STUDIA UNIVERSITATIS
Revistă ştiinţifică a Universităţii de Stat din Moldova, 2009, nr.8(28)

STATUTUL JURIDIC AL INFORMAŢIEI ELECTRONICE ÎN DREPTUL PENAL COMPARAT

Flavius-Vasile ONOFREI

Catedra Drept Penal şi Criminologie

This scientific research is dedicated to the definition and analysis of the legal status of electronic information in accordance with comparative penal law. Especially, the criminal legislation of several states (the Ukraine, Republic of Belarus, the Russian Federation and Republic of Kazakhstan) is submitted to an investigation regarding cyber crimes and other offences, which are linked to the electronic information. The author has tried to classify those crimes in function of different criteria. Some scientific methods have been applied. Several conclusions are strongly recommended in order to be used in the legislation of Republic of Moldova.

Legislaţia penală a Ucrainei, Republicii Belarus, Federaţiei Ruse şi a Republicii Kazahstan în ceea ce priveşte protecţia informaţiei electronice a cunoscut transformări esenţiale îndată după adoptarea şi intrarea în vigoare a codurilor penale actuale, în urma reformelor legislative care au avut loc în anii 1996-2002.

Aşadar, cu adoptarea noului ***Cod penal al Ucrainei*****,** la 5 aprilie 2001, pentru prima dată în mod separat a fost introdus Titlu XVI dedicat infracţiunilor săvârşite în sfera utilizării a computerelor, sistemelor şi reţelelor informaţionale [1].

Astfel, legislaţia penală a Ucrainei asigură protecţia proceselor legale de culegere, prelucrare, stocare, păstrare, căutare şi de răspândire a informaţiei electronice.

Legitimitatea acestor procese este determinată, în primul rând, de iniţiativa şi consimţământul proprietarului acestei informaţii, de existenţa accesului liber la efectuarea proceselor sus-nominalizate, de respectarea prevederilor legislative referitoare la operaţiuni cu informaţie confidenţială şi la cerinţe înaintate faţă de exploatarea calculatoarelor, sistemelor şi reţelelor informaţionale.

Reprezentanţii doctrinei penale din Ucraina unanim au recunoscut accepţiunea, conform căreia noţiunile *„informaţie”* şi *„suport de informaţie”* nu sunt identice, deoarece informaţia este un obiect imaterial care, la rândul său, se conţine şi poate fi transmis în timp şi în spaţiu prin intermediul suporturilor materiale [2].

În această ordine de idei, M.V. Karcevski defineşte *informaţia electronică* ca anumite date, ştiri, cunoştinţe despre fenomenele obiective sau procese, ale căror integritate, confidenţialitate şi accesibilitate sunt asigurate prin intermediul tehnicii computaţionale care aparţine proprietarului concret şi care poate fi valorificată [3]. Totodată, autorul D.Azarov propune spre utilizare o definiţie a noţiunii „informaţie electronică”, fiind una clară şi simplă: „anumite ştiri despre procese şi fenomene obiective care sunt reprezentate într-o formă electronică” [4].

Totodată, autorul A.V. Zaghika subliniază avantajele informaţiei electronice prin simplitatea relativă în expedierea, transformarea şi multiplicarea acesteia, iar în cazul copierii acesteia ea îşi păstrează toate proprietăţile în sursa primară [5]. În plus, autorul atenţionează că numai informaţia electronică asigură accesul nelimitat şi simultan al mai multor persoane.

Analizând Titlu XVI din Codul penal al Ucrainei, observăm că acest compartiment cuprinde trei articole:

- Implicarea ilegală în procesul de lucru al calculatoarelor, al sistemelor şi al reţelelor computaţionale (art.361);
- Sustragerea, însuşirea, extorcarea informaţiei electronice sau obţinerea acesteia prin înşelăciune ori abuz de serviciu (art.362);
- Încălcarea regulilor de exploatare a sistemelor informaţionale (art.363).

Precizăm în acest sens că toate aceste articole cuprind atât componenţe simple (necalificate) ale acestor infracţiuni, cât şi cele calificate (alin.(2) art.361, alin.(2) art.362, alin.(2) art.363) sau deosebit de calificate (alin.(3) art.362 CP).

Aşadar, *art.361 al Ucrainei* prevede răspunderea penală pentru implicarea ilegală în procesul de lucru al calculatoarelor, al sistemelor sau al reţelelor computaţionale, care a condus la alterarea sau distrugerea informaţiei electronice sau a suporturilor acesteia; precum şi răspândirea programului virulent pentru calculatoare

prin utilizarea mijloacelor tehnice, destinate pentru pătrunderea ilegală în aceste maşini, sisteme sau reţele informaţionale care pot provoca alterarea sau distrugerea informaţiei electronice sau a suporturilor acesteia.

Obiectul juridic special al acestei infracţiuni îl constituie relaţiile sociale în sfera asigurării securităţii folosirii de mijloace materiale sau intelectuale a tehnicii de calculator [6].

Această infracţiune conţine atât *obiect material*, cât şi *obiect imaterial*. În special, în calitate de *obiect material* este recunoscut suportul material în care se conţine informaţia electronică, cum ar fi: maşină automatizată de calcul electronic (calculatorul), sistemul de calculatoare, reţeaua computaţională, dispozitive speciale ce îndeplinesc rolul suporturilor materiale ale informaţiei (obiecte fizice, acumulatoare de date în sistemele informaţionale etc.), mijloace tehnice şi de programare destinate pentru pătrunderea ilegală în sistemele automatizate. Totodată, informaţia electronică reprezintă *un obiect imaterial*, fiind destinată pentru utilizarea ei în calculatoare, care este stocată în calculator sau alte dispozitive tehnice, precum şi informaţia care se transmite prin intermediul reţelelor de telecomunicaţii, dar care poate fi prelucrată de calculator.

Latura obiectivă a acestei infracţiuni se caracterizează prin săvârşirea a două fapte alternative:

Prima variantă:

1. *Acţiunea* de implicare ilegală în procesul de lucru al calculatoarelor, al sistemelor sau al reţelelor computaţionale;
2. *Urmările prejudiciabile* sub formă de alterare sau distrugere a informaţiei electronice sau a suporturilor acesteia;
3. *Legătura cauzală* dintre fapta prejudiciabilă şi rezultatul produs.

A doua variantă constă în:

1. *Acţiunea* de răspândire a programului virulent pentru calculatoare;
2. *Mijlocul săvârşirii infracţiunii:* utilizarea mijloacelor tehnice, destinate pentru pătrunderea ilegală în aceste maşini, sisteme sau reţele informaţionale care pot provoca alterarea sau distrugerea informaţiei electronice sau a suporturilor acesteia.

În prima variantă este vorba despre componenţă materială, iar în a doua – despre componenţa formală.

Latura subiectivă a infracţiunii prevăzute în art.361 CP al Ucrainei se caracterizează prin vinovăţie sub formă de intenţie directă sau indirectă în cazul primei variante de infracţiuni, iar în cazul răspândirii programului virulent pentru calculatoare intenţia poate fi numai directă.

Subiectul acestei infracţiuni este persoana fizică responsabilă care a atins vârsta de 16 ani.

Totodată, componenţă calificată a acestei infracţiuni (alin.(2) art.361 CP al Ucrainei) prevede răspunderea penală pentru aceleaşi acţiuni:

- dacă ele au cauzat prejudiciul considerabil;
- dacă ele au fost săvârşite repetat;
- dacă ele au fost săvârşite prin înţelegere prealabilă de un grup de persoane.

Totodată, art.362 CP al Ucrainei stabileşte răspunderea penală pentru sustragerea, însuşirea, extorcarea informaţiei electronice sau obţinerea acesteia prin înşelăciune ori abuz de serviciu.

Obiectul juridic special al acestei infracţiuni îl constituie dreptul de proprietate asupra informaţiei electronice. Dreptul de proprietate asupra informaţiei este proclamat şi în art.38 al Legii Ucrainei privind informaţia din 02.10.1992 [7].

Obiectul imaterial al acestei infracţiuni îl constituie informaţia electronică.

Latura obiectivă a acestei infracţiuni poate fi exprimată în una din următoarele fapte:

- sustragerea informaţiei electronice;
- însuşirea informaţiei electronice;
- extorcarea informaţiei electronice;
- obţinerea informaţiei electronice prin înşelăciune;
- obţinerea informaţiei electronice prin abuz de serviciu.

Precizăm în acest sens că numai extorcarea informaţiei electronice este o componenţă formală, fiind consumată din momentul înaintării cererii privind transmiterea acestei informaţii, iar în celelalte cazuri putem vorbi numai despre componenţe materiale; în alţi termeni, fapta se consideră consumată din momentul intrării în posesiune asupra acestei informaţii.

Latura subiectivă a infracţiunii prevăzute la art.362 CP al Ucrainei se caracterizează prin vinovăţie sub formă de intenţie directă.

Subiectul acestei infracţiuni este persoana fizică responsabilă care a atins vârsta de 16 ani.

Componenţa calificată a acestei infracţiuni (alin.(2) art.362 CP al Ucrainei) prevede răspunderea penală pentru aceleaşi acţiuni:

- dacă ele au fost săvârşite repetat;
- dacă ele au fost săvârşite prin înţelegere prealabilă de un grup de persoane.

Totodată, alin.(3) art.362 CP al Ucrainei prevede o circumstanţă deosebit de gravă, cum ar fi cauzarea prejudiciului considerabil.

Însă, *art.363 CP al Ucrainei* prevede răspunderea penală pentru încălcarea regulilor de exploatare a calculatoarelor, a sistemelor computaţionale sau a reţelelor informaţionale săvârşită de persoana responsabilă pentru exploatarea lor, dacă cele săvârşite au condus la sustragerea, alterarea sau distrugerea informaţiei computerizate, a mijloacelor de protecţie a acesteia; sau copierea ilegală a informaţiei computerizate ori încălcarea esenţială a regimului de lucru al calculatoarelor, al sistemelor sau al reţelelor acestora.

Obiectul juridic special al acestei infracţiuni îl constituie regulile stabilite de exploatare a calculatoarelor, a sistemelor computaţionale sau a reţelelor informaţionale.

Latura obiectivă a acestei infracţiuni se caracterizează prin săvârşirea a trei fapte alternative:

Prima variantă:

1. *Acţiunea (inacţiunea)* exprimată în încălcarea regulilor de exploatare a calculatoarelor, a sistemelor computaţionale sau a reţelelor informaţionale;
2. *Urmările prejudiciabile* sub formă de sustragere, alterare sau distrugere a informaţiei computerizate sau a mijloacelor de protecţie a acesteia;
3. *Legătura cauzală* dintre fapta prejudiciabilă şi rezultatul produs.

A doua variantă constă în copierea ilegală a informaţiei computerizate.

Totodată, *a treia variantă* se exprimă în încălcarea esenţială a regimului de lucru al calculatoarelor, al sistemelor sau al reţelelor computaţionale.

După cum observăm, prima variantă a acestei infracţiuni este consumată din momentul survenirii urmărilor prejudiciabile sub formă de sustragere, alterare sau distrugere a informaţiei computerizate sau a mijloacelor de protecţie a acesteia (componenţă materială). Însă, în celelalte cazuri infracţiunea va fi consumată la săvârşirea acţiunilor (inacţiunilor) de copiere ilegală a informaţiei computerizate sau în cazul încălcării esenţiale a regimului de lucru al calculatoarelor, al sistemelor sau al reţelelor computaţionale (componenţe formale).

Latura subiectivă a infracţiunii prevăzute la art.363 CP al Ucrainei se caracterizează prin vinovăţie atât sub formă de intenţie directă, cât şi sub formă de imprudenţă.

Subiect al acestei infracţiuni este special, şi anume: persoana responsabilă pentru exploatarea calculatoarelor, sistemelor computaţionale sau a reţelelor informaţionale.

Totodată, alin.(2) art.363 CP al Ucrainei prevede o circumstanţă agravantă, cum ar fi cauzarea prejudiciului considerabil.

Mai mult, putem menţiona că în privinţă la săvârşirea infracţiunilor în sfera informaţiei electronice Codul penal al Ucrainei nu s-a limitat numai la aceste trei componenţe (art.361-363 CP), dar şi a indicat expres în art.163 CP la posibilitatea încălcării secretului corespondenţei, inclusiv prin intermediul reţelelor de telecomunicaţii şi calculatoare.

Totodată, ***Codul penal al Republicii Belarus***, adoptat la 9 iulie 1999 [8], se caracterizează printr-o diversitate amplă a componenţelor de infracţiuni comise în sfera informaţiei electronice. În cele ce urmează ne vom strădui să evidenţiem doar anumite momente particulare, fără a supune unei analize juridico-penale amănunţite componenţele existente în sfera informaţiei electronice în legea penală a Republicii Belarus.

În special, Capitolul 31 *„Infracţiuni contra securităţii informaţionale”* din Codul penal cuprinde şapte articole în sfera săvârşirii infracţiunilor ce atentează la securitatea informaţională:

1. Accesul neautorizat la informaţia computerizată (art.(349);
2. Modificarea informaţiei computerizate (art.350);
3. Sabotajul informaţional (art.351);
4. Obţinerea ilegală a informaţiei computerizate (art.352);
5. Confecţionarea sau înstrăinarea mijloacelor speciale pentru efectuarea accesului neautorizat la sistemul sau la reţeaua de calculatoare (art.353);
6. Elaborarea, utilizarea sau răspândirea programelor dăunătoare (art.354);
7. Încălcarea regulilor de exploatare a sistemelor sau a reţelelor de calculatoare (art.355).

Mai mult, Capitolul 24 *„Infracţiuni contra proprietăţii"* din Codul penal cuprinde două articole care stabilesc răspunderea penală pentru săvârşirea sustragerii sau pentru cauzarea prejudiciului material prin utilizarea informaţiei electronice:

1. Sustragerea săvârşită prin utilizarea tehnicii de calculator (art.212);

2. Cauzarea prejudiciului material în lipsa semnelor de sustragere (art.214).

Capitolul 37 *„Infracţiuni militare"* din Codul penal prevede răspunderea penală pentru divulgarea secretelor de stat sau pentru pierderea din imprudenţă a documentelor sau a informaţiei computerizate ce conţin astfel de secrete (art.458).

De menţionat că în aceste cazuri informaţia electronică (computerizată) este folosită sau în calitate de mijloc al săvârşirii infracţiunilor contra proprietăţii (art.212, 214 CP), sau în calitate de obiect imaterial al infracţiunii (art.458).

Doctrina penală a Republicii Belarus tratează *informaţia electronica* ca fiind o informaţie care se conţine în sistemul calculatorului sau în alte dispozitive tehnice dacă se asigură descifrarea ulterioară a acestei informaţii prin intermediul calculatorului [9].

După cum corect au observat autorii V.Kozlov [10] şi V.Puşcin [11], în Codul penal al Republicii Belarus sunt evidenţiate trei categorii de infracţiuni săvârşite în sfera informaţiei electronice:

a) infracţiuni în cadrul cărora informaţia electronică este recunoscută în calitate de obiect imaterial (art.349-355, art.458);

b) infracţiuni în cadrul cărora informaţia electronică este privită ca mijloc de săvârşire a acestora (art.212, 214).

c) infracţiuni săvârşite prin intermediul tehnicii speciale de calculator (art.179 „Culegerea ilegală sau răspândirea informaţiei despre viaţa privată", art.188 „Calomnie", art.203 „Încălcarea secretului corespondenţei, a convorbirilor telefonice, sau a altor mesaje", art.219 „Distrugerea sau deteriorarea bunurilor din imprudenţă", art.254 „Spionajul comercial" etc.)

Suntem de acord cu sistematizarea propusă şi, ca urmare, recomandăm ca sintagma *„prin intermediul informaţiei electronice sau cu folosirea tehnicii speciale de calculator"* să fie introdusă în calitate de semn calificativ în legislaţia penală actuală atât a României, cât şi a Republicii Moldova.

***Codul penal al Federaţiei Ruse**,* adoptat la 24 mai 1996 [12], prin introducerea Capitolului XXVIII al Părţii Speciale „Infracţiuni în sfera informaţiei computerizate" a reuşit să înlăture lacuna care a existat în domeniul protecţiei juridico-penale a informaţiei în legislaţia rusă.

În doctrina penală rusă majoritatea savanţilor sunt de părere că *infracţiunea săvârşită în sfera informaţiei computerizate* este o faptă socialmente periculoasă (acţiune sau inacţiune) ce atentează la informaţia electronică care aparţine statului, persoanei juridice sau fizice, sau ce atentează la ordinea stabilită de stat sau de alt proprietar în sfera creării, obţinerii sau utilizării acestei informaţii, dacă cele săvârşite au cauzat sau au creat pericol real de cauzare a prejudiciilor materiale posesorului acestei informaţii sau a dispozitivelor tehnice automatizate în care se conţine, se prelucrează, se transmite sau se distruge informaţie electronică, ori dacă au condus la survenirea altor urmări grave [13].

Analizând legislaţia penală a Federaţiei Ruse, observăm că Capitolul XXVIII *„Infracţiuni în sfera informaţiei computerizate"* al Părţii Speciale din Codul penal actual conţine următoarele articole:

- Accesul neautorizat la informaţia computerizată (art.272);
- Crearea, folosirea şi răspândirea programelor dăunătoare pentru calculator (art.273);
- Încălcarea regulilor de exploatare a calculatoarelor, sistemelor sau a reţelelor de calculatoare (art.274).

Articolul 272 CP al Federaţiei Ruse asigură protecţia juridico-penală a informaţiei computerizate ce aparţine oricărei întreprinderi, instituţii, organizaţii sau persoanei fizice. Dispoziţia articolului respectiv prevede răspunderea penală pentru accesul ilegal (neautorizat) la informaţia computerizată, adică la orice informaţie ce se află pe un dispozitiv material într-o formă electronică, cum ar fi: calculator, sistemul de calculatoare sau reţeaua de calculatoare [14]. Noţiunea *„informaţia computerizată ocrotită de lege"* este o noţiune vagă şi cuprinde aproape toată informaţia conţinută pe vreun suport tehnic. Acest tip de informaţii este reglementat şi ocrotit de o listă întreagă de acte normative din Federaţia Rusă [15].

De menţionat că această componenţă este una materială, deoarece survenirea urmărilor prejudiciabile (cum ar fi: distrugerea, blocarea, modificarea sau copierea informaţiei, încălcarea regimului de lucru al calculatorului, sistemului sau al reţelei de calculatoare) este obligatorie.

Crearea acestei norme a fost dictată de faptul că majoritatea normelor existente nu asigură protecţia corespunzătoare a informaţiei computerizate, în special, art.137 CP – încălcarea inviolabilităţii vieţii personale;

art.138 CP – încălcarea secretului corespondenței sau a altor mesaje; obținerea ilegală şi divulgarea datelor ce constituie secret comercial, bancar sau fiscal etc. [16].

Totodată, norma juridico-penală prevăzută în art.273 CP al Federației Ruse este destinată pentru protecția intereselor materiale ale utilizatorului contra viruşilor de calculator [17]. Aşadar, dispoziția art.273 CP al Federației Ruse cuprinde crearea programelor pentru calculator, introducerea modificărilor în programele existente ce provoacă în mod intenționat distrugerea, blocarea, modificarea sau copierea neautorizată a informației, încălcarea regimului de lucru al calculatoarelor, sistemelor sau al rețelelor de calculatoare, precum şi utilizarea sau răspândirea acestor programe sau a dispozitivelor ce conțin astfel de programe. Infracțiunea se consideră a fi consumată indiferent de survenirea consecințelor dăunătoare; componența este formală.

Varianta agravată a acestei infracțiuni este prevăzută la alin.(2) art.273 CP al Federației Ruse şi prevede răspundere penală pentru aceeaşi faptă dacă ea a provocat urmări grave. În literatura de specialitate se menționează că în calitate de urmare gravă poate fi recunoscută avaria sau suspendarea continuă a activității unei întreprinderi sau organizații, decesul unei persoane, prejudicierea sănătății a mai multor persoane, pierderea informației tehnico-ştiințifice unicale etc. [18].

Însă, art.274 CP al Federației Ruse prevede răspunderea penală pentru încălcarea regulilor de exploatare a calculatoarelor, sistemelor sau a rețelelor de calculatoare. Pentru survenirea răspunderii penale conform acestui articol este necesar de a stabili, în primul rând, că subiectul a avut acces la calculator, la sistemul sau la rețeaua de calculatoare, iar, în al doilea rând, că această faptă a cauzat prejudiciu considerabil prin distrugerea, blocarea sau modificarea informației computerizate ocrotite de lege [19].

Precizăm în acest sens că, în cazul săvârşirii infracțiunilor prevăzute în art.272-273 CP al Federației Ruse, latura subiectivă se caracterizează prin vinovăție sub formă de intenție directă, iar în cazul infracțiunii prevăzute în art.274 CP al Federației Ruse vinovăția poate fi manifestată atât prin intenție, cât şi prin imprudență.

Evidențiem că faptele sus-menționate deseori sunt alese de către făptuitor în calitate de metoda a săvârşirii infracțiunilor contra proprietății, cum ar fi: escrocheria, însuşirea sau delapidarea averii străine etc. Majoritatea practicienilor propun ca astfel de fapte să fie calificate în cumul ideal, argumentându-şi poziția prin diferența în obiectele atentării criminale [20]. În special, sustragerea unei sume băneşti prin intermediul accesului neautorizat la informația computerizată trebuie încadrată ca cumul ideal al infracțiunilor prevăzute la art.159 (160) şi art.272 CP al Federației Ruse [21].

Mai mult, infracțiunile săvârşite în sfera informației computerizate pot fi conexe cu infracțiunile ce atentează la drepturile de autor (art.146 CP al Federației Ruse) sau la drepturile de invenție (art.147 CP al Federației Ruse). În cazurile date cele săvârşite trebuie calificate în cumul conform art.146 (147) şi 272 (273) CP al Federației Ruse [22].

În opinia mai multor savanți şi practicieni din Federația Rusă [23], legea penală actuală trebuie completată cu un articol de sine stătător care ar prevedea răspunderea penală pentru sabotajul informațional, obținerea ilegală a informației computerizate prin escrocherie şi confecționarea sau înstrăinarea mijloacelor speciale pentru efectuarea accesului neautorizat la sistemul sau rețeaua de calculatoare.

Analizând legislația penală în vigoare a Ucrainei, a Republicii Belarus şi a Federației Ruse, concluzionăm, că, în general, infracțiunile informatice se referă la folosirea unuia sau mai a multor calculatoare pentru a facilita sau realiza comiterea unei infracțiuni şi care trebuiesc împărțite în următoarele categorii generale:

- ✓ infracțiuni în care calculatorul este o țintă (calculatorul sau calculatoarele unei părți inocente sunt atacate, exemplele incluzând vandalismul sau sabotajul informatic, şantajul etc.);
- ✓ infracțiuni în care calculatorul este o armă sau unealtă a infracțiunii (folosită pentru comiterea de infracțiuni „tradiționale", cum ar fi falsul, încălcarea dreptului de proprietate intelectuală, înşelăciune, spălarea banilor etc.) *şi*
- ✓ infracțiuni în care calculatorul este incidental în comiterea unor infracțiuni (spre exemplu, pentru păstrarea evidențelor asupra infracțiunilor comise).

Generalizând cele expuse, recomandăm ca sintagma *„prin intermediul informației electronice sau cu folosirea tehnicii speciale de calculator"* să fie introdusă în calitate de semn calificativ în legislația penală actuală atât a României, cât şi a Republicii Moldova.

Referințe:

1. Уголовный кодекс Украины от 5 апреля 2001 года // Ведомости Верховной Рады Украины. - 2001. - №25-26.
2. Карчевський М.В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальных машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину). Спеціальність 12.00.08 –

кримінальне право та кримінологія; кримінально-виконавче право: Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук. – Харків, 2003, с.14; Д.С. Азаров. Кримінальна відповідальність за злочини у сфере комп'ютерної информації. Спеціальність 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук. - Київ, 2003, с.12.

3. Карчевський М.В. Op. cit., p.9.
4. Азаров Д.С. Кримінальна відповідальність за злочини у сфере комп'ютерної информації. Спеціальність 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право: Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук. - Київ, 2003, с.11.
5. Уголовное право Украины. Общая и Особенная части: Учебник / Под общей редакцией профессора Е.Л. Стрельцова. – Харьков: ООО «Одиссей», 2002, с.561.
6. Уголовный кодекс Украины. Комментарий / Под редакцией Ю.А. Кармазина и Е.Л. Стрельцова. Издание второе. – Харьков: ООО «Одиссей», 2002, с.747.
7. *Citat după:* Кармазин Ю.А. и Стрельцов Е.Л. Op. cit., p.752.
8. Уголовный кодекс Республики Беларусь от 9 июля 1999 года // Переопубликован: Национальный реестр правовых актов Республики Беларусь. - 2006. - №122.
9. Вехов В. Проблема определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. - 2004. - №4. - С.15.
10. Козлов В. „Computer crime"? Что стоит за названием? (криминалистический аспект) // http://www.crime-research.ru/library/CCrime.html
11. Пущин В. Преступления в сфере компьютерной информации // http://www.mgua.newmail.ru/pub/glava28.htm
12. Уголовный кодекс Российской Федерации от 24 мая 1996 года // Собрание законодательства Российской Федерации. - 1996. - №25, ст.2955.
13. Менжега М.М. Некоторые дискуссионные вопросы понятия и содержания статьи 273 УК РФ (создание, использование и распространение вредоносных программ для ЭВМ) // Следователь. - 2004. - №3. - С.9-12; Мерзогитова Ю.А. Понятие компьютерной преступности // Вестник МВД России. - 2001. - №5-6. - С.84-88; Селиванов Н. Проблемы борьбы с компьютерной преступностью // Законность. - 1993. - №8. - С.36-40.
14. Уголовное право. Особенная часть: Учебник / Под редакцией Н.И. Ветрова и Ю.И. Ляпунова. - Москва: Новый Юрист, 1998, с.548-549.
15. Яшков С. Информация и УК РФ: теоретические проблемы применения норм закона // Российский судья. - 2004. - №7. - С.32.
16. Лопашенко Н.А. Уголовно-правовая и криминологическая политика государства в области высоких технологий // Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. - Киев: Национальная академия наук Украины, 2003, с.89-97.
17. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. - 1997. - №1. - С.8-15.
18. Карелина М.М. Преступления в сфере компьютерной информации // http://www.relcom.ru/Archive/1997/ComputerLaw/New_code.htm
19. Гульбин Ю. Преступления в сфере компьютерной информации // http://jurqa.hut.ru/all.docs/u/a/m7vryadd.html
20. Султанаева Г.Я. Компьютерные преступления как посягательство на информационную безопасность / Актуальные проблемы обеспечения безопасности, общества и государства в современных условиях: Сборник материалов российской научно-практической конференции. 26 апреля 2001 года: В 2-х частях. Часть 2. - Уфа: Уфимский юридический институт, 2001, с.331-337.
21. Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: Автореферат диссертации на соискание ученой степени кандидата юридических наук. - Волгоград, 2001, с.14.
22. Квалификация и доказывание преступных деяний, совершаемых в сфере компьютерной информации // http://koi.afisha.spb.ru/sec/method_01.htm
23. Семенов Г.В. Телекоммуникационное мошенничество: введение в проблему // Воронежские криминалистические чтения. Вып.1 / Под ред. О.Я. Баева. - Воронеж: Издательство Воронежского государственного университета, 2000, с.100-106; Федоров В.И. Борьба с транснациональной организованной преступностью в сфере «высоких технологий» // Прокурорская и следственная практика. - 1999. - №3. С.29-34; Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: Автореферат диссертации на соискание ученой степени кандидата юридических наук. - Красноярск: Красноярский Государственный Университет, 2002, с.11.

Prezentat la 20.10.2009