii speciale a autorităţilor administraţiei publice pe întreg teritoriul Republicii Moldova".

Termen de realizare: conform Planului aprobat de Guvern.

Responsabil principal este Cancelaria de Stat (CS).

Informația privind Planul de dezvoltare a reţelei de comunicaţii speciale a autorităţilor administraţiei publice pe întreg teritoriul Republicii Moldova, care urma să fie aprobat de Guvern, în adresa MTIC n-a fost prezentată.

Cancelaria de Stat (CS) și Centrul de Telecomunicaţii Speciale (CTS) informează că extinderea rețelei de comunicații speciale (sistemului de telecomunicații) al autorităților publice la nivel național este unul din pilonii principali pentru implementarea cu succes a mai multor proiecte de importanță națională: Strategia națională de edificare a societății informaționale – "Moldova electronică 2020", Programul strategic de modernizare tehnologică a guvernării (e-Transformare), Strategia națională pentru siguranța rutieră etc., care sunt orientate nemijlocit să asigure la nivel național dezvoltarea, integrarea, implementarea și menținerea serviciilor publice electronice, protecția unui flux de date securizat, reingineria serviciilor publice şi a proceselor operaționale, securitatea canalelor moderne de acces la serviciile publice, crearea şi utilizarea platformei tehnologice guvernamentale comune, consolidarea centrelor de date, implementarea cadrului arhitecturii guvernamentale pe scară largă, implementarea cadrului de interoperabilitate, etc.

În sem. I curent, CTS a finalizat proiectul de implementare a cadrului de interoperabilitate și a demarat negocierile cu compania Huawei privind implementarea acestuia.

La nivel departamental, în scopul asigurării securizate a schimbului de date între subdiviziunile teritoriale subordonate MAI, precum și cu alte autorități ale administrației publice pe întreg teritoriul Republicii Moldova, STI al MAI a încheiat la 03.06.2016 cu CTS un Contract, obiectul căruia este prestarea serviciilor de transport date, crearea și mentenanța rețelei globale Wide Area Network (WAN MAI). Această rețea include 94 puncte de contact și de prezență a subdiviziunilor subordonate MAI.

III. OBIECTIVUL SPECIFIC "Dezvoltarea capacităţilor de prevenire şi reacţie urgentă la nivel naţional (reţeaua CERT naţională)"

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

În sem. I 2016, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, urmau a fi iniţiate toate acţiunile, rezultatele executării cărora se expun după cum urmează mai jos.

Acţiunea 3.1 "Crearea Centrului naţional de reacţie la incidentele de securitate cibernetică (CERT)".

Termen de realizare: 2016.

Responsabil principal este CS.

Conform informațiilor CS și CTS, pînă în prezent în Republica Moldova nu a fost creată o structură de tip CERT cu competenţe naţionale. Însă, Centrul de Securitate Cibernetică (CERT-GOV-MD) din cadrul CTS, exercită atribuţii de răspuns la incidentele de securitate la nivel de Guvern pentru sistemele informatice ale autorităţilor şi instituţiilor publice centrale, aflate în administrarea tehnică a CTS.

Totodată, CERT-GOV-MD a preluat o parte din prerogativele unui CERT naţional, respectiv: asigurarea Punctului naţional de Contact pentru incidente de securitate cibernetică, diseminarea alertelor de securitate primite de la partenerii internaţionali către toţi operatorii de reţele şi sisteme informatice, coordonarea campaniilor de conştientizare a utilizatorilor de Internet asupra pericolelor existente în mediul online, etc. Cu toate eforturile depuse, CERT-GOV-MD reuşeşte să acopere doar sectorul public, de nivel central, respectiv celelalte instituţii ale statului care nu sunt în subordinea Guvernului, cum ar fi autorităţile şi instituţiile din cadrul Administraţiei Publice Locale, nu se pot derula activităţii de asigurare a securităţii cibernetice. De aceea, ce simte tot mai mult necesitatea creării unui CERT naţional, instituţie care va dispune de capabilităţile necesare pentru prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice la nivel naţional. CERT-ul naţional va elabora şi disemina politici publice de prevenire şi contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competenţă.

Finanţarea unei astfel de structuri de tip CERT este foarte costisitoare şi la moment poate fi o problemă în alocarea de resurse financiare din bugetul de stat pentru crearea unei asemenea structuri. CTS a propus Consiliului Naţional de Securitate să fie creat la nivel de Guvern un Comitet de coordonare şi gestionare a incidentelor cibernetice, format din reprezentanţi ai instituţiilor implicate în implementarea PNSC 2016-2020. Preşedintele acestui Comitet se propune să fie Prim-Ministrul, care va emite decizii şi implementarea acestora să fie efectuată de către operatorul tehnico-tehnologic al Guvernului CTS, şi anume CERT-GOV-MD

Potrivit informaţiilor prezentate în cadrul executării pct.3.11 "Privind urgentarea măsurilor de a reduce vulnerabilitățile și riscurile informaționale, precum și de finalizare a procesului de constituire a Centrului național de reacție la incidente de securitate cibernetică (CERT)" din Decizia Consiliului Suprem de Securitate nr.01/1-02-02 din 23.03.2015, MF şi CTS au viziuni diferite.

În cadrul Centrului de Telecomunicații Speciale funcționează Centrul pentru Securitate Cibernetică (CERT-GOV-MD), care exercită funcții de prevenire a incidentelor de securitate cibernetică în sistemele informatice la nivel guvernamental.

Reieşind din această situaţie, MF, luînd în consideraţie constrîngerile bugetare severe, consideră oportun crearea CERT-ului sus numit în baza CERT-GOV-MD, care își va exercita competențele la nivel național în limita alocațiilor bugetului de stat aprobate pe anul 2016.

Această propunere a MF, conform argumentării CTS, nu este acceptabilă, deoarece pentru crearea capabilităților operaționale aferente unei entități de tip CERT, care trebuie să asigure funcții specifice managementului securității sistemelor informatice și de comunicații la nivel național, sunt necesare eforturi bugetare semnificative.

Potrivit informaţiei MAI pentru sem. I curent, acesta a planificat constituirea la nivel de MAI a unui CERT instituțional de reacționare la incidente cibernetice ce pot surveni în cadrul infrastructurilor critice gestionate. Însă constituirea acestuia necesită alocații bugetare și resurse din partea partenerilor de dezvoltare. Totodată, MAI comunică că urmare scr. nr. 03/3-04-160 din 17.06.2016 a Aparatului Președintelui

Republicii Moldova privind prezentarea propunerilor de rigoare în vederea consolidării MAI la modelul cel mai potrivit de asigurare a securității cibernetice pentru Republica Moldova, a fost înaintată propunerea de constituire la nivel național a unui CERT de dirijare și coordonare, care la rîndul său să aibă în sarcină cooperarea cu CERT-urile constituite în cadrul fiecărei instituții la nivel de bază, urmărind drept scop asigurarea securității cibernetice a infrastructurilor critice gestionate de către instituții în cazuri de importanță majoră ce ar putea atenta la securitatea cibernetică a Republicii Moldova.

Acţiunea 3.2 "Crearea unui sistem naţional de alerte şi informare în timp real despre incidentele de securitate cibernetică".

Termen de realizare: 2016-2017.

Responsabil principal este CS.

CS și CTS informează că pentru diminuarea riscurilor şi îmbunătăţirea climatului naţional de securitate cibernetică, CTS a propus ca în anul 2016 sau la începutul anului 2017 să fie demarat proiectul privind extinderea sistemului de alertă timpurie şi informare în timp real despre incidente de Securitate cibernetică. Aşa cum Internetul nu are graniţe, incidentele cibernetice devin tot mai complexe, de aceea necesitatea unei abordări coordonate şi în strînsă colaborare cu alte instituţii este tot mai necesară pentru a răspunde acestor ameninţări în creştere. Aşa cum securitatea cibernetică deja constituie o preocupare majoră a tuturor actorilor implicaţi, atît la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării unor politici coerente în domeniu, cît şi la nivelul instituţiilor private interesate de protejarea proprietăţii private. CTS a elaborat Studiul de fezabilitate și urmează să fie identificate resurse financiare pentru implementarea acestuia.

Acţiunea 3.3 "Crearea centrelor de reacţie la incidentele de securitate cibernetică departamentale în autorităţile administraţiei publice centrale şi locale, în alte entităţi deţinătoare de sisteme informaţionale de stat".

Termen de realizare: 2016-2017.

Responsabil principal este orice autoritate a administraţiei publice centrale sau locale, precum şi orice altă entitate, care potrivit normelor legale, deţine sisteme informaţionale de stat.

Potrivit informației MAI, STI al 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 oportunitatea constituirii la nivel de MAI a unui CERT instituțional de reacționare la incidente cibernetice ce pot surveni în cadrul infrastructurilor critice gestionate. Însă constituirea CERT-ului departamental al MAI necesită alocații bugetare și resurse din partea partenerilor de dezvoltare.

SIS comunică că a inițiat procesul de extindere a capacităţilor instituţionale în acest context, precum şi, în limită competenţelor, acordă suportul necesar autorităților administrației publice centrale și locale și altor entități deținătoare de sisteme informaționale de stat de profil în acest context.

CNPDCP informează că persoana responsabilă de politica de securitate a datelor cu caracter personal exercită și atribuții ce țin de activitatea Centrului de reacție la incidentele de securitate cibernetică din cadrul acestei instituţii.

Acţiunea 3.4 "Stabilirea obligaţiilor pentru autorităţile administraţiei publice centrale şi locale şi mediul de afaceri din domeniul tehnologiei informaţiei şi comunicaţiilor privind raportarea operativă obligatorie a incidentelor de securitate cibernetică în baza unui mecanism de schimb de date şi roluri bine definite".

Termen de realizare: 2016-2017.

Responsabil principal este CS.

MAI informează că în prezent această acțiune nu poate fie realizată din motivul lipsei constituirii Centrului de reacție la incidente de securitate la nivel național și a celor din cadrul instituțiilor ce dețin sisteme informatice de stat.

Acţiunea 3.5 "Organizarea unei baze de date cu acces al autorităţilor responsabile privind ameninţările, vulnerabilităţile şi incidentele de securitate cibernetică identificate sau raportate, tehnicile şi tehnologiile folosite pentru atacuri, bunele practici pentru protecţia domeniului tehnologiei informaţiei şi comunicaţiilor".

Termen de realizare: permanent.

Responsabil principal este CS.

Conform informaţiei MAI, în adresa acestuia n-au parvenit propuneri și solicitări de participare la organizarea a unei astfel de baze de date. De asemenea, MAI consideră că constituirea unei astfel de baze va fi oportună după crearea CERT-urilor la nivel național.

SIS comunică că în calitate de instituţie partener, este disponibil în limita competenţelor, să acorde suportul necesar instituțiilor de profil în acest context.

CNPDCP informează că n-a fost implicat de instituțiile responsabile în realizarea acestei acţiuni.

Acţiunea 3.6 "Desfăşurarea exerciţiilor şi antrenamentelor comune de consolidare a capacităţilor de reacţie la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate".

Termen de realizare: permanent.

Responsabil principal este CS.

Potrivit informaţiei CS, CTS a organizat în sem. I curent mai multe exerciţii de securitate cibernetică la care au participat atît funcţionari din sectorul public, cît și reprezentanți din sectorul privat, precum şi mediul academic. Necesitatea pentru un răspuns rapid și eficient în cazul unui incident cibernetic, cunoașterea procedurilor și a fluxurilor de informații este esențială. În contextul acestor necesităţi au fost instruiţi participanţii la aceste exerciţii. Aceste exerciţii sunt un reper important pentru construirea încrederii, pentru o mai bună înțelegere a mecanismelor de cooperare cibernetică existente la nivel de instituţii și pentru consolidarea gestionării la nivel de Guvern a incidentelor cibernetice. De asemenea, CTS în comun cu partenerii internaţionali a organizat training-uri, ateliere de lucru, cursuri pentru formarea profesională în domeniul securităţii cibernetice, destinate conştientizării riscurilor la

care sunt supuse sistemele informatice ale autorităţilor publice precum şi modalităţile de a răspunde acestor noi ameninţări. A fost creată o echipă de experţi din reprezentanţii instituţiilor participante la aceste training-uri, care în cazul unor incidente de securitate cibernetică, poate operativ şi eficient să depăşească situaţiile de criză.

Acţiunea 3.7 "Consolidarea capacităţilor echipei Centrului naţional de reacţie la incidentele de securitate cibernetică pentru a asigura analiza strategică a incidentelor de securitate şi coordonarea acţiunilor de răspuns la incidente de securitate în sectorul public, privat şi academic, inclusiv prin organizarea trainingurilor de către experţi calificaţi".

Termen de realizare: 2016-2018.

Responsabil principal este CS.

CS și CTS informează că urmare analizei datelor deținute de către CERT-GOV-MD, rezultă faptul că amenințările de natură informatică asupra spațiului cibernetic guvernamental s-au diversificat, fiind relevate tendințe evolutive din perspectiva cantitativă şi complexitate tehnică. Această tendință este confirmată și de rapoartele internaționale, precum cel publicat de Trend Micro, în care se menționează că ținta principală a atacurilor cibernetice este Guvernul. Prin urmare, se impune necesitatea fortificării activității Centrului pentru securitatea cibernetică (CERT-GOV-MD) din cadrul CTS, prin elaborarea unui proiect de hotărâre de Guvern, care va stabili anumite reguli în ceea ce privește raportarea și răspunsul în cadrul unor incidente de securitate. Elaborarea proiectului acestei hotărîri de Guvern este în curs de realizare.

De asemenea, CTS în comun cu partenerii internaţionali au organizat o serie de instruiri pentru funcţionarii publici, dar şi cei din cadrul CERT-GOV-MD, scopul acestor instruiri fiind scoaterea în evidență a vulnerabilităților tipice întîlnite în domeniul securității cibernetice, precum și sublinierea importanței deosebite acordate cooperării în astfel de cazuri. În cadrul acestor instruiri, participanţii au acumulat şi cunoştinţe ce ţin de desfășurarea practică a unor investigații digitale, precum și de monitorizare a datelor de trafic. Au fost discutate şi chestiuni ce ţin de necesitatea procedurilor de cooperare între instituţii și de diseminare pentru combaterea infracțiunilor cibernetice. Instruirile sus menţionate au fost desfăşurate în perioadele 18-20 aprilie 2016 şi 23-24 aprilie 2016. În prima perioadă s-a desfăşurat un workshop în domeniul securității cibernetice, coordonat de către experţi cu renume internațional în domeniu. La acest workshop au participat reprezentanţi din 20 de instituţii din Republica Moldova, care a avut drept scop sporirea nivelului securității și durabilității rețelelor TI și de comunicare din Republica Moldova prin construirea și formarea capacităților locale pentru a preveni, a răspunde și a contracara, în mod corespunzător, atacurile cibernetice și/sau defecțiunile accidentale. În cadrul acestui workshop participanţii au studiat procesul de a răspunde la incidente, inclusiv conştientizarea riscurilor şi necesităţii implementării măsurilor de prevenire a acestora. În a doua perioadă sus menţionată, a fost organizat un curs specializat TRANSITS I, care au avut loc în or. Praga (Republica Cehă). Obiectivul general al cursului a fost de a contribui la formarea specialiștilor CSIRT prin consolidarea cunoștințelor în domeniul securității cibernetice. Programul cursului a fost împărţit în

mai multe etape precum: tehnici de bază de contracarare și de reacție la incidentele cibernetice, practici operaționale, precum și aspecte organizatorice și juridice. Cunoştinţele obţinute la acest curs au ajutat la înţelegerea corectă a funcţionării unei instituţii de tip CERT.

Angajații din cadrul STI al MAI, au participat la Atelierul de lucru privind Securitatea Cibernetică, organizat la 12 mai 2016 de către MTIC în parteneriat cu Centrul Global de Securitate Cibernetică pentru Dezvoltare, fiind prezentată situaţia securității cibernetice în Republica Moldova și Coreea de Sud, precum și prezentate cele mai bune practici ale Coreei de Sud referitor la sistemul de management al securității informației, protecția infrastructurilor critice de informație, legislația și politicile naționale de securitate cibernetică

Acţiunea 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.

CS și CTS informează că odată cu creşterea numărului de servicii electronice, sfidările cibernetice cresc şi iau forma unor ameninţări şi atacuri mai sofisticate, constituind o ameninţare majoră la adresa securităţii statului, precum şi a sectorului privat. CTS a inclus ca prioritate în planul de acţiuni a întreprinderii de a avea o cooperare mai strînsă cu sectorul public, privat şi cu instituţiile competente în domeniul securităţii cibernetice. Cooperarea la nivel operaţional în promovarea unui schimb mai eficient de informaţii între autorităţile publice şi sectorul privat privind ameninţările cibernetice este crucială şi are ca scop asigurarea securităţii reţelelor şi a informaţiilor. Pentru a garanta integritatea, disponibilitatea şi confidenţialitatea serviciilor critice, în special, identificarea şi clasificarea infrastructurii critice, trebuie să fie stabilite cerinţele minime de securitate necesare pentru sistemele de informaţii şi reţele. În acest context, CTS dezvoltă parteneriate de tip public-privat pentru a stimula schimbul reciproc de informaţii privind ameninţările, riscurile, precum şi măsurile întreprinse în cazul incidentelor sau atacurilor cibernetice. Au fost semnate memorandumuri şi acorduri de colaborare în scopul schimbului de informaţii precum şi schimb de experienţă în depistarea și contracararea incidentelor de securitate cibernetică.

IV. OBIECTIVUL SPECIFIC "Prevenirea şi combaterea criminalităţii informatice"

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

În sem. I 2016, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, urmau a fi iniţiate toate acţiunile, rezultatele executării cărora se expun după cum urmează mai jos.

Acţiunea 4.1 "Elaborarea proiectului de lege privind modificarea şi completarea legislaţiei penale şi contravenţionale pentru prevenirea şi combaterea crimelor informatice în scopul armonizării continue a acesteia la

prevederile Convenţiei Europene privind criminalitatea informatică şi la deciziile Comitetului acestei Convenţii".

Termen de realizare: 2016.

Responsabil principal este MAI.

MAI informează că pe parcursul perioadei vizate "Proiectul de lege pentru modificarea și completarea unor acte legislative" a fost inclus pe ordinea de zi a Guvernului, ulterior fiind aprobat. În aprilie 2016 au fost organizate un şir de discuţii publice și o conferință de presă asupra acestui proiect. La 20.05.2016, proiectul în cauză a fost examinat în şedinţa comună a Comisiei permanente a Parlamentului, precum şi la şedinţele a 5 comisii parlamentare. De asemenea, acest proiect de Lege a fost examinat şi în ședința comună a reprezentanţilor CCCI a INI al IGP, DGJ a MAI, Companiei "Orange". Urmare acestor dezbateri publice, proiectul de Lege sus numit a fost modificat în corespundere cu propunerile acestei Companii. În iunie 2016, proiectul de Lege sus numit a fost remis spre expertizare în adresa Consiliului Europei.

Modificările şi completările legislative au fost propuse în scopul armonizării cadrului legislativ naţional la prevederile Convenţiei Consiliului Europei privind criminalitatea informatică şi implementării unor prevederi ale acesteia sub aspectul garantării cercetării și urmăririi penale eficiente a infracțiunilor prevăzute de Convenția sus numită. Astfel, în premieră pentru Republica Moldova sunt propuse procedurile privind percheziţia informatică, conservarea rapidă a datelor informatice şi interceptarea datelor informatice.

Totodată, au fost propuse prevederi de completare a "Legii privind prevenirea şi combaterea criminalităţii informatice", în scopul reglementării procedurii de elaborare, coordonare şi aprobare a Planului naţional de prevenire şi combatere a criminalităţii informatice, precum şi a procedurii de instituire a unui Comitet al securităţii informatice, inclusiv norme de reglementare generală a activităţii acestuia.

De asemenea, în contextul realizării acestei acţiuni, MAI a remis spre examinare Guvernului proiecte de legi privind modificarea și completarea Codului penal, Codului de procedură penală, Codului contravențional și altor acte legislative, adoptarea cărora va armoniza legislația penală şi contravenţională cu prevederile Convenției Europene privind criminalitatea informatică și deciziilor Comitetului acestei Convenții.

Acţiunea 4.2 "Instruirea angajaţilor organelor de drept, specialiştilor certificaţi în domeniul securităţii cibernetice privind: a) depistarea, investigarea, urmărirea penală şi judecarea infracţiunilor informatice; b) legătura dintre criminalitatea informatică, crima organizată, infracţiunile economice şi alte categorii de infracţiuni".

Termen de realizare: 2016-2020.

Responsabil principal este Institutul Naţional de Justiţie (INJ).

Procuratura Generală (PG) asigură instruirea continuă a angajaților săi și a instanțelor judecătorești în domeniul securității cibernetice privind depistarea, investigarea, urmărirea penală și judecarea infracțiunilor informatice, precum și legătura dintre criminalitatea informatică, crima organizată, infracțiunile economice și alte categorii de infracțiuni. Instruirea este efectuată cu sprijinul INJ.

Totodată, PG comunică suplimentar că INJ:

În 2013 a organizat 9 seminare, în cadrul cărora au fost instruite 104 persoane, inclusiv: 41 judecători, 61 procurori, 2 alte categorii, inclusiv:

a) 4 seminare la subiectul "Calificarea infracțiunii, particularitățile urmării penale și judecării cauzelor privind infracțiunile informatice" (11.02.2013, 13.03.2013, 11.04.2013, 27.11.2013, în cadrul cărora au fost instruite 63 de persoane, inclusiv: 25 judecători, 36 procurori, 2 alte categorii;

b) 2 seminare la subiectul "Legătura dintre criminalitatea cibernetică, crima organizată, infracțiunile economice și alte categorii de infracțiuni" (23.09.2013, 14.11.2013), în cadrul cărora au fost instruite 17 persoane, inclusiv: 2 judecători, 15 procurori;

c) un seminar la subiectul "Analiza crimelor cibernetice, analiza mijloacelor de reacționare împotriva crimelor cibernetice, protejarea proprietății intelectuale, a dreptului de autor și a drepturilor conexe, măsuri organizatorice în domeniul securității informaționale, analiza riscului la administrarea resurselor informaționale" (02.10.2013), în cadrul cărora au fost instruite 7 persoane, inclusiv: 4 judecători, 3 procurori;

d) 2 seminare la subiectul "Depistarea, investigarea, urmărirea penală și judecarea infracțiunilor cibernetice" (10.12.2013, 16.12.2013), în cadrul cărora au fost instruite 17 persoane, inclusiv: 10 judecători, 7 procurori.

În 2014 a organizat 4 seminare, fiind instruite 64 persoane, inclusiv 26 judecători, 34 procurori, 4 de alte categorii, inclusiv:

a) 2 seminare la subiectul "Depistarea, investigarea, urmărirea penală și judecarea infracțiunilor cibernetice. Legătura dintre criminalitatea cibernetică, crima organizată, infracțiunile economice și alte categorii de infracțiuni" (09.04.2014, 25.11.2014), în cadrul cărora au fost instruite 28 persoane, inclusiv: 11 judecători, 17 procurori;

b) 2 seminare la subiectul "Securitatea informațională și implementarea cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora" (13.02.2014, 11.11.2014), în cadrul cărora au fost instruite 36 persoane, inclusiv: 15 judecători, 17 procurori, 4 de alte categorii.

În perioada de raportare, INJ a organizat și desfășurat 3 seminare de instruire:

a) aspecte practice privind protecția datelor cu caracter personal în activitatea judecătorească. Depersonalizarea hotărîrilor și sentințelor judecătorești (31.03.2016; persoane instruite – 39, din ele: șefi secretariate – 3, asistenți judiciari – 22, grefieri – 13, altele – 1).

b) asigurarea drepturilor omului și a libertăților fundamentale în mediul off-line și on-line (în colaborare cu CoE la 22-23.02.2016; persoane instruite – 43, din ele: judecători – 12, procurori – 13, audienți INJ – 18).

c) tehnologii informaționale, colectarea probelor electronice. Utilizarea softului i2, Analyst, iBase și Encase. Posibilități de cercetare a surselor credibile din țara de origine (în colaborare cu IPD la 25.05.2016; persoane instruite – 20, din ele: judecători – 11, procurori – 9).

Total sem. I: 3 seminare. Participanți – 102, din ei: judecători – 22, procurori – 22, audienți INJ – 18, șefi secretariate – 3, asistenți judiciari – 22, grefieri – 13, altele – 2).

Acţiunea 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.

MAI a iniţiat elaborarea Curriculumului privind investigarea infracțiunilor informatice.

Acţiunea 4.4 "Elaborarea şi aprobarea proiectului de lege privind ratificarea protocolului adiţional la Convenţia Consiliului Europei privind criminalitatea informatică".

Termen de realizare: 2016.

Responsabil principal este MAI.

Potrivit informației MAI, pe parcursul tr. II 2016, angajații subdiviziunii specializate a INI al IGP (CCCI) au efectuat expertiza anti-corupție a "Proiectului de lege privind ratificarea Protocolului Adiţional la Convenţia Consiliului Europei privind criminalitatea informatică privind incriminarea actelor de natură rasistă şi xenofobă săvîrşite prin intermediul sistemelor informatice". Totodată, urmare propunerilor CNA, proiectul în cauză a fost definitivat şi urmează a fi prezentat Guvernului spre examinare. Concomitent, MAI a remis spre examinare Guvernului proiecte de lege privind modificarea și completarea Codului penal, Codului de procedură penală, Codului contravențional și altor acte legislative, urmare incriminării actelor de natură rasistă şi xenofobă săvîrşite prin intermediul sistemelor informatice.

Acţiunea 4.5 "Ajustarea legislaţiei naţionale la prevederile Convenţiei Consiliului Europei pentru protecţia copiilor împotriva exploatării şi abuzurilor sexuale şi a Protocolului adiţional la Convenţie (Lanzarote, 25 octombrie 2007)".

Termen de realizare: 2016-2017.

Responsabil principal este MAI.

MAI a elaborat proiectul de Lege pentru modificarea și completarea unor acte legislative în scopul ajustării acestora la cadrul juridic internaţional şi înlăturării deficienţelor constatate în procesul de aplicare practică a prevederilor legale în domeniul protecţiei copiilor împotriva exploatării şi abuzurilor sexuale. Urmare adoptării acestor modificări şi completări se vor implementa prevederile ce ţin de contracararea pornografiei din Convenţia Consiliului Europei privind criminalitatea informatică şi un şir de prevederi ale Convenției Consiliului Europei pentru protecția copiilor împotriva exploatării sexuale și abuzurilor sexuale (Lanzarote, 2007), sub aspectul garantării cercetării și urmăririi eficiente a infracțiunilor prevăzute de aceste Convenții. Totodată, prin adoptarea proiectului de Lege sus numit se vor implementa şi recomandările Directivei 2011/92/UE a Parlamentului European și a Consiliului Europei din 13.12.2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile.

Acţiunea 4.6 "Efectuarea unui studiu pentru perfecţionarea cadrului normativ în domeniul prevenirii şi combaterii crimelor informatice".

Termen de realizare: 2016.

Responsabil principal este Procuratura Generală (PG).

PG a efectuat un studiu privind rezultatele obținute de instituțiile competente în cursul primelor 6 luni ale anului 2016 în contracararea criminalității cibernetice. Conform rezultatelor acestui studiu, în această perioadă au fost pornite 60 cauze penale privind infracțiunile cibernetice, inclusiv:

a) 14 – privind încălcarea inviolabilității vieții personale;

b) 6 – violarea secretului corespondenței;

c) 7 – încălcarea drepturilor de autor şi drepturilor conexe;

d) 14 – pornografie infantilă;

e) 2 – cartele false de plată;

f) 2 – accesul ilegal la informația computerizată;

g) 2 – producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau produselor program;

h) 1 – interceptarea ilegală a unei transmisii de date informatice;

i) 1 – alterarea integrității datelor informatice ținute într-un sistem informatic;

j) 3 – perturbarea funcționării sistemului informatic;

k) 1 – fals informatic;

l) 6 – fraudă informatică;

m) 1 – accesul neautorizat la rețelele și serviciile de telecomunicații.

În aceiași perioadă procurorii au expediat în judecată pentru examinarea în fond 8 cauze penale privind infracțiunile cibernetice.

Instanțele de judecată au pronunțat 4 sentințe de condamnare în privința a 4 persoane învinuite.

Acţiunea 4.7 "Consolidarea în cadrul Procuraturii Generale, Serviciului de Informaţii şi Securitate şi Inspectoratului General al Poliţiei al Ministerului Afacerilor Interne a capacităţilor pentru prevenirea şi combaterea criminalităţii informatice şi, după caz, formularea unor propuneri de modificare a cadrului normativ şi crearea unui laborator de testare şi expertiză".

Termen de realizare: 2016-2019.

Responsabil principal este MAI.

Conform informaţiei prezentate de MAI, a fost elaborată și aprobată la data de 12.03.2016 prin Ordin Interdepartamental nr. 75/01/342/10/19/9 (MAI, SIS, PG, MTIC şi CTS) "Concepția integrată de analiză a riscului în domeniul combaterii criminalităţii informatice". Obiectivul acestei Concepţii este prevenirea ameninţărilor din domeniul tehnologiilor informaţionale şi asigurarea securităţii informaţionale. La elaborarea Concepţiei sus numite au fost luate în vedere un şir de recomandări expuse în mai multe studii privind analiza riscurilor în domeniul combaterii criminalităţii informatice. Concepţia stabileşte obiectivele, principiile şi direcţiile de acţiune într-o manieră coerentă şi unitară în vederea cunoaşterii, prevenirii şi contracarării riscurilor şi ameninţărilor la adresa securităţii informatice a Republicii Moldova.

Urmare Hotărîrii Parlamentului nr.77 din 04.05.2010 privind aprobarea structurii Procuraturii Generale, în cadrul acesteia a fost creată Secția tehnologii informaționale și investigații ale infrastructurilor în domeniul informaticii. De la 01.08.2016, potrivit

ordinului Procurorului General-interimar nr.587-p din 31.05.2016, în cadrul Direcției urmărire penală și criminalistică a Procuraturii Generale este creată Secția tehnologii informaționale și combaterea crimelor cibernetice. În Codul de procedură penală, prin Legea nr.152 din 01.07.2016, a fost inclus un articol nou (art.270^2) care stabilește competența Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale (PCCOCS) care conduce urmărirea penală în cauzele efectuate de către organele de urmărire penală cu competență pe întreg teritoriul Republicii Moldova (menționate la art.266 și 268 din Codul de procedură penală), inclusiv Centrul pentru Combaterea Crimelor Informatice (CCCI) al Inspectoratului Național de Investigații (INI) al Inspectoratului General al Poliției (IGP). Procuratura specializată PCCOCS va exercita urmărirea penală pentru mai multe categorii de infracțiuni, inclusiv infracțiunile informatice și cele din domeniul telecomunicațiilor, prevăzute de art.259-261^1 din Codul penal.

În contextul realizării acestei acţiuni, SIS a iniţiat procesul de extindere a capacităţilor sale instituţionale.

V. OBIECTIVUL SPECIFIC "Consolidarea capacităţilor de apărare cibernetică"

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

În sem. I 2016, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, urmau a fi iniţiate toate acţiunile, rezultatele executării cărora se expun după cum urmează mai jos.

Acţiunea 5.1 "Elaborarea compartimentului de apărare cibernetică a Republicii Moldova, ca parte componentă a Strategiei securităţii informaţionale a Republicii Moldova".

Termen de realizare: 2016.

Responsabil principal este SIS.

SIS a iniţiat procesul de elaborare a compartimentului de apărare informaţională (inclusiv şi cibernetică) a Republicii Moldova, care va fi parte componentă a Strategiei securităţii informaţionale.

Acţiunea 5.2 "Stabilirea autorităţilor responsabile şi cooperarea reciprocă pe timp de pace, în situaţii de criză, asediu şi război în cadrul spaţiului cibernetic".

Termen de realizare: 2016-2017.

Responsabil principal este SIS.

SIS a iniţiat procesul de executare a acestei acţiuni.

MAI informează, că în baza solicitării nr.03/3-04-160 din 17.06.2016 a Aparatului Președintelui Republicii Moldova cu privire la prezentarea propunerilor de rigoare în vederea consolidării Ministerului Afacerilor Interne la modelul cel mai potrivit de asigurare a securității cibernetice pentru Republica Moldova, a înaintat propunerea ca la nivel național să fie constituit un CERT de dirijare și coordonare, care la rîndul său să aibă în sarcină cooperarea cu CERT-urile constituite în cadrul fiecărei instituții la nivel de bază, urmărind drept scop asigurarea securității

cibernetice a infrastructurilor critice gestionate de către instituții în cazuri de importanță majoră ce ar putea atenta la securitatea cibernetică a Republicii Moldova.

Acţiunea 5.3 "Valorificarea oportunităţilor spaţiului cibernetic pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic".

Termen de realizare: 2016-2018.

Responsabil principal este SIS.

SIS a iniţiat procesul de executare a acestei acţiuni.

Acţiunea 5.4 "Dezvoltarea capabilităţilor militare de protecţie a infrastructurii şi serviciilor critice destinate apărării naţionale".

Termen de realizare: 2016-2017.

Responsabil principal este Ministerul Apărării (MA).

MA a identificat un set de subacțiuni în Strategia Națională de Apărare care este în proces de elaborare. De asemenea, în cadrul structurilor Armatei Naționale sunt desfășurate 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.

Acţiunea 5.5 "Stabilirea programelor de conştientizare şi educare a personalului destinat securităţii şi apărării naţionale în domeniul securităţii cibernetice".

Termen de realizare: 2016-2017.

Responsabil principal este SIS.

SIS a iniţiat elaborarea propunerilor respective, fiind discutate în cadrul mai multor şedinţe interdepartamentale.

Angajații din cadrul STI al MAI, pe parcursul sem. I al anului 2016, au participat la diverse ședințe de instruire a specialiștilor IT, desfășurate de către companii prestatoare de servicii de asigurare a securității informaționale şi de instituţiile 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 MTIC 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 CTS cu suportul Proiectului de Îmbunătățire a Securității Cibernetice.

Acţiunea 5.6 "Stabilirea relaţiilor de cooperare cu instituţiile naţionale şi cele internaţionale din domeniu".

Termen de realizare: 2016-2018.

Responsabil principal este SIS.

SIS a iniţiat executarea acestei acţiuni şi asigură permanent schimbul de informaţii privind ameninţările şi incidentele de securitate informaţională 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 şi EUROJUST.

VI. OBIECTIVUL SPECIFIC "Educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice"

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

În sem. I 2016, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, urmau a fi iniţiate toate acţiunile, rezultatele executării cărora se expun după cum urmează mai jos.

Acţiunea 6.1 "Elaborarea conceptului campaniilor de informare şi conştientizare despre riscurile spaţiului cibernetic".

Termen de realizare: 2016-2017.

Responsabil principal este CS.

PG informează continuu societatea despre riscurile spațiului cibernetic, cauzele penale de rezonanță social sporită în domeniu, în vederea prevenirii criminalității informatice, precum și datele statistice cu privire la contracararea acestor categorii de infracțiuni.

Acţiunea 6.2 "Completarea curriculumului de învăţământ în domeniul securităţii cibernetice".

Termen de realizare: 2016-2018.

Responsabil principal este Ministerul Educaţiei (MEd).

MEd informează că Grupul de lucru responsabil este în proces de definitivare a noului concept al cadrului de referință a curriculumului, după care în anul 2017 va avea loc revizuirea curriculumului pentru stabilirea și includerea cerințelor minime în domeniul securității cibernetice.

Acţiunea 6.3 "Crearea unui portal cu anunţarea operativă a pericolelor din spaţiul cibernetic (digital)".

Termen de realizare: 2016-2018.

Responsabil principal este CS.

CS informează că CTS a iniţiat un Studiu de fezabilitate pentru elaborarea şi implementarea acestui portal. Este elaborat conceptul Proiectului.

Acţiunea 6.4 "Stabilirea cerinţelor de competenţă în domeniul securităţii cibernetice pentru personalul din sectorul public şi privat, precum şi organizarea procesului de instruire, evaluare şi certificare a specialiştilor pentru acest domeniu".

Termen de realizare: 2016-2018.

Responsabil principal este MTIC.

MTIC a iniţiat executarea acţiunii în cauză. Unele cerinţe de competenţă generală a personalului în cauză au fost deja incluse în proiectele elaborate în cadrul acţiunilor prevăzute la pct. 1.5 şi pct. 2.2 din PAI PNSC 2016-2020.

În contextul realizării acestei acțiuni MAI comunică, că angajații din cadrul STI al MAI, pe parcursul sem. I al anului 2016, au participat la diverse ședințe de instruire a specialiștilor IT, desfășurate de către companii prestatoare de servicii de

asigurare a securității informaționale şi de instituţiile publice: Conferința informativă, desfășurată de către compania "BitDefender", în cadrul căreia au fost prezentate soluții de asigurare a securităţii informaționale a stațiilor de muncă, de asigurare a necesităților cu hardware și software de protecție; seminarul organizat de MTIC 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 CTS cu suportul Proiectului de Îmbunătățire a Securității Cibernetice.

Acţiunea 6.5 "Organizarea şi efectuarea trainingurilor şi workshopurilor în domeniul securităţii cibernetice pentru personalul din sectorul public şi privat, deţinătorii de elemente de infrastructură critică".

Termen de realizare: permanent.

Responsabil principal este MTIC.

Serviciul de Informaţii şi Securitate (SIS) este în proces de finalizare a elaborării proiectului de Lege privind infrastructura critică şi a actualizat proiectul Concepţiei securităţii informaţionale a Republicii Moldova. Proiectul Concepţiei este remis Guvernului spre examinare.

Potrivit informaţiei MAI:

În perioada 15-16 februarie curent, 2 angajați ai CCCI au participat la un Workshop din domeniul Securității Cibernetice, organizat de CTS în comun cu CERT-ul din Praga (Cehia). Acest Workshop s-a desfășurat în mun. Chișinău în cadrul Proiectului de Îmbunătățire a Securității Cibernetice, finanţat din fondul Comisiei Europene "Enhancing Cyber Security".

La 23 martie curent, un angajat al CCCI a participat la sesiunea de instruire cu genericul "Bunele practici în gestionarea fondurilor externe nerambursabile", organizat în contextul lansării unui nou proiect comun între MAI al Republicii Moldova și MAI al României "Transfer de know-how România –Republica Moldova în domeniul securității cibernetice, a protecției infrastructurilor critice, a gestionării situațiilor de criză și a luptei împotriva criminalității grave, inclusiv a terorismului".

În perioada 18-19 aprilie curent, doi angajați ai CCCI au participat la alt Workshop din domeniul Securității cibernetice, organizat de către CTS în comun cu proiectul de îmbunătățire a securității cibernetice finanţat din fondul Comisiei Europene "Enhancing cyber security". Acest Workshop s-a desfăşurat în mun. Chişinău în 2 sesiuni: "Infrastructuri critice şi securitatea sistemelor industriale. Crime informatice, spionaj şi război cibernetic" şi "Securitatea digitală şi spionajul mobil".

La 12 mai curent, un reprezentant al CCCI a participat la atelierul de lucru privind Securitatea cibernetică, organizat de către MTIC în parteneriat cu Centrul Global de Securitate Cibernetică pentru Dezvoltare.

CS informează că CTS a organizat mai multe workshopuri, atît în Republica Moldova, cît şi peste hotarele acesteia, la care au participat reprezentanţi ai sectorul public şi privat, inclusiv din domeniul infrastructurii critice. De asemenea şi în cadrul proiectului ENCYSEC (Enhancing Cyber Security/Îmbunătățirea Securității Cibernetice), fiind un Instrument al Uniunii Europene pentru Stabilitate şi Pace din

cadrul Comisiei Uniunii Europene, au fost organizate mai multe workshopuri pentru funcționarii publici și reprezentanții mediului privat.

Potrivit informației CS, Academia de Administrare Publică a inclus module cu elemente de Securitate Cibernetică sau totalmente dedicate Securității Cibernetice în cadrul a 3 cursuri, dintre care două sunt cursurile privind Agenda de e-Transformare a Guvernării:

- pentru funcționarii publici începători (Cursul "Introducerea în Funcția Publică" include modulul e-Transformare - 3 zile);
- pentru funcționarii publici cu experiența (cursuri de consolidare a capacităților, care includ modulul de 1 zi privind Agenda de e-Transformare a Guvernării);
- masteratul în TI include modulul de Securitate Cibernetică.

Conform datelor de care dispune CS, pînă la 30.06.2016, în cadrul cursurilor respective, organizate la AAP, au fost instruiți peste 1300 funcționarii publici.

SIS, în calitate de instituţie-partener, permanent acordă o asistență sporită evenimentelor în cauză, participînd activ la aceste evenimentele.

Acţiunea 6.6 "Crearea unui laborator de securitate cibernetică".

Termen de realizare: 2016-2018.

Responsabil principal este CTS.

Potrivit informației CS, în scopul realizării acestei acţiuni, CTS colaborează cu organizaţia internaţională NATO în vederea dezvoltării domeniului securității cibernetice, consolidării capacităților de reacție rapidă la noile provocări cibernetice, combaterii noilor amenințări la adresa securității informaționale. CTS şi NATO implementează în comun un proiect de creare a unui Laborator de securitate cibernetica, care va fi amplasat în sediul Universității Tehnice din Moldova. În acest Laborator se vor desfăşura exerciții de securitate cibernetică, training-uri, experimente, activități de cercetare. În aceste activităţi vor fi implicaţi funcţionari publici, reprezentanţi ai mediului privat şi academic, precum şi studenţi care ulterior vor fi atraşi în cîmpul muncii în cadrul instituţiilor academice, publice şi private. Laboratorul va fi lansat oficial în luna octombrie curent.

VII. OBIECTIVUL SPECIFIC "Cooperarea şi interacţiunea internaţională în sferele ce ţin de securitatea cibernetică"

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

În sem. I 2016, în conformitate cu termenele stabilite pentru implementarea acestui obiectiv, urmau a fi iniţiate toate acţiunile, rezultatele executării cărora se expun după cum urmează mai jos.

Acţiunea 7.1 "Încheierea acordurilor de cooperare cu alte echipe naţionale de răspuns la incidentele legate de securitatea cibernetică (CERT), precum şi US–CERT, europene şi nord-atlantice (NATO NCERT)".

Termen de realizare: 2016-2018.

Responsabil principal este CS.

CS și CTS informează, că CERT-GOV-MD, în calitate de CERT guvernamental de contact și de reacţie la incidente de securitate cibernetică, a semnat acorduri de

colaborare cu parteneri interni și externi în scopul schimbului de informaţii despre incidentele de securitate cibernetică. În prezent, CERT-GOV-MD are semnate acorduri de cooperare cu CERT-RO, CERT-GOV-GE, Biroul de Securitate Cibernetică din Geoorgia, Kaspersky, Bitdefender, Team Cymru, Shadowserver, CERT din Macedonia, CERT Kosova.

CERT-GOV-MD este membru a comunităţii Europene de echipe CSIRT, supranumită din ianuarie 2014 "Trusted Introducer". Acesta deja a inițiat procedura de a fi membru cu drepturi depline al asociației centrelor de tip CERT la nivel mondial FIRST (Forum of Incident Response and Security Teams/Forumul echipelor de răspuns la incidente de securitate cibernetică). Statutul de membru al asociaţiei FIRST va oferi posibilitatea de a fi recunoscute competențele echipei CERT-GOV-MD la nivel internațional. Prin acreditare, CERT-GOV-MD va avea acces autorizat la baza globală de resurse informaționale ce ţin de domeniul securității cibernetice. Acreditarea va permite colaborarea directă a CERT-GOV-MD cu alte echipe similare din lume în cazul unui atac cibernetic, punîndu-se la dispoziție surse credibile de informații și măsuri tehnologice care să reducă impactul dăunător al acestuia asupra sistemelor și utilizatorilor.

MAI constată, că încheierea acorduri de cooperare cu alte echipe naționale și internaționale, va putea fi realizată după constituirea CERT-urilor la nivel național. Astfel, din cauza lipsei acestora, acțiunea în cauză nu poate fi realizată.

Acţiunea 7.2 "Elaborarea unei platforme de coordonare şi consultare în ceea ce priveşte evaluarea ameninţărilor cibernetice şi identificarea soluţiilor".

Termen de realizare: 2016-2018.

Responsabil principal este CS.

Informaţia privind realizarea acestei acţiuni n-a fost prezentată.

Acţiunea 7.3 "Dezvoltarea cooperării cu sectorul privat (identificarea unor aplicaţii necesare implementării măsurilor de securitate; înfiinţarea de puncte de contact în vederea asigurării solicitării unor date şi informaţii conform prevederilor legale şi stabilirea unui sistem modern de transmitere a solicitărilor; realizarea de întruniri periodice în cadrul unor forumuri de dezbateri pentru cunoaşterea mai bună a situaţiei operative şi pentru înţelegerea nevoilor fiecărei instituţii)".

Termen de realizare: 2016-2019.

Responsabil principal este CS.

Informaţia privind realizarea acestei acţiuni n-a fost prezentată.

Acţiunea 7.4 "Promovarea intereselor naţionale de securitate cibernetică în formatele internaţionale de cooperare la care participă Republica Moldova".

Termen de realizare: permanent.

Responsabil principal este MTIC.

Potrivit informaţiei prezentate, SIS realizează această acţiune prin participarea permanentă la executarea obiectivelor stabilite în cadrul: Procesului de Revizuire şi Planificare a Parteneriatului (PARP); Planului Individual de Acţiuni al Parteneriatului (IPAP) Republica Moldova – NATO; Comisiei pe Securitate Informaţională pe lîngă Consiliul Conducătorilor Organelor de Securitate şi Serviciilor Speciale ale ţărilor

membre CSI; Comisiei pe Securitate Cibernetică pe lîngă Consiliul Conducătorilor Autorităţilor Naţionale de Securitate din ţările Europei de Sud-est, membre ale Consiliului de Cooperare Regională (CCR) - (SEENSA); şedinţelor Organelor de Securitate şi Serviciilor Speciale ale ţărilor Europei centrale (MEC) şi de Sud-est (SEEIC) pe problemele securităţii cibernetice.

În contextul realizării prezentei acţiuni, conducerea MAI a participat în perioada 14-15 martie curent la Reuniunea Consiliului de Asociere RM-UE desfăşurată în or. Bruxelles (Belgia), iar la 9 iunie curent, reprezentanţii MAI au participat la reuniunea subcomitetului de asociere REM-UE "Justiție, Libertate și Securitate" desfăşurată în or. Bruxelles (Belgia).

CS și CTS informează, că echipa CERT-GOV-MD reprezintă un punct de contact cu structurile de tip CERT care funcţionează în cadrul instituţiilor sau autorităţilor publice şi altor organizaţii naţionale şi internaţionale. Experţi din cadrul CERT-GOV-MD au participat cu prezentări la mai multe evenimente naţionale şi internaţionale şi au publicat articole despre activitatea instituţiei, despre trendurile şi situaţia de ansamblu în domeniul securității cibernetice în Republica Moldova la nivel de Guvern. În cadrul acestor evenimente au fost identificaţi potenţialii partenerii care ar putea finanța proiecte de dezvoltare a capacității cibernetice în RM, iar experţilor CERT-GOV-MD le au fost înmînate certificatele respective de participare.

Acţiunea 7.5 "Promovarea cooperării dintre universităţile din Moldova şi liderii mondiali în instruirea şi certificarea în domeniul securităţii cibernetice, cum ar fi (ISC) 2, ISACA, SANS".

Termen de realizare: permanent.

Responsabil principal este MEd.

MEd a inițiat procesul de cooperare și stabilire a unui parteneriat cu autoritățile responsabile vizate în Planul de acțiuni. Pe parcursul anului de studiu universitățile realizează întruniri cu companii și parteneri externi, care oferă prelegeri teoretice şi susținerea exercițiilor practice în domeniul securității cibernetice. În rezultatul întrunirilor sunt încheiate acorduri de colaborare, datorită cărora are loc schimbul activ de experiență între instituțiile domeniului vizat.

Acţiunea 7.6 "Stabilirea şi dezvoltarea relaţiilor cu comunitatea internaţională de cercetare în domeniile specifice care stau la baza securităţii cibernetice".

Termen de realizare: 2016-2019.

Responsabil principal este MEd.

MEd este la etapa de colaborare și stabilire a relațiilor cu partenerii externi care realizează cercetări în domeniile specifice care stau la baza securității cibernetice.

Acţiunea 7.7 "Stabilirea şi dezvoltarea relaţiilor cu liderii mondiali în domeniul securităţii cibernetice pentru a crea un Centru de excelenţă pentru cercetare şi dezvoltare în Republica Moldova".

Termen de realizare: 2016-2018.

Responsabil principal este MEd.

MEd informează, că în prezent are loc stabilirea cadrului normativ în domeniul cercetărilor, după care va fi inițiată realizarea acestei acțiuni.

ANALIZA ŞI CONCLUZII
Privind realizarea PNSC 2016-2020 în sem. I 2016

Analizînd gradul de realizare a acţiunilor din Planul de acțiuni privind implementarea Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (PAI PNSC 2016-2020), în baza informaţiilor prezentate în adresa MTIC de către instituţiile implicate în realizarea acţiunilor, constatăm că majoritatea acestora au fost iniţiate (34 acţiuni din 50 sau 68%), unele din ele fiind şi în proces de realizare (19 acţiuni din 34 sau 56%) şi circa a treia parte din acţiuni nu sunt iniţiate din diverse motive (16 din 50 sau 32%).

Ţinem să menţionăm că, primul semestru de implementare (din cele 10) a Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (PNSC 2016-2020) şi de realizare a PAI PNSC 2016-2020 a demonstrat existenţa a suficiente provocări şi probleme cauzate atît de circumstanţe obiective, cît şi subiective: insuficienţă de fonduri materiale, insuficienţă de resurse calificate, fluctuaţia cadrelor, întîrzieri şi inacţiuni în realizarea acţiunilor.

Cea mai mare provocare poate fi considerat faptul că implementarea PNSC 2016-2020 şi realizarea PAI PNSC 2016-2020 au început fără a avea resursele necesare în buget pentru anul curent.

Implementarea PNSC 2016-2020 şi realizarea PAI PNSC 2016-2020 presupun alocări financiare considerabile. Respectiv, instituţiile implicate sunt în situaţia de a realiza acţiunile prevăzute în condiţiile unei finanţări insuficiente, fără a avea surse necesare în acest scop. Și astfel acestea depun eforturi suplimentare considerabile pentru a atrage potenţiali donatori.

Majoritatea acţiunilor au perioade de realizare de la 2 şi mai mulţi ani (41 acţiuni din 50 sau 82%), dar există o parte de acţiuni cu finalizare în anul 2016 (9 acţiuni din 50 sau 18%).

În acest context, MTIC a pus sub monitorizare sporită aceste 9 acţiuni.

Urmare unei analize separate a gradului de executate a acţiunilor cu finalizare în anul 2016 constatăm că:

- 2 acţiuni din PAI PNSC 2016-2020 nu sunt iniţiate (acţiunile 1.7 şi 4.3);
- 2 acţiuni din PAI PNSC 2016-2020 sunt iniţiate (acţiunile 1.2 şi 3.1);
- 5 acţiuni din PAI PNSC 2016-2020 sunt în proces de realizare (2.1, 4.1, 4.4, 4.6 şi 5.1).

Întîrzierile ce ţin începerea realizării acestor acţiuni se explică prin faptul că unele instituţii se implică mai lent în procesul de implementare a PNSC 2016-2020, fiind implicate într-un număr destul de mare de acţiuni din cadrul altor documente de politici guvernamentale.

Statistica din lista de mai jos cu repartiția acțiunilor pe instituţii responsabile principale (IRP), constată neuniformitatea acestei repartiții:

1) Cancelaria de Stat (CS) – IRP de 13 acţiuni (P=26%), inclusiv sunt în proces de realizare 3 acţiuni (APR=23%);

2) Ministerul Tehnologiei Informaţiei şi Comunicaţiilor (MTIC) – IRP de 12 acţiuni (P=24%), inclusiv sunt în proces de realizare 6 acţiuni (APR=50%);

3) Serviciul de Informaţii şi Securitate (SIS) – IRP de 6 acţiuni (P=12%), inclusiv sunt în proces de realizare 2 acţiuni (APR=33%);

4) Ministerul Afacerilor Interne (MAI) – IRP de 4 acţiuni (P=8%), toate sunt în proces de realizare (APR=100%);

5) Ministerul Educaţiei (MEd) – IRP de 4 acţiuni (P=8%), nici o acţiune nu este în proces de realizare (APR=0%);

6) Autorităţile administraţiei publice centrale şi locale, precum şi alte entităţi, care potrivit normelor legale, deţin sisteme informaţionale de stat (APCLE), lista cărora urmează a fi alcătuită – IRP de 3 acţiuni (P=6%), nici o acţiune nu este în proces de realizare (APR=0%);

7) Institutul Naţional de Justiţie (INJ) – IRP de 2 acţiuni (P=4%), inclusiv o acţiune este în proces de realizare (APR=50%);

8) Procuratura Generală (PG) – IRP de o acţiune (P=2%), care este în proces de realizare (APR=100%);

9) Ministerul Apărării (MA) – IRP de o acţiune (P=2%), care nu este în proces de realizare (APR=0%);

10) Ministerul Finanţelor (MF) – IRP de o acţiune (P=2%), care nu este în proces de realizare (APR=0%);

11) Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI) – IRP de o acţiune (P=2%), care este în proces de realizare (APR=100%);

12) Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (CNPDCP) – IRP de o acţiune (P=2%), care nu este în proces de realizare (APR=0%);

13) Î.S. "Centrul de Telecomunicaţii Speciale" (CTS) – IRP de o acţiune (P=2%), care este în proces de realizare (APR=100%).

Totodată, în statistica de mai sus este indicat indicatorul de performanţă a realizării acţiunilor (APR), care reprezintă raportul dintre numărul acţiunilor în proces de realizare şi numărul acţiunilor care urmau a fi realizate de IRP, exprimat în %, precum şi ponderea (P) care reprezintă raportul dintre numărul de acţiuni al IRP și numărul total de acţiuni din PAI PNSC 2016-2020, exprimat în %.

Analiza aprofundată a datelor statistice din lista de mai sus denotă faptul că procesul de executare a acţiunilor nu depinde de numărul acţiunilor repartizate instituţiilor responsabile principale (IRP). Există instituţii cu o pondere (P) destul de mare de acţiuni şi totodată, au şi un indicator de performanţă APR destul de înalt. Sunt şi instituţii cu aceiaşi pondere medie (P=8%), dar au indicatori de performanţă APR diametral opuşi. Totodată, există mai multe instituţii (61%) cu o pondere (P) foarte mică de acţiuni cuprinsă între 2% şi 6%), care au indicatori de performanţă (APR) foarte diferiţi. Constatăm, că în responsabilitatea acestor instituţii sunt puse realizarea a 11 acţiuni (22%). Acţiunile acestor instituţii au fost puse de MTIC sub o monitorizare sporită.

Există instituţii care, fie din cauza unei structuri interne complexe, fie din cauza unor probleme de comunicare în interior, nu se implică la nivelul aşteptat în realizarea acţiunilor și în raportarea adecvată a informaţiei despre realizarea acestor acțiuni.

În mai multe cazuri, colaboratorii instituţiilor nu fac faţă alcătuirii exhaustive și în termenele stabilite a informaţiei, conform prevederilor pct.2 din Hotărîrea Guvernului nr.811 din 29.10.2015 atît din cauza numărului mare de activităţi, cît şi din cauza calificării acestora. Or, noile tipuri de activităţi solicită suplimentarea cadrelor specializate în domeniul securităţii cibernetice sau recalificarea celor existente.

Totuşi, din rapoartele instituţiilor, reiese că acestea sunt dispuse să colaboreze cu MTIC în procesul de implementare a PNSC 2016-2020.

Urmare acestei analize, MTIC va întreprinde măsuri organizatorice suplimentare în scopul monitorizării sporite şi coordonării eficiente a procesului de realizare a PNSC 2016-2020.