

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ministerul Afacerilor Interne** | **Ministerul Afacerilor Externe și Integrării Europene** | **Procuratura Generală** | **Serviciul de Informații și Securitate** | **Î.S. „MoldData”** | **Centrul de telecomunicații speciale** |

 **O R D I N C O M U N**

**“ \_\_\_\_ „ martie 2016 mun. Chişinău nr.** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Cu privire la aprobarea Concepției integrate de analiză a riscului în domeniul combaterii criminalității informatice**

În scopul implementării punctului 16 acțiunea nr. 20 din Titlul III al Planului național de acțiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană în perioada 2014-2016, aprobat prin Hotărîrea Guvernului nr. 808 din 07.10.2014,

**O R D O N Ă M:**

1. Se aprobă Concepția integrată de analiză a riscului în domeniul combaterii criminalității informatice, conform anexei.
2. Controlul instituţional asupra executării prevederilor prezentului Regulament se pune în sarcina conducătorilor instituţiilor semnatare.
3. Prezentul ordin intră în vigoare la data semnării de către instituţiile responsabile.

**Ministrul afacerilor interne Alexandru JIZDAN**

**Viceprim-ministru, ministrul afacerilor externe**

**și integrării europene Andrei GALBUR**

**Prim-adjunct al Procurorului general Eduard HARUNJEN**

**Director al Serviciul de Informații**

**și Securitate Mihai BALAN**

**Administrator Î.S. „MoldData” Ana BRADU**

**Director general al**

**Î.S. „Centrul de telecomunicații speciale” Serghei POPOVICI**

**Tabelul de repartizare:**

1. Direcţia documentare ……………………………………………………....1 ex;
2. Direcţia generală juridică…………………………………………………...1 ex;
3. Inspectoratul General al Poliţiei………………………………………….....1 ex;

Total 3 ex.

**Şef adjunct al IGP al MAI,**

**colonel de poliţie Gheorghe CAVCALIUC**

**Anexă**

 la ordinul comun nr.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ din \_\_\_\_\_\_\_\_\_2016

 **CONCEPȚIA INTEGRATĂ DE ANALIZĂ A RISCULUI ÎN DOMENIUL COMBATERII CRIMINALITĂŢII INFORMATICE**

**I. Importanța analizei riscurilor în domeniul combaterii criminalităţii informatice**

Criminalitatea informatică reprezintă un fenomen social negativ caracterizat printr-un ansamblu de activităţi infracţionale în care datele informatice şi/sau sistemele informatice constituie instrument de comitere a infracţiunilor sau obiect al infracţiunilor.

Procesul de implementare a tehnologiilor informaționale în toate domeniile vieții economice, sociale și de altă natură a Republicii Moldova a determinat evoluția fenomenului infracțional și extinderea acestuia asupra spațiului cibernetic. Astfel, 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.

Luînd în considerație aspirațiile de integrare europeană și rigorile statului de drept în raport cu ameninţările actuale la securitatea informațională, procesul continuu de dezvoltare și modernizare a tehnologiilor, consolidarea forțelor orientate la prevenirea și combaterea fenomenului infracțional în sectorul vizat a devenit o prioritate a procesului de guvernare în sectorul asigurării ordinii de drept.

Analizînd situaţia actuală la capitolul dezvoltării accesului publicului la internet, constatăm o extindere accelerată a gradului de utilizare a resurselor informaţionale globale. Astfel, odată cu dezvoltarea informatizării serviciilor în domeniul economic, social, administrativ etc., se impune asigurarea securităţii informaţionale şi combaterea criminalităţii informatice, precum şi a altor infracţiuni a căror instrument de bază sînt resursele informaţionale.

Criminalitatea informatică cu un nivel ridicat de dezvoltare în țările din jurul Republicii Moldova, este un factor care trebuie să argumenteze implementarea anumitor politici în raport cu noile provocări infracționale.

**II. Starea de fapt**

2.1. Cadrul normativ

- Convenţia Consiliului Europei privind criminalitatea informatică, ratificată la 02 februarie 2009;

- Convenţia Consiliului Europei pentru protecţia copiilor împotriva exploatării sexuale şi a abuzurilor sexuale, ratificată la 19 decembrie 2011;

- Directiva 2011/92/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile;

- Codul penal al Republicii Moldova nr. 985 din 18 aprilie 2002;

- Codul de procedură penală al Republicii Moldova nr. 122 din 14 martie 2003;

- Legea nr. 59 privind activitatea specială de investigaţii din 29 martie 2012;

- Legea nr. 20-XVI privind prevenirea şi combaterea criminalităţii informatice din 3 februarie 2009;

- Legea comunicaţiilor electronice nr. 241 din 15 noiembrie 2007;

- Legea nr. 753 din 23 decembrie 1999 privind Serviciul de Informaţii şi Securitate al Republicii Moldova;

- Legea nr. 294 din 25.12.2008 cu privire la Procuratură;

- Ordinul comun nr.45/84/250/105/373 din 28 august 2014 ”Cu privire la modul de colaborare între organele de drept ale Republicii Moldova şi Centrul cooperare poliţienească internaţională al Inspectoratului General al Poliției”.

2.2. Cadrul instituțional

2.2.1. Ministerul Afacerilor Interne.

În contextul procesului de reformare a Poliției, desfășurat în conformitate cu Hotărîrea Guvernului Republicii Moldova nr. 986 din data de 24 decembrie 2012, în cadrul Ministerului Afacerilor Interne a fost creat Centrul pentru combaterea crimelor informatice al INI al IGP. În atribuțiile Centrului intră îndeplinirea responsabilităților și punerea în aplicare a politicii de stat în domeniul combaterii infracțiunilor informatice.

2.2.2. Serviciul de Informații și Securitate.

Spaţiul cibernetic ajunge să reprezinte o platformă confortabilă pentru pregătirea şi efectuarea crimelor informatice, a actelor de terorism cibernetic şi a altor acţiuni maliţioase, menite să afecteze, direct sau indirect, securitatea naţională. Astfel, penetrarea sistemelor informaţionale sau de comunicaţii electronice ale autorităţilor administraţiei publice şi ale altor instituţii şi întreprinderi de stat sau private, în cadrul cărora se gestionează informaţie sensibilă, poate duce la compromiterea confidenţialităţii, integrităţii sau disponibilităţii acestei informaţii, şi, prin urmare, la cauzarea prejudiciilor financiare sau de altă natură, inclusiv la afectarea securităţii statului. De asemenea, penetrarea sistemelor informatice aferente infrastructurii critice ale Republicii Moldova poate duce la obţinerea controlului neautorizat asupra acestor sisteme, şi, în consecinţă, la afectarea proceselor economice, sociale, politice, informaţionale, militare etc. În acest context, Serviciul de Informații și Securitate este chemat să combată agresiunile din mediul virtual, intern sau extern, îndreptate spre sistemele informatice şi de comunicaţii electronice de importanţă statală.

2.2.3. Procuratura Generală.

Procuratura Generală exercită coordonarea, conducerea şi urmărirea penală în cazurile comiterii infracţiunilor informatice, reprezintă acuzarea în numele statului în instanţele de judecată, în vederea atragerii la răspundere penală a infractorilor.

2.2.4. CERT-GOV-MD.

Misiunea Centrului pentru Securitatea Cibernetică este de a susţine societatea moldovenească în protejarea împotriva incidentelor IT. CERT-GOV-MD va fi punctul central de raportare şi coordonare privind incidentele de securitate în sistemele de comunicaţii şi informatice aflate în administrarea Întreprinderii de Stat ”Centrul de telecomunicaţii speciale”. CERT-GOV-MD va facilita schimbul de informaţii privind incidentele IT între organizaţiile din societate şi va disemina informaţiile legate de noi probleme, care ar putea împiedica funcţionarea sistemelor IT guvernamentale. Totodată, CERT-GOV-MD asigură informaţii şi consultanţă privind măsuri pro-active, precum compilarea şi completarea statisticilor.

2.3. Cooperarea dintre sectorul public și privat.

2.3.1. Furnizorii de servicii de comunicații electronice și sectorul bancar privat.

În Republica Moldova, parteneriatul public-privat în domeniul combaterii criminalității informatice este într-o fază incipientă. La nivelul cooperării cu furnizorii de servicii de comunicații electronice și sectorul bancar, care au un rol important în procesul de combatere a criminalității informatice în calitate de deținători de date informatice, persistă un grad scăzut de comunicare și de cunoaștere reciprocă.

Sectorul privat nu cunoaște structura și responsabilitățile unităților specializate din cadrul autorităților publice și nici modalitățile de raportare a unor activități ilicite sau a incidentelor de securitate. Nu există puncte de contact între partenerii privați și cei din sectorul public și există o lipsă de evenimente de pregătire în comun. Sectorul privat este descurajat în raportarea activităților ilegale datorită neclarităților din legislație cu privire la competențele structurilor specializate și a impedimentelor în derularea unor investigații în domeniu (Ex: necesitatea unui prejudiciu minim de 50.000 Lei).

2.3.2. Banca Națională a Moldovei

Inspectoratul General al Poliției a semnat acordul de colaborare cu Banca Națională a Moldovei. Acordul prevede schimbul de informații cu privire la fraude, infracțiuni informatice și contravenții în domeniul comunicațiilor, aferente activității desfășurate de către prestatorii serviciilor de plată, precum și cele aferente utilizării instrumentelor de plată fără numerar.

2.3.3. Î.S. ”MoldData”

Inspectoratul General al Poliției a semnat acordul de colaborare cu Întreprinderea de Stat ”MoldData”, care prevede schimbul de informații în scopul prevenirii și combaterii infracțiunilor, sesizării contravențiilor din domeniul informatic, asigurării securității spațiului cibernetic, precum și neadmiterii funcționării ilicite a unor nume de domenii de nivel superior din zona ”MD” ce direcționează la conținuturi cu informații și imagini cu caracter obscen sau ofensator, sau ce defăimează Republica Moldova sau alte state, cheamă la violență sau pot aduce prejudicii imaginii Republicii Moldova pe plan internațional.

2.3.4. ONG-urile.

Inspectoratul General al Poliției a semnat acorduri de colaborare cu Centrul International „La Strada” și Centrul Naţional de Prevenire a Abuzului faţă de Copii (CNPAC). Acordurile includ cooperarea în combaterea pornografiei infantile și exploatării sexuale on-line a copiilor, dezvoltarea parteneriatului social, stabilirea cooperării permanente, egale şi reciproce dintre organele de drept şi societatea civilă în scopul implementării politicii de stat în combaterea fenomenului vizat, aplicarea pe segmentul poliţienesc a Instrucţiunilor privind mecanismul intersectorial de cooperare pentru identificarea, referirea, evaluarea, asistenţa şi monitorizarea copiilor victime a infracțiunilor respective, precum și alte măsuri de cooperare.

2.4. Dezvoltarea relațiilor internaţionale

Organele de drept din Republica Moldova pot colabora cu statele-membre OIPC Interpol sau OEP Europol în domeniul combaterii criminalităţii informatice.

2.4.1. OIPC-INTERPOL este organizația internațională a poliției criminale, avînd 190 state-membre. Scopul de bază al OIPC Interpol este sporirea interacţiunii între forţele de poliţie la nivel internaţional pentru a asigura securitatea locală, regională şi globală.

2.4.2. Europol este o agenție a Uniunii Europene de aplicare a legii al cărei scop principal este de a contribui la realizarea unei Europe mai sigure pentru beneficiul tuturor cetățenilor UE. Scopul principal al Europol este de eficientiza și extinde cooperarea între autoritățile competente ale statelor membre ale UE în domeniul prevenirii și combaterii criminalității internaționale organizate.

Europol lucrează în strînsă colaborare cu agențiile de aplicare a legii în toate statele membre ale UE, precum și în alte state partenere din afara UE, cum ar fi Australia, Canada, SUA, Norvegia și Republica Moldova.

La 18 decembrie 2014 Republica Moldova a semnat Acordul de cooperare operațională și strategică cu Europol.

**III. Analiza SWOT de bază**

3.1. Puncte forte:

* Structura instituțională;
* Cooperarea interinstituțională;

3.2. Puncte vulnerabile:

* Grad redus de informare a publicului referitor la fenomenul criminalității informatice și autoritățile competente în examinarea cazurilor cu privire la infracțiunile informatice.
* Probleme logistice;
* Nivel de salarizare a specialiștilor în domeniul IT;
* Dotarea și instruirea tehnică;
* Lacunele legislative;
* Colaborarea cu operatorii de telefonie fixă și mobilă;
* Colaborarea cu companiile care prestează servicii Internet;
* Colaborarea cu administrația site-urilor din Republica Moldova;
* Schimbul de experiență cu alte state în domeniul prevenirii și combaterii criminalității informatice;
* Anonimitatea în rețeaua Internet;

3.3. Oportunităţi:

* Dezvoltarea unei cooperări eficiente în domeniul combaterii criminalității informatice cu omologii din alte state, organizații internaționale de profil**;**
* Stabilirea relațiilor de cooperare cu echipele CERT, în scopul facilitării schimbului de informații și oferirii suportului necesar în cazul atacurilor cibernetice;
* Dezvoltarea capacităților practice a personalului în cadrul proiectelor internaţionale;

3.4. Riscuri:

- Dezvoltarea rapidă a tehnologiilor informaţionale la nivel global;

- Imperfecțiunea cadrului juridic normativ în raport cu procesele tehnologice indisolubil legate de fenomenul criminalității informatice;

- Evidența necorespunzătoare de către furnizorii de servicii a utilizatorilor rețelei Internet.

**IV. Procesul de analiză a riscurilor**

În plan internațional, au fost elaborate și implementate mai multe principii de analiză a riscului. Metoda modelului în cascadă constituie una din metodele recunoscute pe plan internațional şi aplicate frecvent în practică. În cadrul analizei riscului în domeniul combaterii criminalităţii informatice, aceasta poate cuprinde următoarele şapte etape:

1) – identificarea valorilor protejate;

2) – identificarea tipurilor de infracțiuni informatice;

3) – analiza statistică a fenomenului de criminalitate informatică;

4) – determinarea consecinţelor prejudiciabile ale infracțiunilor informatice;

5) – stabilirea soluţiilor pentru minimizarea riscului;

6) – evaluarea eficienţei implementării soluţiilor pentru minimizarea riscului;

7) – determinarea raportului cost/nivel de combatere a infracțiunilor informatice.

4.1. Identificarea valorilor protejate - reprezintă o etapă de analiză complexă, care vizează:

4.1.1. Definirea entități care a devenit ținta infracțiunii informatice, incluzînd, după caz, domeniul de activitate, infrastructura, structura organizatorică, strategia şi tacticile utilizate, sistemul de relaţii cu furnizorii şi clienţii, natura comportamentului, adaptabilitatea și flexibilitatea, nivelul de informatizare, categoriile de informaţii şi de surse de informaţii etc.

4.1.2. Stabilirea proprietăţii care se referă la resursele informatice și mijloacele de plată electronice, tehnologiile, datele cu caracter personal etc.

4.1.3. Identificarea informaţiilor care se referă la datele, activităţile şi materialele confidenţiale sau care constituie proprietatea intelectuală a entității, dar şi la informaţiile operaţionale sau structurate în baze documentare.

4.2. Identificarea tipurilor de infracțiuni informatice - constă în stabilirea evenimentelor concrete nedorite (atacurile hacker-ilor, atacuri malware, atacuri botnet, sustrageri din conturi bancare, exploatarea sexuală în Internet a copiilor etc.) care pot afecta valorile protejate.

4.2.1. Identificarea are la bază analiza evenimentelor, obiectivelor, organizaţiilor, infrastructurii şi a mediului, fiind concretizată în evidenţierea evenimentelor care se pot produce, a frecvenţei de producere, a gamei de intensităţi, a influenţei asupra valorilor protejate, precum şi a corelaţiilor dintre acestea, mediul și infrastructura.

4.2.2. Infracţiunile sau evenimentele de natură criminală se identifică în funcţie de natura activităţii și structurii entității, de categoriile şi mărimea valorilor, de distribuţia şi circulaţia acestora.

4.2.3. Infracţiunile identificate se grupează într-o matrice de ameninţări criminale în care, pe lîngă infracţiunile identificate, ierarhizate după diferite criterii (frecvenţă, intensitate, prejudiciul etc.), se trec şi caracteristicile acestora: frecvenţa producerii (posibilitatea, probabilitatea), intensitatea sau virulenţa, numărul de participanţi, valorile vizate, prejudiciul produs direct și indirect etc.

4.3. Analiza statistică a fenomenului de criminalitate informatică - se bazează pe studiul impactului fenomenului infracțional asupra unei entități în cazul repetării aceluiași tip de infracțiune şi presupune o analiză a statisticilor în domeniu, observaţii atente asupra modalităţilor de producere, analize de caz, discuţii cu autorităţile competente etc.

4.3.1. O importanţă majoră în analiza statistică o are studiul mediului în care se află entitatea, vizînd natura mediului, consistenţele infrastructurii, precum şi orice alt factor care ar putea influenţa activitatea entității şi favoriza infracțiunile informatice.

4.3.2. Frecvenţa infracțiunilor informatice se poate materializa sub următoarele forme cantitative şi/sau calitative:

1) frecvenţa de producere (zilnic, o dată la zece zile, o dată la o sută de zile, o dată la 3 ani etc.);

2) posibilitatea (permanent, frecvent, posibil, puţin posibil, aproape imposibil).

4.1.Determinarea consecinţelor prejudiciabile ale infracțiunilor informatice - este o etapă complexă de analiză și evaluare, avînd în vedere și necesitatea prognozării posibilelor consecințe atît directe, cît şi indirecte.

Determinarea consecinţelor trebuie realizată de o echipă de profesionişti (în securitate, tehnologie, finanţe, organizare etc.) care trebuie să analizeze fiecare faptă infracțională posibilă şi, în funcţie de intensitatea şi frecvenţa sa de producere, să stabilească:

 1) consecințele prejudiciabile directe:

– cheltuielile cauzate de înlăturarea consecințelor infracțiunii și de restabilire a stării de normalitate;

– pierderile financiare cauzate de infracțiune (valoarea mijloacelor financiare sustrase sau a informației degradate);

– cheltuielile cauzate de modernizarea sau readaptarea măsurilor şi mecanismelor de protecție;

– cheltuielile pentru operaţionalizarea managementului general, de securitate şi de normalizare a situaţiei de funcţionalitate a entității după producerea infracțiunii;

– cheltuielile pentru restabilirea integrării în mediu, reluării legăturilor cu furnizorii şi clienţii, precum şi pentru refacerea climatului de comunicare;

– penalităţile contractuale cauzate de nerespectarea termenelor de livrare sau de prestare a serviciilor.

2) consecințele indirecte:

– consecințele cauzate de percepţia negativă a imaginii entității (insecuritate generală şi/sau tehnologică).

5.1. Stabilirea soluţiilor pentru minimizarea riscului.

5.1.1. Deoarece riscul reprezintă o variabilă analitică, rezultată din conjuncţia a doi factori (ameninţări şi vulnerabilităţi), minimizarea riscului este un proces analitic și material complex, care nu presupune numai micşorarea maxim posibilă a valorii sale, ci şi identificarea celor mai eficiente metode şi soluţii de tratare raţională a riscului.

5.1.2. Identificarea unui risc trebuie să fie urmată de elaborarea unor scenarii/opţiuni, care să conţină activităţile care vor fi derulate în cazul infracțiunii (pentru reducerea efectelor negative datorate riscului). Pentru fiecare opţiune, se stabilesc care sunt avantajele şi dezavantajele acesteia, pentru a selecta varianta cea mai bună.

6.1. Evaluarea eficienţei implementării soluţiilor pentru minimizarea riscului.

În funcţie de tipul infracțiunii, nivelurile consecințelor prejudiciabile și ale riscurilor asociate, se stabilesc mecanisme de combatere a criminalității informatice.

Urmare evaluării eficienţei implementării soluţiilor pentru minimizarea riscului, se elaborează un document de politici - strategia - cu ulterioara aplicare în situații practice.

7.1. Determinarea raportului cost/nivel de combatere a infracțiunilor informatice - asigură repartizarea eficientă a resurselor orientate spre combaterea criminalității informatice, oferind răspunsurile la următoarele întrebări:

- Cum pot fi utilizate resursele pentru a obține rezultatul maximal?

- Cum pot fi reduse consecințele infracțiunilor informatice pentru societate?

- Care este volumul resurselor ce necesită a fi alocate pentru ameliorarea stării infracționale?

În funcţie de valoarea raportului cost/nivel în combaterea infracțiunilor, se ia decizia implementării soluţiilor sau reluării evaluării, pînă la obținerea unui raport acceptat.

Reluarea evaluării se poate produce de la oricare etapă, în funcţie de acceptarea sau neacceptarea rezultatului obţinut în etapa respectivă.

**V. Obiectivele de dezvoltare**

5.1. Asigurarea investigării şi urmăririi penale eficiente a infracţiunilor informatice.

5.2. Perfecţionarea cadrului juridic:

5.2.1. Elaborarea și promovarea proiectelor de acte normative întru eliminarea lacunelor și barierelor cu caracter normativ;

5.2.2. Elaborarea unei strategii naționale privind securitatea informatică;

5.3. Dezvoltarea instituțională.

5.3.1 Dotarea și pregătirea personalului în funcție de nevoile fiecărei instituții, de situația operativă în domeniul criminalității informatice la nivel național și internațional;

5.3.2. Înființarea unui CERT național;

5.4. Delimitarea clară a responsabilităților și crearea de instrumente de colaborare interinstituțională:

5.4.1. Identificarea rolului și locului Procuraturii și a Poliției în cadrul activităților de combatere a infracțiunilor informatice;

5.4.2. Cooperarea interinstituțională trebuie înțeleasă ca un parteneriat, conform principiilor responsabilității și legalității și bazată pe încredere. Instituțiile trebuie să colaboreze și să creeze un sistem național în care atribuțiile acestora să nu fie în competiție și fără tendința de a-și asuma poziția de leader.

5.5. Coordonarea la nivel național a tuturor eforturilor și crearea unei strategii naționale privind securitatea cibernetică;

5.6. Dezvoltarea parteneriatului cu sectorul public și privat, bazate pe respectarea prevederilor legale și încredere reciprocă.