Larisa CUJBA, Cristina VOINU,
U.C.C.M., Republica Moldova

REGLEMENTAREA JURIDICĂ A SECURITĂȚII SISTEMELOR INFORMATICE

The legislation of Republica Moldova is not very employed in informational security.

Trecerea la economia de piață a condiționat transformarea informației într-una din cele mai importante resurse ale persoanelor, societății, statului, care îşi efectuează activitatea îin baza operațiunilor de colectare, înregistrare, procesare, stocare şi transmitere a informației. Pretutindeni, organele de stat, agenții economici şi persoanele fizice elaborează şi pun în funcțiune sisteme informatice. În baza tehnicii de calcul şi mijloacelor de telecomunicații moderne, se funcționează sisteme automatizate de plăți intra- şi interbancare. Sunt răspândite sistemele gestionate de persoane fizice şi juridice ce permit conectarea şi accesul la sisteme informatice internaționale.

Într-un stat constituțional, oricare tip de activitate trebuie să fie reglementat. Din păcate, asigurarea legislativă a relațiilor informaționale, în Republica Moldova, lipseşte, iar acest domeniu al legislației este „terra incognita" pentru organele legislative din țară.

Constituirea societății informaționale contemporane, în Republica Moldova, necesită rezolvarea unui complex de sarcini în vederea formării mediului informațional, care ar asigura dezvoltarea eficace a sistemelor informatice şi a rețelelor de transfer al datelor, formarea resurselor, elaborarea produselor, prestarea serviciilor de categorii informaționale, pregatirea specialiştilor în acest domeniu etc.

La conferința de la Madrid cu privire la securitatea sistemelor informaționale, directorul general al uneia din corporații a afirmat "tâlhăriile înarmate, care au loc în lume, nu constituie nimic, în comparație cu jafurile "electronice", cu ajutorul cărora miliarde de dolari se virează de pe un cont pe altul şi dintr-o tara în alta …". Doar băncile SUA pierd zeci de miliarde de dolari pe an, fapt care se poate compara cu privilegiile economice de pe urma aplicării computerelor. Totodată, deja jumătate din crimele lumii afacerilor sunt legate de utilizarea tehnologiilor informatice.

Printre alte consecințe negative ale informatizării cauzate de dereglarea securității informaționale, se înscriu terorismul şi huliganismul computerial. Fanaticul telephonic", "Hacherul", "Cracherul" sunt expresiile lexicului actual. Daca hacherii pătrund în memoria sistemelor computerizate pentru satisfacerea ambițiilor proprii, apoi cracherii mai şi "storc" băncile informaționale. Asemenea "specialişti" sunt periculoşi, în mod catastrofal, pentru sistemele computerizate.

Cadrul juridic este chemat să realizeze dreptul de proprietar asupra informației cu diferențierea proprietății organizațiilor de stat, a organelor administrative; structurilor comerciale, datelor personale ale cetățenilor.

La finele anilor 70 ai secolului XX, comunitatea internațională a formulat următoarele principii, ce au fost luate ca baza la crearea cadrului juridic al securității informaționale in mai multe țări:

1.Stabilirea limitelor amestecului in viata personala a cetățenilor prin intermediul sistemelor informatice;

2.Implementarea mecanismelor administrative de protecție a cetățenilor contra unor astfel de amestecuri.

Prin intermediul normelor de drept în domeniul securității informaționale, trebuie să fie realizate următoarele sarcini:

1) referirea informației drept deschisă sau închisă;
2) definirea drepturilor de acces la informații;
3) definirea drepturilor persoanelor de răspundere în vederea atribuirii şi modificării paragrafelor anumitor informații;
4) modalitățile şi procedurile de acces la informații;
5) modul de control, documentare şi analiză a acțiunilor personalului;
6) responsabilitățile pentru neîndeplinirea cerințelor definite;
7) demonstrarea vinovăției infractorilor;
8) pedepsirea vinovaților.

Într-un stat constituțional, trebuie să fie definite politica de stat în domeniul securității informaționale, care conține definițiile a cel puțin următoarelor principii:

1) limitarea accesului la informații se realizează numai în baza legislației;
2) responsabilitatea pentru păstrare, aplicarea şi anularea parafei se personifică;
3) accesul la informații, de asemenea, şi restricțiile de acces se aplică numai în conformitate cu

prevederile legislației;

Tezele politicii de stat în domeniul securității informaționale, sunt următoarele:

1) formarea bazei legislative, de reglementare a drepturilor, responsabilităților tuturor subiecților care acționează in sfera informațională;
2) realizarea controlului asupra creării şi utilizării mijloacelor de protecție a informației;
3) realizarea politicii protecționiste în vederea susținerii activității producătorilor autohtoni ai mijloacelor de informatizare şi mijloacelor de protecție a informației, precum şi luarea măsurilor în vederea prevenirii pătrunderii pe piața internă a produselor informatice necalitative;
4) crearea unui program unitar în domeniul securității informaționale, ce va împreuna eforturile organizațiilor de stat şi a structurilor comerciale în vederea creării unui sistem comun de protecție a informațiilor în țară.

Baza juridică a securității informaționale include *baza legislativă şi practica de drept*. **Baza legislativă** se prezintă, sub formă de mulțime de acte normative, predestinate să reglementeze modul de prelucrare şi utilizare a informațiilor şi a tehnologiilor informatice, să definească categoriile de acces, drepturile şi responsabilitățile persoanelor de răspundere în vederea stabilirii şi modificării dreptului de acces, modul de control, documentarea şi analiza activității sistemelor informatice şi să stabilească răspunderea pentru încălcarea acestor reguli.

De menționat că, în ultimul timp, s-au format mai multe direcții de reglementare juridică în domeniul elucidat, printre care de bază sunt următoarele:

1) protecția datelor personale;
2) lupta cu criminalitatea informațională;
3) protecția secretelor comerciale şi a secretelor de stat;
4) asigurarea securității sistemelor informatice ale sectoarelor potențial-periculoase;
5) asigurarea informației şi sistemelor informatice;
6) certificarea şi licențierea în domeniul asigurării şi controlului securității sistemelor informatice;
7) organizarea colaborării în domeniul securității informatice cu alte state.

Practica de drept – include activități privind depistarea, cercetarea şi demonstrarea justificată a crimelor informaționale comise. E cunoscut faptul că infracțiunile din domeniul activității informaționale sunt foarte dificile din punct de vedere al depistării, studiului lor şi lichidării consecințelor acestora, din cauza mai multor factori, printre care de bază sunt următorii:

1) complexitatea stabilirii aspectului obiectiv al comiterii infracțiunii;
2) mediul complex al sistemelor informatice;
3) numărul semnificativ de utilizatori, care dispun de posibilități direct sau indirect de a săvârşi infracțiuni cu variate consecințe ale lor;
4) complexitatea stabilirii aspectului subiectiv al infracțiunii cu evidențierea a două momente esențiale: personificarea faptului şi stabilirea caracterului infracțiunii intenționat sau neintenționat.

Concluzii

În baza celor expuse mai sus, este certă concluzia că sunt necesare urgent un şir de măsuri, in vederea creării bazei juridice, strict necesară pentru a reglementa relațiile mediului informațional al Republicii Moldova. În caz contrar, este posibilă pierderea controlului asupra proceselor de informatizare şi fluxurilor informaționale de importanță socială.