KRIMINĀLATBILDĪBA PAR AUTOMATIZĒTU DATU APSTRĀDES SISTĒMU NELIKUMĪGU IZMANTOŠANU
LIABILITY OF UNLAWFUL USE OF AUTOMATED DATA PROCESSING SYSTEMS

Karīna Kairiša
Rēzeknes Tehnoloģiju akadēmija, karina.kairisa@inbox.lv, Rēzekne, Latvija
Zinātniskā vadītāja: **Aija Jermacāne,** Mg.iur., docente

Abstract: *The 21st century is called the technological era where information storage takes place on the website. Due to the diversity there is an interest about the acquisition and use of confidential information in malicious intent. Offences in cyberspace are new in modern society and their discovery and observation is independent research question. Illegal access to automated data processing systems is creation of financial loss and persons legitimate interests violation with the material injury*. In article are analyzed signs Latvian Criminal law of the article 241st, 243rd and *the criteria for the qualification of the criminal offence of composition.*
Keywords: *automatic data processing system, cybercrime.*

Ievads

Pēdējos gados arvien aktuālāki kļūst informācijas sistēmu drošības jautājumi. Nereti personas, kas izdarījušas noziedzīgus nodarījumus pret informācijas sistēmu drošību, netiek sauktas pie atbildības. Šī raksta mērķis ir izvērtēt Krimināllikuma 241. un 243.panta sastāva pazīmes un tiesu praksi to normu pielietošanā. Pielietotās metodes: aprakstošā metode - apkopot informāciju un veikt detalizētu izpēti; analītiskā metode - veikt precīzu un skaidru valodas lietojumu; datu apstrādes statistiskā metode - analizēt un sistematizēt pētījumā iegūtos rezultātus.

Krimināllatbildība iestājas tad, kad apdraudējums ir sasniedzis tādu pakāpi, ka šīs darbības sāk būtiski traucēt personām realizēt savas likumīgās intereses. Krimināllatbildība par nodarījumiem pret informācijas sistēmu drošību, var būt piemērojama tikai tādā gadījumā, ja pantu dispozīcijās paredzētā nozieguma pazīmes ir kvalificētas noziedzīga nodarījuma pilnīgā sastāvā.

Krimināllikuma (turpmāk - KL) 241. panta pirmā daļa nosaka, ka krimināllatbildība piemērojama par patvaļīgu piekļūšanu automatizētas datu apstrādes sistēmas (turpmāk - ADAS) resursiem, ja tas saistīts ar sistēmas aizsardzības līdzekļu pārvarēšanu vai ja tas izdarīts bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības un ja ar to radīts būtisks kaitējums. Savukārt, 243.panta pirmā daļa nosaka, ka krimināllatbildība piemērojama par ADAS esošās informācijas neatļautu grozīšanu, bojāšanu, iznīcināšanu, pasliktināšanu vai aizklāšanu vai apzināti nepatiesas informācijas ievadīšanu ADAS, ja ar to radīts būtisks kaitējums.(*Krimināllikums 1998.g.)*

Ar ADAS parasti saprot datorsistēmu, datortīklu, tehnisko un informācijas resursu kompleksu, kam ir lietotāja pieeja. Izvērtējot šo pantu dispozīcijas autore secināja, ka minēto pantu redakcijas pilnībā atbilst gan Eiropas Padomes Kibernoziegumu konvencijai, gan ES pamatlēmumiem "Par uzbrukumiem informācijas sistēmām". Arī krimināltiesību speciālisti ir atzinuši, ka šajās KL normās, juridiskajā konstrukcijā nav neskaidru terminu, tās aptver visas kvalificējošās pazīmes, šajā gadījuma norādot uz to, ka attiecīgo pantu krimināllatbildības piemērošanā nav saskatāmas problēmas.*(Ķinis, 2007.,413.lpp.)* Pretēju viedokli pauž Informācijas Tehnoloģiju speciālisti, norādot, ka KL 241. un 243.panta dispozīcijas nav viegli uztveramas un saprotamas. Tās rada situāciju, kas liek uzskatīt, ka atbildība par attiecīgo normu pārkāpšanu iestājās tikai gadījumos, kad pierādāms „būtiskais kaitējums", kas noteikts minēto pantu sastāva kvalificējošās pazīmēs.*(Ķinis, 2014.,8.lpp.)* Būtiskā kaitējuma pazīmes nosaka likums Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību 23.pants. Atbildība par KL paredzēto noziedzīgo nodarījumu, ar kuru radīts būtisks kaitējums, iestājas, ja noziedzīgā nodarījuma rezultātā iestājušās kādas no minētajām sekām: 1)nodarīts mantisks zaudējums, kas noziedzīga nodarījuma izdarīšanas brīdī nav bijis mazāks par piecu tai laikā Latvijas Republikā

http://dx.doi.org/10.17770/iss2017.3016

noteikto minimālo mēnešalgu kopsummu, un apdraudētas vēl citas ar likumu aizsargātās intereses; 2) nodarīts mantisks zaudējums, kas noziedzīga nodarījuma izdarīšanas brīdī nav bijis mazāks par desmit tai laikā Latvijas Republikā noteikto minimālo mēnešalgu kopsummu; 3) ievērojami apdraudētas citas ar likumu aizsargātās intereses.(*Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību,2002.g.)* Piemēram, personai ir personīgais dators, kurā persona glabā tam piederošas privātas fotogrāfijas. Cita persona, šajā gadījumā likumpārkāpējs, iekļūstot ar speciālu programmu palīdzību, iegūst personai piederošās fotogrāfijas. Šajā gadījumā krimināLatbildība iestāsies par to, ka persona patvaļīgi piekļuvusi citas personas ADAS resursiem, bez attiecīgas sistēmas īpašnieka atļaujas. Pēc šāda nodarījuma izdarīšanas ir nepieciešams pierādīt, cik lielā mērā tika nodarīts kaitējums un vai tas ir atzīstams par būtisku. No augstāk minētā izriet, ka būtiski radīts kaitējums materiāli atlīdzināms ar piecām līdz desmit Latvijā noteiktām mēnešalgām. No minētā piemēra (nelikumīgi iegūtās fotogrāfijas) autore secina, ka nodarījuma rezultātā mantiskā zaudējuma pazīmju nav, jo noteikt noziedzīgā nodarījuma priekšmeta vērtību fiziski būs sarežģīti. Savukārt, personas likumiskās intereses uz privātās dzīves neaizskaramību tika aizskartas. Tāda veida būtiskā kaitējuma radīšana ir samērojama ar Latvijas Republikas Satversmē aizsargātām tiesībām. Cilvēka goda un cieņas aizskārums, privātīpašuma tiesību ierobežošana, kas rada būtisko kaitējumu morāles pamatnostādnēs. *(Vaznis, 2010., 26.lpp.)*

KL 241.panta dispozīcijā ietvertajiem saistvārdiem „ja" ir saprotams, ka krimināLatbildība iestājas, īstenojās vismaz vienu no šādiem priekšnosacījumiem:

1) tas saistīts ar sistēmas aizsardzības līdzekļu pārvarēšanu;
2) ja tas izdarīts bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības.

Augstāk minētās tiesību normas nav nodalāmas no priekšnoteikuma, ka noziedzīga nodarījuma rezultātā personai ir nodarīts būtisks kaitējums, tas ir vienots komplekss. Tāpat arī KL 243. panta pirmā daļa nosaka noziedzīga nodarījuma sastāva pazīmes, kas ir esošās informācijas neatļauta grozīšana, bojāšana, iznīcināšana, pasliktināšana vai aizklāšana vai apzināti nepatiesas informācijas ievadīšana. (*Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību,2002.g.)* Nelikumīga piekļūšana un apzināta ietekmēšana ir iespējama gan valsts aizsargātās ADAS, gan privātās ADAS, kas pieder fiziskām un juridiskām personām. Latvijas KL noziegumus pret sistēmas drošību iedala pie noziedzīgiem nodarījumiem pret vispārējo drošību un sabiedrisko kārtību, savukārt Vācijā, Francijā, Beļģijā, un Nīderlandē kvalificē kā noziedzīgus nodarījumus pret īpašumu, tādā veidā izdalot valsts aizsargāto īpašumu no personas privātīpašuma. Svarīgi atzīmēt, ka tāda veida iedalījums ir tiesu prakses esības iemesls šajās valstīs.

Saskaņā ar KL 1. pantu pie krimināLatbildības ir saucama persona, kuras darbībās ir visas nozieguma sastāva pazīmes - nodarījuma objekts, objektīvā puse, subjekts un subjektīvā puse. Kā viena no sākotnējām problēmām, kuras dēļ praktiski ir apgrūtināta KL 241. panta piemērošana, ir neskaidrības par noziedzīgā nodarījuma objektīvās puses saturu. Par noziedzīga nodarījuma objektīvo pusi Latvijas krimināltiesību teorijā un praksē atzīst personas uzvedības ārējo izpausmi, kas var radīt kaitīgas izmaiņas apkārtējā pasaulē. KL 241. panta objektīvo pusi raksturo patvaļīga piekļūšana ADAS. Patvaļīga piekļūšana ir nodarījums, kuru var veikt tikai ar aktīvu, mērķtiecīgu darbību. Tas nozīmē, ka persona, kas veic patvaļīgo piekļuvi ADAS, apzinās, ka tā veic prettiesisku darbību, kas ir vērsta uz negatīvu rezultātu - bez tiesībām piekļūt ADAS resursiem un brīvi manipulēt ar sistēmā esošajiem resursiem, tajā skaitā tos nelikumīgi kopēt, pārsūtīt uz citu ADAS u. tml.*(Dimitrova, 2015.,54.lpp.)* Izriet, ka bez šīm pazīmēm jākonstatē, ka šādu darbību rezultātā ir nodarīts būtisks kaitējums cietušā likumīgajām interesēm. Likumdevējs KL 241. pantā paredzēja atbildību par patvaļīgu piekļūšanu atsevišķi novietotai datorsistēmai. Gadījumā, ja datorsistēma nav savienota ar tīklu, vienīgā iespēja, kā piekļūt šādai datorsistēmai, ir fiziski iekļūt attiecīgā telpā, kur izveidota datorsistēma, un iepazīties ar tajā esošo informāciju, jo tieši šis apstāklis ir atzīts par darbību, kas veido noziedzīgā nodarījuma objektīvo pusi. Taču tiesisku fizisku iekļūšanu telpā, kur atrodas datorsistēma, nevar uzskatīt par patvaļīgu ADAS piekļuves sastāvdaļu. Tādējādi norādot uz to, ka KL 241. panta izpratnē patvaļīgas piekļuves saturā neietilpst personas darbības, fiziski

īstenojot nelikumīgu piekļuvi telpai, kur izvietota datorsistēma. KL 241. pantā iekļautajā objektīvas puses saturā, ietilpst tikai tāda veida darbības, kuras tiek īstenotas ar programmatūras līdzekļiem.

Problēmas izraisa patvaļīgās piekļuves saturs, attiecinot to uz atsevišķi novietotu datorsistēmu, jo piekļuves tiesības sastāv no diviem elementiem:

1) personai piešķirtiem identifikatoriem un to identifikācijas;

2) sistēmas spējas pēc šiem identifikatoriem atpazīt lietotāju, respektīvi, autorizēt un dot viņam piekļuvi attiecīgiem sistēmas resursiem. *(Ķinis, 2011., 14.lpp.)*

Ārvalstu praksē piekļuvi ADAS par patvaļīgu atzīst, ja ir pārvarēta drošības sistēma, kas pieļauj pieslēgšanos datorsistēmai. Piemēram, Kanzasas Augstākās tiesas spriedumā krimināllietā State v Allen tiesa precīzi definēja, ka piekļūšana ir brīva iespēja kaut ko lietot. Respektīvi, ja kāds vēlas ierobežot pieeju savai informācijai, viņam tā ir jāizsargā. Brīvība ir spēja izmantot savas tiesības, nepastāvot ierobežojumiem. Tādējādi analizējot patvaļīgas piekļuves jēdzienu, jāievēro princips, ka atļauts ir viss, kas nav aizliegts. Faktiski, ja persona nav ierobežojusi citām personām pieeju savai informācijai, tad nevar uzskatīt, ka šī informācija ir privāta un piekļūšana šai informācijai var netikt uzskatīta par noziedzīga nodarījuma izdarīšanu. Pretējā gadījumā jebkuru informāciju, kurai iespējams publiski piekļūt un kuras piekļūšanai mēs nelūdzam atļauju, var tik uzskatīta par patvaļīgu piekļūšanu. *(Ķinis, 2011., 16.lpp.)* Tātad, ja persona, nav nodrošinājusi savu datu apstrādes sistēmu ar ierobežojumiem, kas ierobežo citu personu piekļuvi - paroles uzstādīšana, balss identifikācija, identifikācija pēc pirkstu nospieduma u.c., tad šādas darbības nevar tikt kvalificētas kā patvaļīga piekļuve ADAS KL 241. panta izpratnē. Tādā veidā apdraudētās intereses nav informācijas sistēmu drošības pazīme – pieejamība, bet gan konfidencialitāte, integritāte un personas mantiskās intereses. Faktiski, par patvaļīgu piekļūšanu citas personas piederošai ADAS var tikt uzskatīts gadījums, kad persona, ievērojot informācijas drošības noteikumus, uzstādījusi savam datoram piekļuves ierobežojumus, taču cita persona – šajā gadījumā – likumpārkāpējs, apejot vai uzlaužot attiecīgos ierobežojumus – iekļuvusi citas personas datorā.

Viena no ES, kas piemēro ierobežojumus publiski pieejamām ADAS ir Itālija. Itālijas Soda likuma 635. pants kā atbildības nosacījumu patvaļīgai piekļuvei publiski pieejamām mājas lapām atzīst tā sauktās klusējošās gribas pārkāpumu, proti, īpašnieks vai lapas autors mājas lapā ievietojot informāciju, ir izteicis savu gribu, ka viņš vēlas to redzēt tieši tādu. Tāpēc nevienam nav tiesību to mainīt bez viņa piekrišanas*.(Krastinš U., Liholaja V., 2008.,57.lp.)* Šāda pieeja ir atbalstāma. Piekļuve publiski pieejamām mājas lapām un to satura izmainīšana nesatur KL 241. panta pirmājā daļā paredzētā nodarījuma sastāva pazīmes, jo šajā gadījumā apdraudētās intereses ir informācijas integritātes nodrošināšana. Tādējādi secināms, ka KL 241. Panta pirmajā daļā paredzēto noziedzīga nodarījuma sastāvu nav iespējams īstenot. Piemērojot šo pantu dzīvē un nonākot lietai tiesā, pastāv iespēja, ka tiesa iedziļinātos lietas būtībā, un secinātu, ka šā panta izpratnē nav iespējams realizēt patvaļīgu piekļuvi ADAS kārtībā un veidā, kā to paredzējis likumdevējs. Ar 2014. gada 29. oktobra grozījumiem KL 241. pantā paredzēto nodarījumu var veikt tikai ar aizsardzības sistēmas pārvarēšanas līdzekļu palīdzību, nevis fiziski kontaktējoties ar datorsistēmu, kas faktiski nav uzskatāms panta mērķi. Likumdevējs, izdodot attiecīgo regulējumu, vēlējās pasargāt cilvēkam piederošās privātās informācijas noplūdi no tiem piederošajiem tehniskajiem – automatizētajiem līdzekļiem, izmantojot speciālās programmas. Taču, no sākotnējās likumā ietvertās un dzīvē realizējamās normas satura izrietēja, ka likumdevējs ir vēlējies ierobežot fizisku piekļuvi cietušās personas ADAS saturam. Izpētot Latvijas tiesu praksi, kas saistīta ar noziedzīgiem nodarījumiem pret ADAS autore secināja, ka pieejamās prakses apjoms ir neliels. Kopumā laika periodā no 2007.-2017.gadam ir izskatītas 12 lietas, kas ir nonākušas līdz tiesvedības procesam un tika kvalificētas pēc 241.un 243.panta sastāva pazīmēm. No tā izriet, ka Latvijā noziedzīgi nodarījumi pret ADAS līdz tiesai nonāk retos gadījumos. Par iemeslu tam var būt zems noziegumu atklāšanas līmenis valstī un nepietiekama praktiskā darba pieredze šo nodarījumu izmeklēšanā un kvalificēšanā. Pastāv varbūtība, ka par šiem noziegumiem neziņo. Katrs uzņēmums vai iestāde rūpējas par savu reputāciju. Līdz ar to ziņojums par iekļūšanu kādā no uzņēmuma vai iestādes ADAS var

negatīvi ietekmēt tās turpmāko darbību. Autore izpētīja vairākus tiesas spriedumus saistībā ar apsūdzības celšanu pēc KL 241. un 243. panta. Augstākās tiesas lēmums lietā SKK-0382-14, kur apsūdzība tika celta pēc KL 175.panta ceturtās daļas un KL 241.panta otrās daļas , kā rezultātā cietušajam tika radīts būtisks kaitējums. Pēc apgabaltiesas sprieduma apsūdzētā persona tika attaisnota pēc 241.panta otrās daļas, atzīstot, ka nodarījumā nav nozieguma sastāva pazīmju. Apelācijas tiesas spriedums tika atcelts un nosūtīts atkārtotai izskatīšanai apelācijas instances tiesā. Augstākā tiesa atzina, ka sprieduma pieņemšanai ir jāizvērtē visi apstākļi, kas saistīti ar nozieguma izdarīšanu, t.i. nozieguma uzsākšana nelikumīgi piekļūstot uzņēmuma ADAS, sistēmas drošības līdzekļus pārvarēšana un bojāšana, līdz nozieguma pabeigšanas stadijai mantkārīgā ceļā nelikumīgu līdzekļu iegūšana.(*Augstākās tiesas lēmums lietā Nr. SKK-0382/14, 2014.)* Autore piekrīt Augstākās tiesas lēmumu. Pasludinot spriedumu, apelācijas instances tiesas pienākums izvērtēt visas nozieguma stadija un noziedzīgā nodarījuma sastāva pazīmes pēc to kvalifikācijas. Patvaļīga piekļūšana ADAS pārvarot sistēmas drošības līdzekļus ar mantkārīgu nolūku ir noziegums, kas ir kvalificējams pēc 241.panta otrās daļas.

Šajā jautājumā būtu nepieciešams analizēt arī sabiedrībā pazīstamu Ilmāra Poikāna jeb Neo lietu. Poikānam apsūdzība celta pēc Krimināllikuma 200.panta otrās daļas - par ekonomisko un citu ziņu, kuras ir komercnoslēpums, neatļautu iegūšanu savai vai citas personas lietošanai. Apsūdzība celta arī pēc Krimināllikuma 145.panta pirmās daļas - par nelikumīgām darbībām ar fiziskās personas datiem, radot būtisku kaitējumu. No apsūdzības oriģināla izriet, ka, būdams reģistrēts EDS lietotājs un apzinoties piekļūšanas kārtību deklarēšanas sistēmā, 2009.gada jūlijā Poikāns konstatējis VID sistēmas ievainojamību. *(Tiesa beidzot sāk skatīt tā saucamo Neo lietu.,2014.)* Pēc autores domām, šī lieta varēja kalpot kā jauns informācijas avots kvalificējot nodarījumus pret ADAS kā pamatā ir patvaļīga piekļūšana ADAS. Grūti spriest par noziedzīgā nodarījuma sastāva saturu un tā pazīmēm, jo informācija ir konfidenciāla, tomēr pamatā noziegums tika balstīts uz patvaļīgu piekļūšanu VID informācijai izmantojot interneta vidi. Strauja jauno tehnoloģiju attīstība rada ne tikai pozitīvās izmaiņas, bet arī negatīvas sekas, tādas kā noziedzību elektroniskajā vidē. Jaunā paaudze arvien vairāk velta laiku komunikācijai interneta vidē. Noziedzīgo nodarījumu skaita pieaugums var būt attiecināms uz patstāvīgu uzturēšanos interneta vidē. Pastāv nepieciešamība pievērst lielāku uzmanību ADAS drošības jautājumiem.

Secinājumi un priekšlikumi

1. Kvalificējot noziedzīgo nodarījumu pēc KL 241.vai 243.panta nepieciešams noteikt kāda veida būtisks kaitējums tika nodarīts cietušajai personai. Ja būtisks kaitējumus radīja mantiskos zaudējumus, tad šos zaudējumus ir iespējams aprēķināt. Turpretī, ja tiek pārkāptas personas likumīgās intereses uz konfidencialitāti, persona var tikt pakļauta sabiedrības kritikai un atstumšanai. Likumdevējam ir nepieciešams paredzēt cietušās personas aizsardzību un labas slavas atjaunošanu tiktāl cik to paredz likums. Būtu nepieciešams piemērot soda sankcijas par personas likumīgo interešu apdraudējumu izdalot to pēc radītā būtiskā kaitējuma satura.
2. Salīdzinot Itālijas, Vācijas, Francijas un Beļģijas krimināLkodeksu tika secināts, ka noziedzīgie nodarījumi pret ADAS tiek kvalificēti kā noziedzīgi nodarījumi pret īpašumu. Latvijas KL būtu nepieciešams ieviest normas, kas nodalītu valsts institūciju ADAS apdraudējumu no privātpersonu ADAS apdraudējuma. Tādā veidā nosakot sankciju apmēru pamatojoties uz radītā būtiskā kaitējuma apmēru.
3. Tiesu prakses trūkums liecina ne tikai par zemu noziedzīgo nodarījumu atklāšanu valstī, kas vērsts pret ADAS, bet privātpersonu un iestāžu nevēlēšanos atklāt problēmas savā iestādē vai uzņēmumā. Šajā gadījumā būtu nepieciešams uzlabot kompetento institūciju darbu sadarbībā ar sabiedrību, kas spētu veikt darbu augstā konfidencialitātes līmenī. Tādā veidā būtu iespējams panāk atbildes reakciju no sabiedrības un veicināt sadarbošanās iespējas starp valsts tiesību aizsardzības iestādēm un personu.

Izmantotās literatūras un avotu saraksts

Normatīvie akti:

1. *Krimināllikums* [tiešsaistē]. 25.09.2014. [atsauce 08.05.2017.]. Pieejas veids: https://likumi.lv/ta/id/269516-grozijumi-kriminallikuma
2. *Krimināllikums* [tiešsaistē]. LR 17.06.1998. likums ar groz. Līdz 15.12.2016. [atsauce 08.05.2017.]. Pieejas veids:https://likumi.lv/doc.php?id=88966
3. *Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību* [tiešsaistē]. LR 27.11.2002. likums ar groz.līdz 03.12.015. [atsauce 08.05.2017.]. Pieejas veids: https://likumi.lv/doc.php?id=88966

Grāmatas:

1. Krastinš U., Liholaja V. *Salīdzināmās kriminālties*ības. Rīga: Tiesu namu aģentūra, 2008. 157.lp.
2. Ķinis, U. *Kibernoziegumi*. Rīga: Biznesa augstskolas Turība, 2007.413.lpp.

Autoru publikācijas:

1. Dimitrova, S. *Nacional cybersecurity strategies in member of the European Union*. Administratīvā un Krimināla Justīcija, 2015.g. 4.aprīlis. Nr.73, 54-58.lp.
2. Ķinis, U. *Nodarījumi pret informācijas sistēmas drošību*. Jurista Vārds, 2011.g. 27.sept. Nr. 39., 14-18.lp
3. Ķinis, U. *Krāpšana automatizētā adatu apstrādes sistēmā*. Jurista Vārds, 2014.g. 15.jūl. Nr. 27. 6-15.lp.
4. Vaznis, A. *Satversme garantē, bet kā ir praksē*. Jurista vārds, 2010.g. 30.marts Nr.13., 26-28.lp.

Internet tīklā publiskoto materiālu

1. Tiesa beidzot sāk skatīt tā saucamo Neo lietu. Diena. 14.04.2014. [tiešsaitē]Skatīts: 08.05.2017. Pieejas veids: https://www.diena.lv/raksts/latvija/zinas/tiesa-beidzot-saks-skatit-ta-deveto-_neo-kriminallietu_-14052167

Summary

The questions about relation to information systems security problems are getting more apparent nowadays. The main problem in this field is that there are persons who have committed offences against the security of the information systems, and they is not brought to justice. Responsibility for criminal offences against information security are included in Latvian Criminal law 241st and 243rd article, however this margin is a rare phenomenon in practice. Legislature developing rules, which determine responsibility for offences against the security of information systems, allowed mistakes which made relevant rules originally unpossible to apply. Legislature made substantial mistakes in 241st article first part content, setting incorrect rules applicable to subjective way. Determining rules applicable to subjective way, legislature wasn't considering „arbitrary intrusion" content elements, in that way formulating incorrectly 241st article first part goal of Criminal law. With this provision, the legislature wanted to establish responsibility, for arbitrary access to automated data protection system, which can be implementation with the help of special utility program help, but incorrectly formulated crime content, allowed to extend arbitrary access to automated data processing system through physical contact. By 29 October 2014, amendments to the Criminal contradictions were eliminated on the grounds that an arbitrary access can only be considered by security system resources management. Cyber threat to society is increasing every year as a result it is necessary to pay attention to the crimes and judicial practice creation. It is often believed that what does not appear is disproportionate. Cyberspace volumes are not applicable, so it is necessary to improve and use in country the specialist practice of protection against these crimes. Everyone has the duty to take care of your data processing system security insofar as permitted by law. There are also other problems, which legislature is trying to eliminate progressively, thereby streamlining and updating of offences against the rules applicable to the security of information systems.