*Proiect*

**GUVERNUL REPUBLICA MOLDOVA**

 **HOTĂRÂRE**

nr. **\_\_\_\_\_**

 din \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017

**cu privire la aprobarea Strategiei naționale pentru prevenirea și combaterea criminalității informatice pentru anii 2018 - 2021**

În scopul prevenirii și combaterii criminalității informatice, precum și stabilirea responsabilităţilor în consolidarea eforturilor comune pentru prevenirea acestui fenomen, Guvernul **HOTĂRĂȘTE:**

     **1.** Se aprobă Strategia națională pentru prevenirea și combaterea criminalității informatice pentru anii 2018 - 2021, conform anexei.

 **2.**  Ministerul Afacerilor Interne, în termen de 6 luni, va elabora şi va prezenta Guvernului spre aprobare, Planul de acţiuni pentru implementarea Strategiei menționate în pct. 1.

 **3.** Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Afacerilor Interne.

 **PRIM-MINISTRU PAVEL FILIP**

 Contrasemnează:

 Ministerul afacerilor interne Alexandru JIZDAN

Anexă

la Hotărârea Guvernului

 nr. \_\_\_\_\_\_\_\_ din \_\_\_\_\_\_\_\_

**STRATEGIA NAȚIONALĂ**

**DE PREVENIRE ȘI COMBATERE**

**A CRIMINALITĂȚII INFORMATICE PENTRU ANII 2018 - 2021**

1. **INTRODUCERE**

Strategia Națională de prevenire și combatere a criminalității informatice pentru anii 2018-2021 (în continuare – Strategie), are drept scop definirea și asigurarea preluării politicii de stat cu stabilirea responsabilităților clare pentru actorii implicați, cât și consolidarea eforturilor comune în prevenirea și combaterea criminalității informatice.

În Planul de acțiuni al Guvernului pentru anii 2016-2018, aprobat prin Hotărârea Guvernului nr. 890 din 20 iulie 2016, a fost stabilită acțiunea 7.4. ”Elaborarea Strategiei naționale privind prevenirea și combaterea criminalității informatice”. Reieșind din faptul că la etapa actuală Concepția securității informaționale a Republicii Moldova este înregistrată în Parlamentul Republicii Moldova, Guvernul și-a asumat responsabilitatea abordării compartimentului prevenirii și combaterii criminalității informatice în mod separat.

De menționat că, în scopul abordării subiectului conform standardelor Uniunii Europene, la baza elaborării Strategiei a servit Raportul de analiză IOCTA 2017, elaborat de EC3 a EUROPOL, precum și Raportul național de analiză a riscurilor în domeniul combaterii criminalității informatice și a altor atacuri asupra sistemelor informatice, pentru anul 2016.

Criminalitatea informatică înglobează 3 domenii de bază: atacurile cibernetice, exploatarea sexuală on-line a copiilor și fraudele comise prin utilizarea mijloacelor de plată electronice.

Astfel, luând în considerație aspirațiile de integrare europeană și rigorile statului de drept în raport cu ameninţările actuale la securitatea informațională, precum și procesul continuu de dezvoltare și modernizare al tehnologiilor, consolidarea forțelor orientate la prevenirea și combaterea fenomenului infracțional în sectorul vizat, domeniul securității informaționale a devenit o prioritate a procesului de guvernare pentru asigurarea ordinii de drept.

 În aceiași ordine de idei, se menționează că realizarea Strategiei va facilita implementarea obligațiunilor asumate în urma ratificării Convenției Consiliului Europei privind criminalitatea informatică (Budapesta, 2001).

Promovarea acestei Strategii este generată și de necesitatea stringentă de a consolida răspunsul structurilor de stat și a sectorului privat în raport cu fenomenul criminalității ce a pătruns în spațiul virtual, prin implementarea unor principii directoare inovatoare întru asigurarea drepturilor și libertăților cetățenilor.

1. **SITUAŢIA CURENTĂ**

Procesul de implementare al tehnologiilor informaționale în toate domeniile vieții economice, sociale și de altă natură a Republicii Moldova, a determinat și evoluția criminalității informatice. Ca urmare, în ultimii ani s-a atestat că rețelele de calculatoare și informațiile electronice sunt folosite tot mai frecvent în scopuri criminale, iar materialele ce ar putea constitui probe ale acestor infracțiuni sunt stocate și transmise tot prin intermediul acestor rețele de către făptuitori.

Riscurile din spațiul cibernetic sunt proporționale cu gradul de informatizare a societății, iar combaterea fenomenului de criminalitate cibernetică trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi.

Tendințele ascensiunii crimei organizate în ultimii ani se află în tandem cu evoluția criminalității informatice, stimulată tot mai intens de aplicabilitatea și accesibilitatea tehnologiei în comiterea infracțiunilor.

Practica internaţională demonstrează impactul pozitiv al infrastructurii informaţionale şi de comunicaţii asupra dezvoltării societăţii contemporane. Aceasta constă în diversificarea posibilităţilor de acces la informaţie şi la resursele informaţionale publice în toate domeniile de activitate umană, precum: guvernarea electronică, economia electronică, comerţul electronic, învăţământul electronic, cultura electronică, medicina electronică etc., precum şi în creşterea nivelului de ocupaţie a populaţiei prin crearea de noi locuri de muncă.

Prosperarea şi dezvoltarea economică a Republicii Moldova depinde de integrarea rapidă în economia regională şi globală tot mai competitivă. Din aceste considerente, edificarea societăţii informaţionale este de o importanţă majoră pentru dezvoltarea ţării şi trebuie să fie realizată într-un mod, în care să poată beneficia toţi cetăţenii de rezultatele acesteia.

Mediul virtual facilitează comiterea infracțiunilor, pune la dispoziţia conduitei criminale atât un nou obiect (informaţia conţinută şi procesată de sistemele informatice), cât şi un nou instrument. Acesta oferă un repertoriu vast de tehnici şi strategii de săvârșire a infracţiunilor, generând tendințe noi de infracţiuni.

Fraudele informatice, atacurile informatice, fraudele cu mijloace de plată electronice și pornografia infantilă în internet sunt tipuri infracționale care necesită investigații specializate, o pregătire și dotare corespunzătoare a structurilor de aplicare a legii.

Criminalitatea informatică este un fenomen infracțional care alimentează, la rândul său, foarte multe riscuri și crize în spațiul cibernetic.

Evoluția fenomenului criminogen în Republica Moldova în ultimii ani este strâns legată de spațiul cibernetic, ceea ce se manifestă prin folosirea tot mai intensă a tehnologiilor informaționale la comiterea infracțiunilor. Internetul a devenit o parte integrantă și indispensabilă a societății și economiei.

Cu cât o societate este mai informatizată, cu atât este mai vulnerabilă, iar prevenirea și combaterea criminalității informatice trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.

Analiza Raportului național privind riscurile în domeniul combaterii criminalității informatice și a altor atacuri asupra sistemelor informatice, pentru anul 2016, identifică câteva fenomene - cheie privind criminalitatea informatică, abordarea cărora va servi la diminuarea fenomenului la nivel național.

**1. Atacurile cibernetice:**

 a) produsele-program de tip malware, precum ransomware, RAT și troiane bancare;

 b) malware, ce facilitează comiterea infracțiunilor, precum droperi și spam;

 c) atacurile DDoS;

 d) botnet-uri.

**2. Exploatarea sexuală online a copiilor:**

 a) producerea și distribuirea pornografiei infantile, inclusiv în urma autoproducerii;

 b) discuțiile online cu caracter sexual, grooming și hărțuire sexuală;

 c) recrutarea copiilor în scopul exploatării sexuale și producerii pornografiei infantile;

 d) exploatarea sexuală prin intermediul videoconferințelor;

 e) deplasarea abuzatorilor peste hotare pentru exploatarea sexuală a copiilor;

 f) utilizarea softurilor și platformelor on-line pentru exploatarea sexuală a copiilor.

**3. Fraudele prin utilizarea mijloacelor de plată electronice:**

 a) fraude card-present:

 - malware ATM/POS (Black Boxing, Jackpotting, Man-in-the-Middle);

 - skimere;

 b) fraude card-not-present;

 c) datele financiare compromise.

**4. Adaptarea serviciilor internet pentru comiterea infracțiunilor informatice de diferite genuri:**

 a) web site-uri cu conținut ilegal din Darknet;

 b) servicii de anonimat - VPN, proxy;

 c) money mule și utilizarea frauduloasă a portmoneelor electronice;

Bitcoin și alte valute cryptografice.

1. **DEFINIREA PROBLEMELOR CARE NECESITĂ IMPLICAREA GUVERNULUI PRIN APLICAREA POLITICII DE RIGOARE**

Dezvoltarea tehnologică şi utilizarea pe scară largă a sistemelor informatice aduce după sine şi o serie de riscuri. Dependenţa tot mai accentuată a agenţilor economici, a instituţiilor publice şi chiar a utilizatorilor individuali de sistemele informatice ce le gestionează în mare măsură resursele, face ca aceştia să fie tot mai vulnerabili la impactul pe care îl poate avea criminalitatea informatică, asigurarea prevenirii și combaterii căreia este una din sarcinile de bază ale statului, implementate prin instituțiile sale de drept, inclusiv Procuratură.

Astfel, au fost determinate următoarele probleme care necesită a fi abordate la nivel național:

1. **Cadrul normativ**

În urma analizei legislației naționale au fost atestate un șir de bariere și lacune de ordin normativ, ce includ:

1. Codul penal nr.985-XV din 18.04.2002:

 - majoritatea infracțiunilor informatice sunt incluse în categoria celor mai puțin grave, ceea ce nu permite înfăptuirea măsurilor speciale de investigații necesare;

 - art. 178 ”Violarea dreptului la secretul corespondenţei” nu prevede răspunderea penală pentru faptele comise în privința corespondenței (mesageriei) electronice, întrucât noțiunea de ”trimiteri poștale” conform Legii comunicațiilor poștale din 17.03.2016 prevede numai bunurile fizice expediate și recepționate;

 - art. 208 alin. (1) ”Pornografia infantilă” nu incriminează obţinerea accesului cu bună ştiinţă, prin intermediul tehnologiilor informaţionale şi a comunicaţiilor, la pornografia infantilă, deși aceasta este prevăzut în Convenția Lanzarote;

 - majoritatea infracțiunilor prevăzute în Capitolul XI Cod penal sunt infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor care au componență materială și se consumă la survenirea unui prejudiciu de peste 100.000 lei.

1. Codul de procedură penală nr.122-XV din 14.03.2003:

- nu este reglementată procedura ”Percheziției informatice”, prevăzută în Convenția de la Budapesta și efectuarea copiilor datelor informatice (clonare);

- lipsește măsura specială de investigații de interceptare a datelor informatice;

- nu este prevăzută măsura obținerii comunicărilor prin mijloacele electronice - mesageria textuală prin sisteme informatice în afara serviciilor de telefonie și alte comunicări electronice - de la prestatorii serviciilor de poștă electronică, chat etc;

c) Codul contravențional nr.2018-XVI din 24.10.2008 nu reglementează răspunderea pentru încălcarea de către furnizorii de servicii de comunicații electronice a obligațiilor prevăzute în Legea comunicațiilor electronice nr.36 din 17.03.2016 și Legea privind prevenirea și combaterea criminalității informatice nr. 20-XVI din 03.02.2009.

d) Alte reglementări:

 - nu este prevăzută excluderea accesului prin Internet la pornografie infantilă și alte informații provenite în urma infracțiunilor sau utilizate pentru comiterea acestora;

- actualmente, legislația națională nu reglementează protecția infrastructurilor critice, inclusiv a celor informatice, care odată cu accelerarea procesului de informatizare, devin tot mai importante. Noțiunea de ”infrastructuri critice”, precum și entitățile de importanță vitală, atribuite la această categorie, nu sunt determinate de stat. Această lacună reprezintă o mare vulnerabilitate în asigurarea continuității și normalității funcționării instituțiilor de bază ale statului și a serviciilor de importanță vitală.

În contextul dat, menționăm că la 8 decembrie 2008 a fost adoptată Directiva 2008/114/CE „Privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora”. La etapa actuală a progresului tehnologic şi procesului de informatizare a vieţii economice, politice, sociale şi de altă natură, funcţionarea mecanismelor principale ale statului se realizează prin utilizarea produselor program şi schimbului de date digitalizate, care formează în ansamblu infrastructura critică informatică.

Infrastructura oricărei naţiuni asigură funcţionarea normală a instituţiilor publice şi private din sectoarele economic, financiar, alimentar, al comunicaţiilor, al sănătăţii publice şi de altă natură. Într-o societate modernă, mecanismul de funcţionare al acestor instituţii se sprijină pe anumite sisteme cibernetice, formate din reţele de computere, servere şi produse de program ce asigură dirijarea automatizată a proceselor. Ameninţările actuale din partea criminalităţii cibernetice determină acordarea unei atenţii deosebite protecţiei infrastructurilor critice informatice. Complexitatea şi interdependenţa elementelor acestei infrastructuri impun luarea unor măsuri de protecţie la nivel naţional.

1. **Cadrul instituțional:**

- lipsa specialiștilor cu cunoștințe avansate în domeniul IT;

- lipsa unor programe de instruire dedicate angajaților cu atribuții de investigare și urmărire penală, procurorilor, judecătorilor, personalului tehnic;

- lipsa echipamentului și soft-ului dedicat investigării infracțiunilor informatice;

- nivel jos de salarizare a funcționarilor publici în raport cu sectorul privat din domeniul IT;

- participarea insuficientă în cadrul proiectelor și evenimentelor internaționale de consolidarea capacităților și schimbului de bune practici;

- lipsa unor câmpuri specifice activității desfășurate în domeniul criminalității informatice, în Banca Centrală de date a sistemului informațional automatizat ”Registru informații criminalistice și criminologice”;

- lipsa resurselor financiare necesare măsurilor de prevenire a criminalității informatice;

- lipsa delimitării clare a responsabilităților a fiecărei instituții implicate în procesul de prevenire și combatere a criminalității informatice.

1. **Tehnologiile ce facilitează comiterea infracțiunilor informatice:**

**-** mijloacele de anonimizare;

**-** puncte de acces wireless deschis la rețeaua globală Internet (Wi-Fi public);

**-** utilizarea algoritmelor complexe asimetrice de criptare a informației critice la estorcarea mijloacelor financiare;

**-** utilizarea sistemelor de plată electronice desconcentrate în baza cripto-algoritmelor (cripto-valuta Bitcoin ș.a.);

**-** rețelele de schimb direct de date dintre utilizatori, ceea ce nu lasă careva urme a activităţii în conţinutul istoricului înregistrat în sistemul informatic sau în log-urile deţinute de furnizorii de servicii;

**-** utilizarea web hosting-ului de către infractori. Astfel, deşi persoanele care distribuie pornografie infantilă sau administrează web site-uri cu conţinut interzis sunt înregistrate cu adrese IP atribuite Republicii Moldova, deseori aceştia au contracte încheiate cu furnizorii naţionali de servicii, aflându-se peste hotarele statului;

- furnizorii ”mici” nu asigură un nivel minim de securitate cibernetică a propriei rețele și deseori nu duc evidența utilizatorilor de servicii și nu înregistrează metadatele privind accesul la rețeaua Internet;

**-** serviciile de Internet fix prestate pe teritoriul din stânga Nistrului.

**IV. FACTORI DE RISC ÎN IMPLEMENTAREA STRATEGIEI**

În procesul de prevenire și combatere a criminalității informatice au fost identificate următoarele obstacole sau factori de risc în implementarea prezentei Strategii:

a) problemele economice ale ţării nu permit acordarea unui sprijin financiar pentru implementarea Strategiei per ansamblu şi implementarea sa în mare parte va depinde de asistenţa tehnică internaţională;

b) procesele periodice de reorganizare a instituțiilor de resort, transformarea şi reducerea statelor de personal, nivelul jos de salarizare a funcționarilor publici pun în pericol mecanismul de implementare, coordonare și monitorizare realizării obiectivelor Strategiei;

c) necesitatea asigurării unei pregătiri continuă a specialiştilor, cu scopul de a creşte nivelul de sensibilizare a acestora în ceea ce priveşte problema criminalității informatice şi nivelul capacităţii de abordare a problemei;

d) instabilitatea politică, ceea ce poate conduce la o schimbare în priorităţile politicii interne şi externe;

e) atitudinea conservatorie, cât și nivel jos de conștientizare a pericolului spațiului virtual, poate conduce la imitarea activităţii, realizarea formală și lipsa progresului real în atingerea obiectivelor Strategiei.

Factorii de risc identificaţi pot afecta cu siguranţă implementarea prezentei Strategii. În acelaşi timp, existenţa anumitor obligaţii internaţionale ale RM în domeniul combaterii criminalității informatice, participarea la lucrările Comitetului Consiliului Europei privind criminalitatea informatică, alte organisme internaționale, creează premize favorabile pentru implementarea cu succes a prezentei Strategii.

1. **OBIECTIVELE SRATEGIEI**

Obiectivele Strategiei au o importanţă extrem de majoră în procesul de realizare a obligațiunilor asumate de către stat pe calea integrării în spațiul comunitar european și în particular la perfecţionarea bazei normative ce reglementează combaterea criminalității informatice.

Adoptarea şi dezvoltarea continuă a unor bune practici de investigare, codificate în proceduri standard unitare la nivelul instituţiilor de aplicare a legii, completate de măsuri de îmbunătăţire a capacităţii de colectare şi analiză a informaţiilor din surse variate, reprezintă premisele unui răspuns coerent şi eficace în descurajarea acţiunilor criminale pe acest domeniu.

De asemenea, urmărirea profitului obţinut de grupările criminale organizate trebuie să reprezinte un deziderat în anchetarea cauzelor de infracțiuni informatice, inclusiv în cauzele cu componentă transfrontalieră.

Obiectivul principal al Strategiei, stabilit în urma analizei efectuate și identificării problemei de bază, este consolidarea eforturilor comune în prevenirea și combaterea criminalității informatice, identificarea intervenţiilor necesare pentru diminuarea impactului dăunător al criminalității, atacurilor și incidentelor cibernetice asupra dezvoltării sigure a societății informaționale.

Realizarea obiectivului principal al Strategiei, în conformitate cu problemele identificate, se va produce prin realizarea complexă a următoarelor obiective specifice:

1. implementarea Convenției Consiliului Europei privind criminalitatea informatică (Budapesta, 2001) și a Convenției Consiliului Europei pentru protecţia copiilor împotriva exploatării sexuale şi a abuzurilor sexuale(Lanzarote, 2007);
2. combaterea atacurilor cibernetice asupra datelor și rețelelor;
3. combaterea exploatării sexuală online a copiilor;
4. combaterea fraudelor prin utilizarea mijloacelor de plată electronice;
5. combaterea utilizării frauduloase a tehnologiilor la comiterea crimelor informatice;
6. dezvoltarea capacităților de prevenire și reacție urgentă la nivel național;
7. educația, formarea și informarea continuă în domeniul criminalității informatice;
8. cooperarea internațională.
9. **MĂSURILE NECESARE PENTRU ATINGEREA OBIECTIVELOR ŞI REZULTATELOR SCONTATE**
10. **Combaterea atacurilor cibernetice asupra datelor și rețelelor**

Dezvoltarea mijloacelor de comunicații într-un ritm fără precedent este, proces cu un impact semnificativ atât asupra societății, cât și asupra cetățenilor. Lumea globalizată este caracterizată de interdependențe complexe. Totodată, această dezvoltare aduce, pe lângă multitudinea de beneficii incontestabile, o serie de provocări. Astfel, datorită dezvoltării tehnologice, mediul de securitate devine tot mai dinamic, vulnerabilitățile şi amenințările depășind barierele spațiului fizic și manifestându-se, deseori, în mediul virtual.

În temeiul celor expuse, apare necesitatea de a întreprinde măsuri interdepartamentale, la nivel național în următoarele direcții:

- înființarea în cadrul Centrului pentru Securitate Cibernetică(CERT) a unui Sistem național de alertă și informare în timp real despre incidentele de securitate cibernetică. Acest sistem va permite gestionarea incidentelor de securitate în timp real prin preluarea automatizată a alertelor de securitate de la parteneri naționali sau internaționali și transmiterea acestora către operatorii/deținătorii/ administratorii sistemelor informatice suspectate de derularea unor activități malițioase în internet;

- alocarea resurselor suficiente pentru investigarea infracțiunilor informatice;

- informarea publicului privind modalitățile de prevenire a atacurilor asupra datelor informatice și rețelelor, inclusiv privind fenomenele nou-apărute la nivel național.

1. **Combaterea exploatării sexuală online a copiilor**

În vederea combaterii exploatării sexuale a copiilor în mediul online, este necesar de întreprins un șir de acțiuni, cu implicarea activă a societății civile:

- acordarea priorității asistenței copilului victimă în cadrul investigațiilor;

- identificarea soluțiilor tehnice de documentare a abuzatorilor care folosesc instrumentele de anonimizare online, rețelele de partajare a fișierelor și rețeaua Darknet;

- desfășurarea companiilor de informare a publicului, inclusiv în cooperarea cu ONG-uri și societatea civilă;

- cooperarea cu furnizorii de servicii de comunicații electronice, în special cei ale căror servicii sunt utilizate de infractori la comiterea infracțiunilor respective: companiilor de hosting, servere VPN și proxy;

1. **Combaterea fraudelor prin utilizarea mijloacelor de plată electronice**

În vederea combaterii fraudelor prin utilizarea mijloacelor de plată electronice, este necesar de întreprins un șir de acțiuni, cu implicarea instituțiilor financiare și prestatorilor serviciilor de plăți electronice:

- schimbul de informații dintre Centrul pentru combatere a crimelor informatice și băncile licențiate, referitor la cardurile bancare compromise;

- implementarea de către bănci a măsurilor de securitate sporită în privința ATM-lor la nivel de hardware și software.

1. **Combaterea utilizării frauduloase a tehnologiilor la comiterea crimelor informatice**

În vederea diminuării utilizării tehnologiilor informaționale în scopuri criminale sunt necesare:

- monitorizarea celor mai noi tendințe de utilizare a tehnologiilor informaționale la comiterea oricărui gen de infracțiune;

- stabilirea relațiilor cu sectorul privat, în vederea abordării continue a vulnerabilității produselor software și a echipamentelor hardware;

- fortificarea cooperării internaționale în vederea identificării utilizatorilor din Darknet, I2P și Freenet.

1. **Educația, formarea și informarea continuă în domeniul criminalității informatice**

- dezvoltarea și implementarea unor programe de instruire dedicate angajaților cu atribuții de investigare și urmărire penală, procurorilor, judecătorilor, personalului tehnic;

 - abordarea în cadrul campaniei ”Luna securității cibernetice” subiectul criminalității informatice;

1. **Cooperarea internațională**

- utilizarea instrumentului EMAS (Europol Malware Analysis Service) al EUROPOL;

- utilizarea metodelor de identificare a victimelor, inclusiv prin utilizarea Sistemului Informațional ”Protecția Copiilor” și a bazei de date ”ICSE” a OIPC INTERPOL;

- utilizarea canalului virtual stabilit cu NCMEC (Centrul Național al SUA privind Copiii Dispăruți și Exploatați), precum și aderarea la alte inițiative similare;

- schimbul de informații cu statele din care provin carduri bancare compromise și statele în care are loc extragerea banilor de pe cardurile respective;

- participarea la evenimente internaționale în domeniul prevenirii și combaterii criminalității informatice.

1. **ESTIMAREA IMPACTULUI ȘI A COSTURILOR (FINANCIARE ŞI NONFINANCIARE) AFERENTE IMPLEMENTĂRII STRATEGIEI**

Pentru realizarea măsurilor planificate, fiecare autoritate responsabilă de executarea acestora, va prevedea în bugetul anual resurse financiare.

Fiecare autoritate, responsabilă în dezvoltarea şi implementarea prezentei Strategiei, va aloca din bugetele proprii mijloacele necesare pentru finanţarea tuturor măsurilor şi intervenţiilor particulare planificate spre realizare, conform Planului de acţiuni privind prevenirea şi combaterea crimelor informatice.

1. **ETAPE DE IMPLEMENTARE**
2. **Strategia naţională de prevenire și combatere a criminalității informatice pentru anii 2018-2021, prevede următoarele etape de implementare:**
	1. Elaborarea unui Plan de acțiuni privind implementarea Strategiei care va stabili responsabilitățile instituțiilor implicate;
	2. Îmbunătățirea capacității instituționale de investigare a infracțiunilor informatice, în vederea asigurării compatibilizării cu structurile europene în conformitate cu convențiile, acordurile, recomandările și legislația națională:

 ***-*** dezvoltarea capacităților instituționale subdiviziunilor specializate ale Ministerului Afacerilor Interne, Serviciului de Informații și Securitate, Procuraturii Generale, Ministerului Economiei și Infrastructurii;

- asigurarea continuităţii şi sustenabilităţii programelor de formare în domeniul combaterii crimelor informatice a specialiştilor din structurile de aplicare a legii;

- urmărirea bunurilor și a profiturilor obţinute din comiterea infracţiunilor cibernetice.

1. **Creșterea capacitățiide colectare și analiză a datelor privind infracțiunile informatice:**

- colectarea, centralizarea şi analizarea datelor privind fenomenul criminalităţii informatice, la nivel naţional, de către subdiviziunea specializată a Procuraturii Generale, Ministerului Afacerilor Interne;

- coordonarea activităților de cooperare ale structurilor specializate;

- dezvoltarea schimbului de date și informații cu autoritățile publice centrale, companiile private, operatorii serviciilor de telefonie mobilă și furnizorii de servicii.

1. **PROCEDURILE DE RAPORTARE ȘI MONITORIZARE**

 Implementarea Strategiei, este asigurată de către Guvern și alte autorități publice centrale: Ministerul Afacerilor Interne, Serviciul de Informații și Securitate, Procuratura Generale, Ministerului Economiei și Infrastructurii, Cancelaria de Stat, Institutul Național de Justiție.

În procesul implementării Strategiei se va efectua monitorizarea periodică a realizării acţiunilor şi evaluarea rezultatelor obţinute pentru ca, în caz de necesitate, să fie operate modificările necesare. La nivel național, procedurile de raportare și evaluare se efectuează de Procuratura Generală în baza informației de raportare a monitorizării și evaluării prezentate semestrial de responsabilii principali de executarea acțiunilor din Planul de acțiuni. Evaluarea se efectuează prin compararea rezultatelor reale obținute față de cele scontate pentru perioada respectivă de raportare.

Rezultatele implementării Strategiei se vor prezenta la sfârşitul anului 2021 într-un raport de evaluare finală a implementării Strategiei, în care se va reflecta realizarea rezultatele atinse în cadrul fiecărei priorități strategice și al Strategiei în general.