Aspectul organizaţional a securităţii informaţionale

Program național de securitate cibernetică a RM (2016-2020, HG nr811 din 29.11.15, MO nr.306-310 art.905)

Vine să implementeze prevederile:

- Acordului de Asociere RM-UE;
- Strategia securității cibernetice a UE;
- Convenția Consiliului Europei privind criminalitatea informatică;
- Recomandările Uniunii Internaționale a Telecomunicațiilor referitoare la asigurarea securității cibernetice a rețelelor și serviciilor de comunicații electronice.

Program național de securitate cibernetică a RM (2016-2020, HG nr811 din 29.11.15, MO nr.306-310 art.905)

Programul include 7 domenii de intervenție:

1) procesarea sigură, stocarea și accesarea datelor;
2) securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice;
3) capacităţi de prevenire şi reacţie de urgenţă (CERT);
4) prevenirea şi combaterea criminalităţii informatice;
5) consolidarea capacităţilor de apărare cibernetică;
6) educaţia şi informarea;
7) cooperarea şi interacţiunea internaţională.

Program național de securitate cibernetică a RM (2016-2020, HG nr811 din 29.11.15, MO nr.306-310 art.905)

Acțiunile din cadrul domeniilor de intervenție sunt orientate spre implementarea a patru componente-cheie:

1) introducerea de cerințe minime obligatorii de securitate cibernetică și standarde naționale de securitate cibernetică privind procesarea, stocarea, transmiterea, păstrarea și accesarea sigură a datelor;
2) certificarea și autorizarea specialiștilor și sistemelor informaționale, conform standardelor aprobate;
3) efectuarea periodică a auditului de securitate cibernetică a sistemelor informaționale și rețelelor de comunicații electronice în cadrul autorităților publice și altor entități deținătoare de sisteme informaționale de importanță vitală pentru societate;
4) introducerea de prescripții și sancțiuni pentru nerespectarea cerințelor minime de securitate și a standardelor naționale în domeniu.

Program național de securitate cibernetică a RM (2016-2020, HG nr811 din 29.11.15, MO nr.306-310 art.905)

Realizarea și implementarea Programului se va face prin respectarea obligatorie al principiului neutralității tehnologice și principiile europene de securitate cibernetică: protecţia drepturilor fundamentale, libertăţii de exprimare, datelor personale şi confidenţialităţii, accesul pentru toţi la informații veridice și protejate, rezilienţa cibernetică a sistemelor, responsabilitatea comună și personalizată de executare a activităților de asigurare a securităţii cibernetice.

Concepţia securităţii informaţionale a Republicii Moldova

Adoptarea Concepţiei este determinată de:

- necesitatea protecţiei intereselor persoanelor, societăţii, statului în spaţiul informaţional;
- de gravitatea şi multitudinea ameninţărilor la adresa securităţii informaţionale în societatea modernă;
- de necesitatea menţinerii unui echilibru între interesele persoanelor, societăţii şi statului pentru asigurarea securităţii informaţionale.

Concepţia securităţii informaţionale a Republicii Moldova

Este sistem integrat de opinii referitoare la scopurile, sarcinile, principiile şi direcţiile de bază ale activităţii de asigurare a nivelului necesar de securitate informaţională şi de protecţie a informaţiei în Republica Moldova.

Concepţia securităţii informaţionale a Republicii Moldova

- securitate informaţională– stare de protecţie a persoanei, societăţii şi a statului, care determină capacitatea de rezistenţă la ameninţările împotriva confidenţialităţii, integrităţii şi disponibilităţii în spaţiul informaţional;

- securitate informaţională a Republicii Moldova – stare de protecţie a persoanei, societăţii şi a statului, a drepturilor şi intereselor acestora în spaţiul informaţional, stipulate de Constituţie şi alte legi ale Republicii Moldova, precum şi a drepturilor şi intereselor ce ţin de căutarea, crearea, recepţionarea, expedierea, distribuirea, prelucrarea, stocarea, utilizarea şi protecţia informaţiei în spaţiul informaţional;

Concepţia securităţii informaţionale a Republicii Moldova

Documente de politici şi acte normative relevante:

1) Constituţia Republicii Moldova;
2) Decretul Preşedintelui Republicii Moldova nr.1743 din 19 martie 2004 privind edificarea societăţii informaţionale în Republica Moldova;
3) Legea nr.112-XVI din 22 mai 2008 pentru aprobarea Concepţiei securităţii naţionale a Republicii Moldova;
4) Legea nr. 619-XIII din 31 octombrie 1995 privind organele securităţii statului;
5) Legea nr. 1069-XIV din 22 iunie 2000 cu privire la informatică;
6) Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat;
7) Legea comunicaţiilor electronice nr.241-XVI din 15 noiembrie 2007;
8) Legea nr. 245-XVI din 27 noiembrie 2008 cu privire la secretul de stat;
9) Legea nr. 20-XVI din 3 februarie 2009 privind prevenirea şi combaterea criminalităţii informatice;
10) Legea nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal;

….

27) alte acte legislative şi normative în vigoare

Concepţia securităţii informaţionale a Republicii Moldova

- Una dintre **direcţiile** principale ale politicii de stat în domeniul asigurării SI este **asigurarea juridică**, în cadrul căreia se elaborează şi se perfecţionează legislaţia ce reglementează relaţiile în domeniul informaţional.

Determinarea statutului juridic al tuturor subiecţilor din spaţiul informaţional, inclusiv al deţinătorilor de informaţie şi utilizatorilor de resurse, sisteme informaţionale şi reţele de comunicaţii electronice, şi responsabilităţii lor pentru nerespectarea legislaţiei Republicii Moldova;

Crearea sistemului de colectare şi analiză a datelor despre sursele de ameninţare la securitatea informaţională şi consecinţele apariţiei acestora, ţinînd cont de orice tipuri şi categorii de informaţii;

Concepţia securităţii informaţionale a Republicii Moldova

Elaborarea legislaţiei care să stipuleze modul de organizare a activităţilor de investigare şi examinare în instanţele de judecată a faptelor ilegale în spaţiul informaţional, precum şi modul de lichidare a consecinţelor acestor acţiuni ilicite;

Elaborarea componentelor delictelor, ţinînd cont de specificul răspunderii penale, civile, contravenţionale şi disciplinare, includerea normelor de drept respective în codurile penal, civil, contravenţional, al muncii şi în alte acte legislative;

Perfecţionarea sistemului de pregătire a cadrelor.

Concepţia securităţii informaţionale a Republicii Moldova

Securitatea informaţională, reprezentînd o componentă inseparabilă de o importanţă maximă a securităţii naţionale, este asigurată de către Parlament, Preşedintele Republicii Moldova, Guvern, Consiliul Suprem de Securitate, Serviciul de Informaţii şi Securitate, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, **Ministerul Afacerilor Interne**, Ministerul Apărării, Procuratură şi Ministerul Educaţiei.

Concepţia securităţii informaţionale a Republicii Moldova

Ministerul Afacerilor Interne, în limitele competenţei sale:

1) realizează măsuri speciale de investigaţii, înfăptuieşte acţiuni de urmărire penală şi de expertiză judiciară în vederea prevenirii şi combaterii infracţiunilor informatice;

2) efectuează măsuri de protecţie civilă şi securitate antiincendiară a resurselor, sistemelor informaţionale şi reţelelor de comunicaţii electronice.

Sursele de ameninţări la securitatea informaţională

Principalele surse **externe** ale ameninţărilor sînt:

1) criminalitatea informatică transnaţională, activitatea organizaţiilor criminale internaţionale, a unor grupuri sau persoane, orientate spre obţinerea accesului nesancţionat la resursele de reţea şi informaţie;
2) activitatea organizaţiilor teroriste şi extremiste internaţionale, interesul acestora faţă de posedarea şi utilizarea armei informaţionale;
3) activitatea structurilor politice, economice, militare, de spionaj şi a serviciilor speciale străine, orientată spre efectuarea controlului global şi obţinerea neautorizată a informaţiei;
4) avansarea tehnologică a structurilor mondiale, înteţirea concurenţei mondiale pentru deţinerea celor mai importante tehnologii şi resurse;
5) elaborarea de către un şir de state a concepţiei de război informaţional.

Sursele de ameninţări la securitatea informaţională

Principalele surse interne ale ameninţărilor sînt:

1) imperfecţiunea cadrului normativ privind organizarea şi funcţionarea sistemului complex unic de protecţie a informaţiei în RM, inclusiv a subsistemelor de protecţie tehnică şi criptografică a informaţiei;
2) activitatea ilegală a unor grupuri sau persoane, orientată spre obţinerea neautorizată a accesului la resursele informaţionale, la tehnologii sau efectuarea controlului asupra funcţionării resurselor, tehnologiei informaţiei, sistemelor informaţionale şi reţelelor de comunicaţii electronice;
3) imperfecţiunea legislaţiei referitoare la prevenirea şi combaterea criminalităţii informatice;

Sursele de ameninţări la securitatea informaţională

Principalele surse interne ale ameninţărilor sînt:

4) coordonarea insuficientă a activităţii, delimitarea neclară a atribuţiilor autorităţilor administraţiei publice ce ţin de elaborarea şi realizarea politicii de stat în vederea asigurării securităţii informaţionale a Republicii Moldova;
5) utilizarea silită a mijloacelor tehnice şi de program importate pentru crearea resurselor, tehnologiei informaţiei, sistemelor informaţionale şi reţelelor de comunicaţii electronice, cauzată de dezvoltarea întîrziată a industriei autohtone;
6) nivelul redus de informatizare a autorităţilor administraţiei publice, a domeniului financiar de creditare, a industriei, agriculturii, educaţiei, sănătăţii, de deservire a cetăţenilor, precum şi de instruire a populaţiei pentru lucrul cu sistemul informaţional;
7) alocarea insuficientă din bugetul de stat a mijloacelor financiare pentru activităţile ce ţin de securitatea informaţională în Republica Moldova.

Cerințele minime obligatorii de securitate cibernetică

- Vor fi implementate în cadrul instituțiilor administrației publice centrale din Republica Moldova și vor contribui la sporirea gradului de securitate şi încredere în spaţiul digital.

- Conform domeniului de aplicare, cerințele minime obligatorii de securitate cibernetică vor fi divizate în două categorii:

  - cerințele de nivelul 1, care se referă la utilizarea tehnologiilor informaționale în activitatea instituțiilor

  - cerințele de nivelul 2, de securitate cibernetică avansată, destinate instituțiilor care prestează servicii bazate pe tehnologiile informaționale și comunicații.

- Proiectul conține standarde de securitate pentru ambele niveluri, inclusiv privind securitatea fizică și cea operațională, schimbul de date.

- Totodată, **documentul delimitează responsabilitățile autorităților publice** în domeniul reglementării procedurilor interne ce vor asigura gradul necesar de securitate cibernetică.

- Astfel, instituțiile publice vor fi responsabile pentru efectuarea auditului intern de securitate cibernetică, instruirea personalului, elaborarea ghidului de utilizare a poștei electronice și alte activități ce vor contribui la procesarea și accesarea în siguranță a datelor.

Cerințele minime obligatorii de securitate cibernetică

Cerințele minime de securitate cibernetică include toate politicile, procedurile, planurile, procesele, practicile, rolurile, responsabilitățile, resursele și structurile care sunt folosite pentru a proteja și păstra intactă informația.

Cerințele de nivelul 1

- Controlul accesului
- Securitatea fizică
- Securitatea operațională

Cerințele de nivelul 2

- Controlul accesului
- Securitatea fizică
- Securitatea operațională