Cursul universitar
Gestiunea securității informatice

Lidia Popov, dr., lect. univ.

Aspecte juridice privind protecția și securitatea informației

Plan

1. **Noțiuni generale ale aspectului legislativ de protecție a informației**
2. **Infracțiuni informatice**
   - 2.1. Accesul ilegal la informația computerizată
   - 2.2. Operații ilegale cu mijloace tehnice sau produse de program
   - 2.3. Interceptarea ilegală a unei transmisii de date informatice
   - 2.4. Alterarea integrității datelor informatice
   - 2.5. Perturbarea funcționării sistemului informatic
   - 2.6. Operații frauduloase cu parole, coduri de acces sau date similare
   - 2.7. Falsul informatic și frauda informatică
   - 2.8. Încălcarea regulilor de securitate a sistemului informatic
   - 2.9. Accesul neautorizat la rețelele de calculatoare
3. **Secretul de stat și secretul comercial**
   - 3.1. Secretul de stat
   - 3.2. Secretul comercial sau bancar
4. **Acte legislative conexe securității informaționale**
   - 4.1. Diverse legi privind SI
5. **Concepția securității informaționale a Republicii Moldova**
6. **Concluzii**

Noțiuni generale ale aspectului legislativ de protecție a informației

Aspectul legislativ, împreună cu alte aspecte, prezintă o importanță majoră în procesul de asigurare a securității informației.

Majoritatea oamenilor nu comit infracțiuni ce țin de securitatea informației, nu din cauza că, din punct de vedere tehnic, ele nu sunt posibile, ci deoarece aceste acțiuni contravin bunului-simț, ele sunt condamnate de societate sau chiar pedepsite.

La nivel legislativ de asigurare a securității informației, evidențiem două grupe de măsuri:

Măsuri ca scop restrictiv, adică măsuri care vizează crearea și menținerea în societate a unei atitudini (inclusiv cu utilizarea sancțiunilor) față de infracțiunile din domeniul securității informațiilor și autorii acestora;

Măsuri cu scop creativ, adică de ghidare și coordonare, care îmbunătățesc educația societății în domeniul securității informațiilor și care contribuie la dezvoltarea și distribuirea instrumentelor și mijloacelor de asigurare a securității informației.

Ambele grupuri de măsuri, în practică, sunt la fel de importante, însă este necesar de subliniat aspectul respectării conștiente a normelor și reglementărilor de securitate a informațiilor, ceea ce este destul de important pentru toți participanții la procesul informațional, deoarece ar fi incorect să credem că ne putem baza doar pe protecția organelor de aplicare a legii.

Pentru cei a căror datorie este de a pedepsi infractorii, la fel, este importantă cunoașterea și respectarea acestor norme și reglementări, deoarece asigurarea concludenții în timpul anchetei și a procesului de instanță, referitor la criminalitatea informatică, ***este imposibilă fără o pregătire specială***.

Constituția Republicii Moldova (CRM)

Legea Supremă a RM este Constituția RM, adoptată la 29.07.1994. Anume prin Constituție, în conformitate cu art. 34, avem ***Dreptul la informație***. Ce este stipulat în acest articol?

Articolul 34. ***Dreptul la informație***

(1) Dreptul persoanei de a avea acces la orice informație de interes public nu poate fi îngrădit.

(2) Autoritățile publice, potrivit competențelor ce le revin, sunt obligate să asigure informarea corectă a cetățenilor asupra trebuirilor publice și asupra problemelor de interes personal.

(3) Dreptul la informație nu trebuie să prejudicieze măsurile de protecție a cetățenilor sau siguranța națională.

Articolul 30 al Constituției RM garantează ***Secretul corespondenței***:

(1) Statul asigură secretul scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice și al celorlalte mijloace legale de comunicare.

(2) De la prevederile alineatului 1 se poate deroga (abate) prin lege în cazurile în care această derogare este necesară în interesele securității naționale, bunăstării economice a țării, ordinii publice și în scopul prevenirii infracțiunilor.

Actul legislativ, care cuprinde norme de drept ce stabilesc principiile și dispozițiile generale și speciale ale dreptului penal, determină faptele ce constituie infracțiuni și prevede pedepsele ce se aplică infractorilor, este ***Codul penal al RM***.

Codul penal se aplică în conformitate cu prevederile CRM și ale actelor internaționale la care RM este parte componentă.

Articolul 180 al Codului penal. ***Încălcarea intenționată privind accesul la informație***, prevede:

Încălcarea intenționată de către o persoană cu funcție de răspundere a procedurii legale de asigurare și de realizare a dreptului de acces la informație;

Încălcarea ce cauzează daune în proporții considerabile drepturilor și intereselor ocrotite de lege ale persoanei care a solicitat informații referitoare la ocrotirea sănătății populației, la securitatea publică, la protecția mediului, se pedepsește cu amendă de la 150 la 300 de unități convenționale cu (sau fără) privarea de dreptul de a ocupa anumite funcții sau de a exercita o anumită activitate pe un termen de până la 3 ani.

Infracțiuni informatice

Articolul 259.

Accesul ilegal la informația computerizată

Accesul ilegal la informația computerizată, de pe suporturile materiale de informație, din sistemul sau rețeaua informatică, al unei persoane, care nu este autorizată în temeiul legii sau al unui contract, ***depășește limitele autorizării*** ori nu are permisiunea persoanei competente să folosească, să administreze sau sa controleze un sistem informatic ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic.

În cazul în care este însoțit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informației, de dereglarea funcționării calculatoarelor, a sistemului sau a rețelei informatice și dacă a provocat daune în proporții mari, ***se pedepsește cu amendă*** în mărime de la 200 la 500 de unități convenționale sau orice alte pedepse.

Articolul 260. ***Operații ilegale cu mijloace tehnice sau produse de program***

Producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau produselor-program:

Producerea, importul, comercializarea sau punerea la dispoziție, sub orice altă formă, în mod ilegal, a mijloacelor tehnice sau produselor-program concepute sau adaptate, în scopul săvârșirii uneia dintre infracțiunile prevăzute la art. 237, 259, 260^{1}-260^{3}, 260^{5}, 260^{6}, se pedepsește cu amendă în mărime de la 500 la 1000 de unități convenționale sau cu orice altă pedeapsă conform legii inclusiv și cu privarea de dreptul de a exercita o anumită activitate sau chiar cu ***lichidarea întreprinderii***.

Articolul 260[1]. ***Interceptarea ilegală a unei transmisii de date informatice***

Interceptarea ilegală a unei transmisii de date informatice care nu sunt publice și care sunt destinate unui sistem informatic, provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic, se pedepsește cu amendă în mărime de la 500 la 1000 de unități convenționale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 3000 la 6000 de unități convenționale cu privarea de dreptul de a exercita, la fel, o anumită activitate sau cu ***lichidarea întreprinderii***.

Articolul 260^2 .
Alterarea integrității datelor informatice

Alterarea integrității datelor informatice ținute într-un sistem informatic:

Modificarea, ștergerea sau deteriorarea intenționată a datelor informatice ținute într-un sistem informatic ori restricționarea ilegală a accesului la aceste date, transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziție, sub orice formă, a datelor informatice cu acces limitat, ***dacă aceste acțiuni au cauzat daune în proporții mari***, se pedepsesc cu amendă în mărime de la 500 la 1000 de unități convenționale sau cu închisoare de la 2 la 5 ani.

Articolul 260^3. ***Perturbarea funcționării sistemului informatic***

(1) ***Perturbarea funcționării unui sistem informatic*** prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la aceste date, ***dacă aceste acțiuni au cauzat daune în proporții mari***, se pedepsește cu amendă în mărime de la 700 la 1000 de unități convenționale sau cu munca neremunerată în folosul comunității de la 150 la 200 de ore, sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 3000 la 6000 de unități convenționale cu privarea de dreptul de a exercita, la fel, o anumită activitate sau cu ***lichidarea întreprinderii***.

Articolul 260^3. ***Perturbarea funcționării sistemului informatic***

(2) ***Aceeași acțiune*:**

a) săvârșită din interes material;

b) săvârșită de două sau mai multe persoane;

c) săvârșită de un grup criminal organizat sau de o organizație criminală;

care a cauzat daune în proporții deosebit de mari, se pedepsește cu amendă în mărime de la 700 la 1000 de unit. conv. sau închisoare de la 3 la 7 ani, cu amendă aplicată persoanei juridice, în mărime de la 3000 la 6000 de un. conv. sau cu lichidarea întreprinderii.

Articolul 260^4 . ***Operații frauduloase cu parole, coduri de acces sau date similare***

Producerea, importul, comercializarea sau punerea ilegală la dispoziție a parolelor, codurilor de acces sau a datelor similare:

(1) Producerea, importul, comercializarea sau punerea sub orice altă formă, în mod ilegal, a unei parole, a unui cod de acces sau a unor date similare, care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia dintre infracțiunile prevăzute de următoarele articole: 237, 259, 260^1-260^3, 260^5 și 260^6, ***dacă aceste acțiuni au cauzat daune în proporții mari***, la fel, se pedepsesc cu amendă în mărime de la 500 la 1000 de unități convenționale sau cu munca neremunerată în folosul comunității de la 150 la 200 de ore, sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 1000 la 3000 de unități convenționale cu privarea de dreptul de a exercita o anumită activitate.

La fel, dacă ne referim la:

1. Falsul informatic (art. **260^{5}**)
2. Frauda informatică (art. **260^{6}**)
3. Încălcarea regulilor de securitate a sistemului informatic (art. **261**)
4. Accesul neautorizat la rețele de calculatoare (art. **261^{1}**)

în cazul în care au fost cauzate daune în proporții mari se pedepsește conform legii.

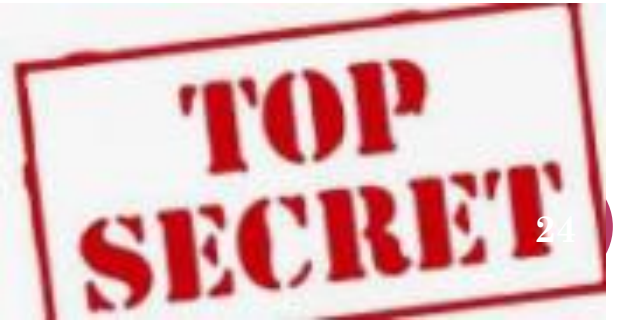
Secretul de stat și secretul comercial

Secretul de stat

Un loc special în legislație îl ocupă ***secretul de stat***, care reprezintă informații protejate de stat în domeniul apărării naționale, economiei, științei și tehnicii, relațiilor externe, securității statului, asigurării ordinii de drept și activității autorităților publice, a căror divulgare neautorizată sau pierdere este de natură să aducă atingere intereselor și/sau securității RM. Secretul de stat este reglementat de Legea nr. 245 din 27.11.2008 cu privire la secretul de stat (http://lex.justice.md/md/330847)

Secretul de stat

Pierderea documentelor ce conțin secrete de stat, precum și a obiectelor datele despre care constituie secret de stat, de către o persoană căreia aceste documente sau obiecte i-au fost încredințate, dacă pierderea a fost un rezultat al încălcării regulilor stabilite de păstrare a documentelor sau obiectelor menționate și a cauzat urmări grave, se pedepsesc cu amendă în mărime de la 150 la 400 de unități convenționale sau cu închisoare de până la 3 ani, în ambele cazuri cu privarea de dreptul de a ocupa anumite funcții sau de a exercita o anumită activitate pe un termen de 5 ani.

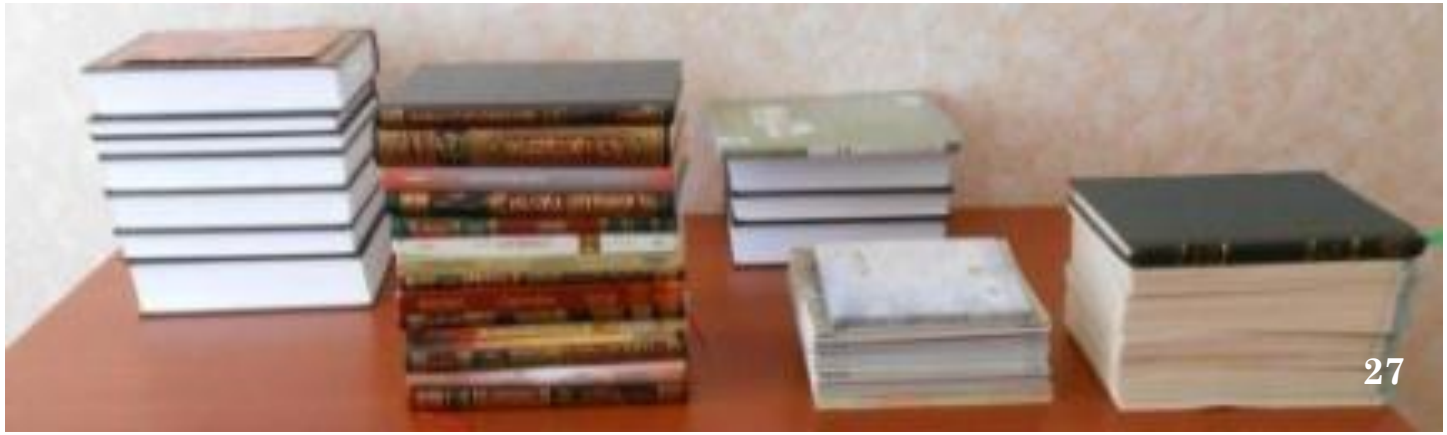


Secretul comercial sau bancar

Informațiile, ce nu constituie secret de stat, și care țin de producție, tehnologie, administrare, de activitatea financiară și de altă activitate a agentului economic, a căror divulgare (transmitere, scurgere) poate să aducă atingere intereselor lui poartă denumirea de ***secret comercial sau secret bancar***.

Acte legislative conexe securității informaționale

Legi, adoptate de către Parlamentul RM, care au un impact asupra procesului de asigurare a securității informaționale.



Legea cu privire la informatizare și la resursele informaționale de stat (http://lex.justice.md/md/313189/)

Legea respectivă stabilește regulile de bază și condițiile de activitate în domeniul creării și dezvoltării infrastructurii informaționale naționale ca mediu de funcționare al societății informaționale din RM, reglementează raporturile juridice, care apar în procesul de creare, formare și utilizare a resurselor informaționale automatizate de stat, a tehnologiilor, sistemelor și rețelelor informaționale.

Sub incidența acestei legi, nu cad raporturile care apar la crearea și funcționarea mijloacelor de informare în masă, resurselor informaționale nestatale, la prelucrarea informației nedocumentate.

Legea comunicațiilor electronice

(http://lex.justice.md/md/327198/)

Această lege stabilește:

- ✓ principalele reguli și condiții de activitate în domeniul comunicațiilor electronice din RM;
- ✓ cadrul general al politicii și strategiei de dezvoltare a domeniului, prin definirea atribuțiilor autorității centrale de specialitate;
- ✓ cadrul general de reglementare a activităților privind rețelele și serviciile de comunicații electronice, prin definirea atribuțiilor și obiectivelor autorității de reglementare;
- ✓ drepturile și obligațiile statului;
- ✓ drepturile persoanelor fizice și juridice în procesul creării, gestionării și utilizării rețelelor de comunicații electronice, în scopul asigurării utilizatorilor cu servicii de comunicații electronice de calitate, moderne și utile, la prețuri rezonabile, precum și al asigurării accesului liber la serviciile publice de comunicații electronice.

Legea privind protecția datelor cu caracter personal (http://lex.justice.md/md/340495/)

Scopul acestei legi constă în asigurarea protecției drepturilor și libertăților fundamentale ale persoanei fizice în ceea ce privește prelucrarea datelor cu caracter personal, în special, a dreptului la inviolabilitatea vieții intime, familiale și private.

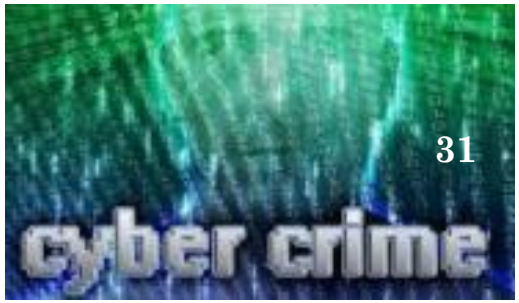
Prezenta lege reglementează relațiile juridice care apar în procesul de prelucrare a datelor cu caracter personal ce fac parte dintr-un sistem de evidență sau care sunt destinate să fie incluse într-un asemenea sistem, efectuată, în totalitate sau în parte, prin mijloace automatizate, precum și prin alte mijloace decât cele automatizate.

Legea privind prevenirea și combaterea criminalității informatice

(http://lex.justice.md/md/333508/)

Această lege reglementează raporturile juridice privind:

- ✓ Prevenirea și combaterea infracțiunilor informatice;
- ✓ Cadrul de asistență mutuală în prevenirea și combaterea criminalității informatice;
- ✓ Colaborarea autorităților administrației publice cu organizații neguvernamentale și alți reprezentanți ai societății civile în activitatea de prevenire și de combatere a criminalității informatice;
- ✓ Cooperarea cu alte state, cu organizații internaționale și regionale având competențe în domeniu.



Legea privind accesul la informație
(http://lex.justice.md/md/311759/)

Această lege reglementează :

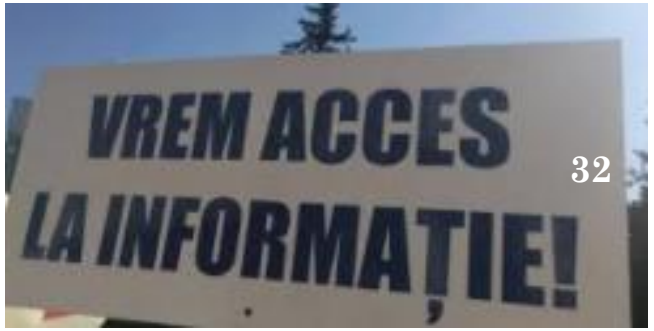
a) Raporturile dintre furnizorul de informații și persoana fizică sau juridică în procesul de asigurare și realizare a dreptului constituțional de acces la informație;

b) Principiile, condițiile, căile și modul de realizare a accesului la informațiile oficiale, aflate în posesia furnizorilor de informații;

c) Drepturile solicitanților informației;

d) Obligațiile furnizorilor de informații în procesul asigurării accesului la informațiile oficiale;

e) Modalitatea apărării dreptului de acces la informație.



Legea privind accesul la informație are drept scop:

a) Crearea cadrului normativ general al accesului la informațiile oficiale;
b) Eficientizarea procesului de informare a populației și a controlului efectuat de către cetățeni asupra activității autorităților publice și a instituțiilor publice;
c) Stimularea formării opiniilor și participării active a populației la procesul de luare a deciziilor în spirit democratic.

Legea privind semnătura electronică și documentul electronic

(http://lex.justice.md/md/353612/)

Scopul legii și domeniul de aplicare:

1. Prezenta lege ***stabilește*** regimul juridic al semnăturii electronice și al documentului electronic, inclusiv cerințele principale față de valabilitatea acestora și cerințele principale față de serviciile de certificare;
2. Prezenta lege nu limitează modul de utilizare a documentelor;
3. Recunoașterea semnăturii electronice și a documentului electronic, în afara RM, este reglementată de tratatele internaționale, la care RM este parte. În cazul în care acestea, stabilesc alte norme decât cele prevăzute de prezenta lege, se aplică normele tratatelor internaționale.

Semnătura electronică (SE)

SE reprezintă date în forma electronică care sunt atașate sau logic asociate cu alte date în formă electronică și care servesc ca metodă de identificare.

Altfel spus, o SE este un bloc de date (cifre binare) ce se ataşează unui mesaj sau document pentru a întări încrederea unei alte persoane sau entităţi, legându-le de un anumit emiţător. Legătura este realizată astfel încât **SE** poate fi verificată de receptor sau de o terţă persoană şi nu se poate spune că a fost uitată. Dacă doar o cifră binară nu corespunde, **SE** va fi respinsă în procesul de validare.

Anume SE stabileşte autenticitatea sursei mesajului !

Semnătura electronică (SE)

În cazul în care o persoană nu-şi divulgă cheia personală privată nimeni nu poate să-i imite **SE**. O **SE**, privat nu înseamnă şi recunoaşterea dreptului de proprietate asupra textului transmis, ci ea atestă faptul că persoana semnatară a avut acces la el şi la semnat.

Atunci când semnarea este cuplată cu crearea documentului, **SE** poate oferi o probă evidentă a originii documentului. Această categorie include fotografii-le făcute cu camere digitale bazate pe chei private, caz în care proba este de necontestat. Procedeul este folosit când se doreşte realizarea protecţiei împotriva manipulării imaginilor cu calculatorul.

În acelaşi mod pot lucra şi camerele video sau alţi senzori care-şi pot semna ieşirea pentru a-i certifica originea. Deşi **SE** este implementată prin sistemul criptografiei cu chei publice, în cazul acesteia componenta privată este folosită pentru semnarea mesajelor în timp ce componenta publică este folosită pentru a verifica **SE**.

Utilizarea semnăturilor electronice

SE ajută la identificarea şi autentificarea persoanelor, organizaţiilor şi a calculatoarelor prin Internet. Sunt utilizate pentru a verifica integritatea datelor după terminarea tranzitului. **SE** sunt asemănătoare semnăturilor de mână, care sunt utilizate zilnic pentru a identifica un individ într-o manieră legală.

De exemplu, în momentul în care o persoană se decide asupra termenilor unui contract, includerea unei semnături de mână indică faptul că acea persoană este de acord cu termenii acelui contract. În continuare, persoana respectivă nu ar mai trebui să nege faptul că a semnat acel document sau că termenii acelui contract nu corespund dorinţelor lui, decât în caz de falsificare.

În mod asemănător, **SE** pot identifica persoana care a semnat o tranzacţie sau un mesaj, dar spre deosebire de semnăturile de mână, o **SE** poate ajuta în verificarea faptului că un document sau o tranzacţie nu a fost modificată faţă de starea originală din momentul semnării.

Utilizarea semnăturilor electronice

Deosebirea principală a SE faţă de semnătura de mână este aceea că, în cazul în care sistemul a fost implementat corespunzător, SE nu se poate falsifica. În condiţii ideale, acest lucru poate însemna faptul că un mesaj semnat digital trebuie să aparţină persoanei a cărei semnătură apare în mesaj. Incapacitatea de a nega faptul că un mesaj sau o tranzacţie a fost executată (semnată) se numeşte ***nerepudiere***.

SE oferă trei servicii de securitate de bază:

- ✓ Autentificare;
- ✓ Integritate;
- ✓ Nerepudiere.

Scopul SE constă în identificarea în mod pozitiv expeditorul unui mesaj şi de a asigura faptul că datele nu au fost modificate.

Riscuri de securitate

Înţelegerea ***riscurilor asociate*** cu utilizarea semnăturilor electronice presupune înţelegerea limitărilor acestei tehnologii. O semnătură electronică, când nu este legată de numele utilizatorului printr-un certificat digital, nu are nici o semnificaţie. Distribuirea securizată a semnăturii electronice este singura garanţie a securităţii ei.

În cazul în care este nevoie de o distribuire la scară a cheilor publice pentru verificarea semnăturilor electronice, trebuie creată BD la care persoanele interesate să aibă acces de citire, în timp ce scrierea trebuie restricţionată cu cele mai puternice tehnologii.

Poate cel mai mare risc al semnăturilor electronice este acordarea unei prea mari încrederi acestei tehnologii. Semnăturile de mână pot fi falsificate sau fotocopiate într-un nou document, dar acest lucru nu ar trebui să fie valabil într-un sistem de semnături electronice implementat în mod corespunzător. O semnătură de mână poate să ofere o certitudine până la ruperea modelului de încredere. Problema cu semnăturile electronice este aceea că nu se ştie încă unde şi când nu se mai poate vorbi de încrederea acordată sistemului.

Concepția securității informaționale a Republicii Moldova

Concepția securității informaționale (CSI)

CSI a RM reprezintă un sistem integrat de opinii referitoare la scopurile, sarcinile, principiile și direcțiile de bază ale activității de asigurare a nivelului necesar de SI și de protecție a informației în RM, care, la rândul lor, sunt considerate părți componente ale sistemului național de securitate. **CSI a RM** a fost votată de Parlamentul RM la 21.12.2017 și a fost publicată în Monitorul Oficial nr. 48-57 la 16.02.2018.

CSI a RM va servi drept bază pentru elaborarea legislației RM, inclusiv a politicii de stat, în domeniul asigurării SI, pentru asigurarea coordonării și sporirii nivelului de eficiență a activității autorităților administrației publice și a altor organizații din sectorul public și privat. Toate acestea sunt orientate pentru elaborarea programelor speciale de asigurare a SI, precum și pentru crearea unui sistem unic de protecție a informației ce întrunește măsurile legale, organizatorice, tehnice, tehnologice și fizice de protecție.

Concepția securității informaționale (CSI)

Concepția are drept scopuri principale crearea sistemului de asigurare a SI în RM, sporirea nivelului de SI a statului în ansamblu și perfecționarea, în continuare, a cadrului legislativ privind SI, fundamentată de prevederile Constituției RM, Concepției securității naționale și Strategiei de securitate națională.

Concepția determină scopurile, principiile și sarcinile de activitate a organelor administrației publice în asigurarea SI, componentele de bază ale SI, amenințările principale și metodele de prevenire a acestora.

Concluzii

Cadrul juridic prezintă o importanță primordială în asigurarea unui nivel înalt de ***protecție a informației***, iar pentru un specialist din domeniul IT cunoașterea măsurilor legislative respective este, la fel, de importantă ca și cunoașterea și aplicarea celorlalte măsuri de asigurare a ***securității informaționale.***

Mulțumim pentru atenție!