LATVIJAS UNIVERSITĀTE
JURIDISKĀ FAKULTĀTE
KRIMINĀLTIESISKO ZINĀTŅU
KATEDRA

# DISERTĀCIJA

## Noziedzīgi nodarījumi pret informācijas sistēmu drošību (kibernoziegumi)

M. iur.Uldis Ķinis
110653-11752

Zinātniskais vadītājs
Dr. habil. jur. profesors
Uldis Krastiņš



Rīga 2005

# Saturs

## Ievads

XXI gadsimts, ko sauc arī par digitālo tehnoloģiju laikmetu, ir radījis sabiedrībai jaunas iespējas. Šodien sabiedrības dzīve nav iedomājama bez elektronisko pakalpojumu izmantošanas, taču līdz ar tehnoloģiju radītām iespējam rodas jauni noziedzīgu nodarījumu veidi, kas kaitīguma ziņā ir daudz bīstamāki par tādiem tradicionāliem noziedzīgiem nodarījumiem kā zādzība, krāpšana, kas izdarīti reālā vidē.

Saskaņā ar Karnegi Mellona datorprogrammu inženierzinātnes institūta CERT/CC statistiku[1] redzams, ka 1988. gadā bija saņemtas ziņas par 8 iebrukumiem informāciju sistēmās, bet 1989.gadā jau par 132, 2002. gadā - 82094, tad 2003. gadā jau notikuši 137529 iebrukumi datorsistēmās. ANO organizētajā pētījumā "Informācijas nedrošība"[2] atzīmēts, ka kibertelpas apdraud šādas personu grupas:

1. Ļaunprātīgi "savi cilvēki" (*malicious insiders*), kas ļaunprātīgi izmanto zināšanas par sistēmas resursiem. Viņu motivāciju var iedalīt divās lielās kategorijās: a) ekonomiskais labums, ko viņi vēlas iegūt no bijušā darba devēja krāpšanas vai izspiešanas veidā; b) kas vēlas nodarīt kaitējumu, lai sariebtu saviem darba biedriem vai darba devējiem gan personisku, gan politisku motīvu vadīti. "Savi cilvēki" ir bīstami tāpēc, ka viņiem ir informācija par sistēmas drošības vārīgām vietām, tie viegli var to izmantot, ievadīt sistēmā kaitīgas ierīces, radīt sistēmā darbības traucējumus, piesavināties datus. Šī grupa ir sevišķi bīstama apstākļos, ja sistēmas darbība ir saistīta ar valstij svarīgas kritiskās informācijas apstrādi. Auditoru firma KMPG aptaujāja 1238 kompānijas par draudu faktoriem viņu sistēmu drošībai. 90% no aptaujātajiem atzina, ka vislielākos draudus sistēmu drošībai rada tieši pašu darbinieki.[3]

---

[1] 2004 Carnegie Mellon University // http://www.cert.org/stats/#incidents (aplūkots 2005.gada 10. janvārī)

[2] Gelbstein Eduardo, Kamal Ahmad Information insecurity. A survival guide to the unchartered theritories of cyber-threats and cyber security.- New York Published by the United Nations ICT Task Force and the United Nations Institute for Training and Research, 2002, p. 24, 25.

[3] Routine external and internal "hacking" , An important par of information assurance. Mary Washington College, MBUS 511, Security Essentials by Benjamin Herman GSEC Practical Assignment - Version 1.2b © SANS Institute 2003,p.1

2. "Skripta[4] bērni" (*script kiddies*) – jauni cilvēki, kuriem nav pietiekamas zināšanas datorzināšanās, bet kuri no dažādiem avotiem iegūst jau gatavus instrumentus, ar ko var realizēt patvaļīgu piekļuvi.
3. Profesionāli sistēmu uzlauzēji- (hakeri) (*haker, cracker*) tehniski izglītotas personas, kas spēj izstrādāt programmas, zina, kā atklāt sistēmās drošības vārīgās vietas. Tas dod iespēju viņiem izstrādāt speciālus rīkus, lai realizētu patvaļīgu piekļuvi, un piedāvāt šos rīkus, programmas citām personām. Hakeru kustība pasaulē ir labi organizēta, un kopš 1993. gada notiek ikgadējas DEFCON - pasaulē lielākās interneta drošības pagrīdes organizācijas kongress.[5] Diemžēl ir jāatzīst, ka pasaulē "hakeru" zināšanas informācijas sistēmu drošības jautājumos ir daudz vispusīgākās kā sistēmu drošības administratoriem. Tāpēc šī "slikto puišu" grupa var būtiski apdraudēt informācijas sistēmu drošību.
4. Politiski motivēti hakeri (*hactivists*) –savu kaitīgo darbību vērš pret valdību, starptautisku organizāciju, finansu institūciju mājas lapām. Iedarbība izpaužas, pārveidojot to saturu, bloķējot pieeju vai nolaupot mājas lapu, tas ir, novirzot mājas lapai paredzēto informācijas plūsmu uz citiem avotiem. Šīs grupas pārstāvji nodarbojas arī ar vardarbības un rasu naida kurināšanu internetā.
5. Spiegi (*spies*). Šajā grupā ietilpst gan rūpnieciskā, gan cita rakstura spiegošana. Jāpiezīmē, ka elektroniskā spiegošana ir plaši izplatīta parādība. 2001. gadā ES Parlaments izveidoja speciālu izmeklēšanas komisiju, kas sagatavoja ziņojumu[6] par ASV globālās spiegošanas sistēmas ESHELON[7] ietekmi uz ES dalībvalstīm.
6. Organizētā noziedzība- plaši izmanto kibertelpu dažādas starptautiskas noziedzīgas organizācijas netīrās naudas atmazgāšanai, krāpniecisku, izspiešanas, pornogrāfijas u.c. noziedzīgu darbību veikšanai.

---

[4] Instrukciju virkne, kas nosaka, kā programmai jāveic kāda specifiska procedūra, piemēram, ieiešana elektroniskā pasta sistēmā. http://www.termini.lv/index.php (aplūkots 2004.gada 12. martā)

[5] DEFCON http://www.defcon.org (aplūkots 2004. gada 23. martā).

[6] Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)) 11. July 2001.

[7] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci560967,00.html (aplūkots 2004.gada 23. martā).

7. Kiberteroristi un kiberkareivji – kiberterorisms ir tīša ar nodomu veikta darbība pret automatizētās datu apstrādes sistēmas resursiem ar mērķi panākt politisku vai ekonomisku labumu, nodarot pēc iespējas lielāku kaitējumu sabiedrības interesēm. Īpaši aktuāls jautājums par kiberterorismu kļuva pēc 2001. gada 11. septembra notikumiem ASV. Šie notikumi parādīja, ka teroristi savā darbībā, lai panāktu savus mērķi ietekmēt sabiedrības dzīvei nepieciešamās kritiskās infrastruktūras sfēras, sekmīgi izmantoja jaunākos zinātnes sasniegumus. Teroristu rokasgrāmatā[8] norādīts, ka, lai veiktu patvaļīgu piekļūšanu informācijas sistēmai ir nepieciešama datora tastatūra un zināšanas par paroļu veidošanas principiem, un interneta pieslēgums, un telefona numurs. Grāmatā ir doti sīki detalizēti skaidrojumi, kādas darbības personai ir jāveic, lai pārvarētu sistēmas drošības līdzekļus, u.c. padomi.

CSI/FBI 2003. gada aptauja parādīja, ka katru gadu pieaug to apdraudējumu skaits, ko personas veic, izmantojot interneta resursus. 2003. gadā 78% no visiem uzbrukumiem ADAS resursiem tika veikti no interneta.[9] Austrālijā 2003. gadā veiktā kibernoziegumu un drošības aptauja[10] parādīja, ka 54% uzbrukumu saistīti ar internetu. Latvijā šobrīd nav daudz reģistrētu noziedzīgu nodarījumu pret informācijas sistēmu drošību, taču tas nekādā nenozīmē, ka šādu gadījumu nav. Tie vienkārši nenonāk tiesībaizsardzības speciālistu redzeslokā. Lai situāciju varētu mainīt un radīt sabiedrībā uzticību, ka Latvijas tiesību aizsardzības speciālisti spēj adekvāti aizsargāt sabiedrību no šiem jaunā veida apdraudējumiem, ir nepieciešams pievērsties visu problēmu lokam, kas saistīts kibernoziegumiem petīšanai. Disertācija ir pirmais šāda rakstura darbs Latvijā. Disertācijā netiek pētīti visi kibernoziegumi, bet tikai viena grupa, kas, autoraprāt, ir uzskatāma par visas kibernoziedzības stūrakmeni, proti, tie ir noziedzīgi nodarījumi pret informācijas sistēmu drošību, kas disertācijā aplūkota kā vispārējās drošības neatņemama sastāvdaļa.

---

8 Anarchy cookbook version 2000, [b.i.] p.53

9 2003 CSI/FBI Computer Crime and Security Survey p.8

10 2003 Australian Computer crime and security survey

Pētījuma uzdevums ir teorētiski analizēt un pamatot jaunā fenomena- kibernoziegumi jēdzienu, šo noziedzīgo nodarījumu sastāvu, īpaši pievēršoties noziedzīgu nodarījumu pret informācijas sistēmu drošību sastāva analīzei. Disertācijā teorētiskā līmenī analizētas šo nodarījumu klasifikācijas problēmas pēc grupas un tiešā apdraudējuma objekta. Īpaši liela vērība ir veltīta objektīvās puses elementu analīzei. Kibernoziegumus var izdarīt tikai ar darbību, tāpēc pētījumā plaši analizēti iespējamo darbību veidi, ko personas var izmantot apdraudējumu veikšanai. Tā kā viens no visizplatītākajiem kibernoziegumiem ir patvaļīga piekļūšana informācijas sistēmai, tad īpaša vērība pievērsta tieši patvaļīgas piekļuves satura pētīšanai. Pētījumā ir dota arī Krimināllikuma 241- 245. pantā ietverto noziedzīgo nodarījumu analīze, un, tā kā ir sagatavoti būtiski labojumi iepriekšminēto pantu redakcijām, tad pētījumā dota šo jauno grozījumu krimināltiesiskais raksturojums. Pamatojoties uz pētījumā iegūtajām atziņām, ir izvirzītas tēzes aizstāvēšanai.

## I nodaļa Kibernozieguma jēdziens

### 1. Kriminālatbildības jēdziens

Personu atbildības tiesiskā izpausme vienmēr ir bijusi un paliek juridiskā atbildība par likumpārkāpumu.[11]P. Pustorosļevs raksta, ka „..jebkurš noziegums ir vispirms tiesiska pienākuma neizpilde, kuram piemīt visas tiesībpārkāpuma pazīmes"[12]. Viņš uzskatīja, ka tiesiski pienākumi iedalāmi :1) „pozitīvā pienākumā", kura būtība ir prasībā, lai persona izpildītu zināmu ārēju darbību (pavēli); 2) „negatīvā pienākumā", kura būtība ir izteikta sentencē „tuvākam ir vajadzība dzīvot- neslepkavo, cilvēkam ir vajadzība uz īpašumu – nezodz."[13] Tādējādi kriminālatbildība parasti iestājas par „negatīvā" pienākuma nepildīšanu. Juridiskā atbildība pamatojas tikai uz likumu vai likumpamatotu normatīvo aktu. Juridiskā atbildība ir īpaša jauna tiesiskā attiecība (saistība), kura rodas no likuma (tiesību normu) pārkāpuma, kas pārkāpējam izpaužas soda, kompensācijas vai

---

[11] Лейст И. Понятие ответсвенности в теории права,// Вестник Московского Университета 1/1994 с. 11 Право с 2

[12] Анализ о преступлении. Исследование П.П. Пусторослева. Москва: Университетская типография, 1892., с.2

[13] Ibid, П.П.Пусторослев.,с.107

citādā personisko mantisko vai nemantisko ierobežojumu formā un kuras piespiedu izpilde var tikt nodrošināta ar valsts piespiedu līdzekļiem[14]. Juridisko atbildību no citiem atbildības veidiem nošķir šādas pazīmes:

1. Tiesībpārkāpums.

2. Valsts piespiedu iedarbība uz tiesībpārkāpēju.

Kā norāda V. Sinaiskis, tad pastāvošās mācības par civiltiesisko pārkāpumu būvētas uz krasu pretstatījumu krimināļajam tiesību pārkāpumam. Tāds iedalījums norādīja, ka romiešu tiesībās pastāvēja uzskats: var pastāvēt divas taisnības - „krimināltiesiskā un otra civiltiesiskā taisnība" vai attiecīgi „krimināļā netaisnība un civilā netaisnība" [15]. Šis iedalījums atbilst tam, kā Romā dalīja tiesību pārkāpumus, proti, *crimina*[16] un *delicta*. Kā norāda P. Lejiņš, tad atšķirība starp civiltiesisko un krimināltiesisko pārkāpumu ir apstāklī, ka valsts, izvērtējot nodarījumu pēc sekām, tam noteikusi krimināltiesisku statusu.[17]

Krimināltiesības kā publisko tiesību daļa regulē zināmas robežas attiecībās starp valsti un indivīdu un valsti.[18] Šīs zināmās robežas ir saistītas galvenokārt ar tiesiskās kārtības traucējumiem. Ne katrs tiesībpārkāpums, kaut arī tas aizskar personu likumīgās intereses, ir krimināltiesiskā regulējuma priekšmets. Noziedzīgs no ārējās puses ir tāds nodarījums, kuru aizliedz likums, piedraudot ar krimināļsodu.[19] Līdz ar to var secināt, ka krimināltiesības ir mehānisms sociālās kontroles nodrošināšanai sabiedrībā. To pienākums ir skaidri, precīzi noteikt tās robežas, kad personas uzvedība ir aizliedzama vai ierobežojama ar krimināļsoda piedraudējumu.

Lai sauktu personu pie krimināļatbildības, ir jābūt stingram juridiskam pamatam.

Latvijā šīs robežas precīzi noteic Krimināllikuma 1. pants „Krimināļatbildības pamats":

---

[14] Bitāns A. Civiltiesiskā atbildība un tās veidi. Rīga: AGB, 1997., 24. lpp.

[15] Sinaiskis V. Civiltiesības I. Rīga: A/S "Valters un Rapa",1935., 45. lpp.

[16] *Crimina*- noziegums, kad valsts kā publiskais tiesību subjekts noteica striktu atbildību.

[17] Docents Lejiņš P. Krimināltiesības Rīga: [b.i.]1940., 61. lpp.

[18] Mincs P. Krimināltiesību kurss. Vispārējā daļa. Otrs pārstrādātais un papildinātais izdevums. Rīga: Autora izdevums, 1934., 1.lpp.

[19] Turpat, Mincs P., 59.lpp.

*(1) Pie krimināllatbildības saucama un sodāma tikai tāda persona, kura ir vainīga noziedzīga nodarījuma izdarīšanā, tas ir, kura ar nodomu (tīši) vai aiz neuzmanības izdarījusi šajā likumā paredzētu nodarījumu, kam ir visas noziedzīga nodarījuma sastāva pazīmes.*

(2) Nevienu nedrīkst atzīt par vainīgu noziedzīga nodarījuma izdarīšanā un nevienam nedrīkst uzlikt krimināsodu citādi kā ar tiesas spriedumu un saskaņā ar likumu.

Krimināllikums satur sevī **abstraktu noteikumu,** kuru piemēro konkrētam noziedzīgam nodarījumam.[20] Līdzīgu secinājumu izsaka japāņu tiesībzinātnieks Š. Dando[21]un A. Traiņins[22], ka„.. nozieguma vispārīgais jēdziens kā „abstrakcija" nerada un nevar radīt krimināltbildību. Tās galvenais uzdevums ir norādīt uz nodarījuma vispārīgām kopīgām pazīmēm.

Aizlieguma aprakstam un sodam ir jābūt tieši paredzētam spēkā esošā krimināllikumā- *de lege lata*[23] princips. *De lege lata* princips cieši sasaucas ar *nullum crimen sine poena, nulla poena sine lege*[24]. Ja aizliegums nav ietverts spēkā esošā krimināllikumā un par to nav noteikts sods, tad šāda prettiesiska darbība, kaut arī tā nākotnē varētu kļūt sodāma *de lege ferranda*, nevar tikt atzīta par noziedzīgu nodarījumu tagadnē. Nevar piekrist P. Lejiņa viedoklim, ka valsts aizliegums nav kritērijs, lai noteiktu, kas ir noziegums, jo, pēc viņa domām, " noziegums ir tas, kas par tādu atzīstams pēc satura, t.i., kas ir sevišķi kaitīgs sabiedrībai, un atbildi par to, kas ir un kas nav kaitīgs, dod tautas izjūta".[25] Jebkurā gadījumā kādam šī tauta būtu jāorganizē, respektīvi, jārada institūcija, kas realizētu šo tautas gribu, un demokrātiskā sabiedrībā tā var būt tautas vēlēta pārstāvniecība, kurai tiek deleģēta ekskluzīva kompetence tautas vārdā padarīt to vai citu tiesību pārkāpumu par noziedzīgu nodarījumu. Pareizi norāda A. Krugļevskis: „.. ja iedzīvotājiem būtu laupīta iespēja iepriekš zināt, kas atļauts un, kas noliegts, tie sāk dzīvot bailēs. Tas

---

20 Turpat, Mincs P., 15.lpp.

21 The Criminal law of Japan The General part by Shigemitsu Dando, translated by B. J. George, Rothman & Co, Littleton, Colorado 80127, 1997., p.1

22 Курс Советского Уголовного права. Общая часть. Т.1. Издательство Ленинградского Университета, 1968., с. 254

23 Romiešu tiesības apzīmē, pamatojoties uz spēkā esošu (pastāvošu) likumu. Čerfase L. Latīņu valodas spārnotie teicieni. Rīga: Zinātne, 1992., 74. lpp.

24 Romiešu tiesību formula "Nav noziegums bez soda, nav soda bez likuma" Čerfase L. "Latīņu valodas spārnotie teicieni" Rīga, Zinātne, 1992., 180. lpp.

25 Turpat, Docents Lejiņš P., 36 lpp.

var pārvērsties par politiskās izrēķināšanās ieroci."[26] Līdz ar to tautas taisnīguma izjūta nevis kalpotu sabiedrības demokrātijas un cilvēku dzīves līmeņa celšanai, bet gluži otrādi- kļūtu var vispārēju sabiedrības attīstības bremzējošu faktoru un cilvēku iebaidīšanas līdzekli. Tāpēc nenoliedzami, ka par noziedzīgu nodarījumu var tikt atzīta uzvedība, ko likumdevējs aizliedzis vai ierobežojis ar soda piedraudējumu.

*De lege lata* princips neatļauj saukt pie krimināltbildības personas par tradicionāliem noziedzīgiem nodarījumiem, kuri veikti, izmantojot kibertelpas[27] vai e- vides mediju, kur darbības nav saistītas ar ietekmi uz konkrētu personu, bet gan ar datorsistēmā vai datortīklā saglabātu vai pārraidītu datu manipulāciju. Krimināltbildība ir smagākais atbildības veids, ko valsts nosaka par personu prettiesiskām darbībām vai bezdarbību, kas izdarīta tīši ar tiešu nodomu (*dolus directus)* vai netiešu nodomu (*dolus eventualis*), vai aiz neuzmanības. Krimināltbildības piemērošanā jāievēro subsidiaritātes[28] princips. Tai jābūt tikai kā galējam ietekmēšanas līdzeklim, ja citi ietekmēšanas līdzekļi nav bijuši pietiekami efektīvi.[29] Tātad krimināltbildības pamats ir krimināli sodāms nodarījums- krimināllikuma pantā aprakstītā dispozīcija, noteikums, par kura pārkāpšanu paredzēts kriminālsods.

U. Krastiņš norāda, ka krimināltbildība ir personai saskaņā ar likumu valsts vārdā tiesas uzlikts piespiedu pasākums par izdarīto noziedzīgo nodarījumu izciest sodu, kas saistīts ar viņas personiskās brīvības, atsevišķu tiesību vai mantiska rakstura ierobežojumiem.[30] Līdzīgs viedoklis ir plaši sastopams juridiskajā literatūrā. Tomēr ir sastopams arī cits viedoklis, ka krimināltiesības nosaka arī „pozitīvo krimināltbildību"[31], kas izpaužas personas atturēšanā no noziedzīgu nodarījumu veikšanas, tādējādi nodrošinot krimināllikumā noteikto pozitīvo

---

26 Profesors Krugļevskis A. "Princips "nulla poena sine lege" un tā nozīme krimināltiesībās. Rīga: [b.i.] 1937., 208. lpp.

27 Terminu izmanto, lai apzīmētu datoru tīklā (t. sk. internetā) veidoto diskrēto pasaules modeli (virtuālo realitāti). Terminu radījis V.Gibsons savā romānā "Neuromancer" http://www.termini.lv

28 Kibernoziegumu konvencijas kontekstā tas nosaukts par nepieciešamības principu. *Principle of necessity*.

29 Council of Europe Legal affairs Computer related crime pefased by August Bequai, European by European Committee on Crime Problems, Strasbour 1990. Recommendation No(89)9 on computer related crime and final report of the European Committee on Crime Problems, p. 24

30 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 6. lpp.

31 Кудрявцев В.Н. Закон, поведение, ответственность. Москва: 1986; Тарбагаев А.Н. Понятие и цели ответственности. Красноярск, 1996. с. 21-366 . Citēts no Курс Уголовного права. Общая часть. Том 1: Учение о преступлении. Под ред. Н.Ф. Кузнецовой и И.М. Тяжковой.Москва: Зеркало,1999, с.192

uzvedību. Jebkura atbildība var tikt noteikta tikai par konkrētu tiesību normu pārkāpumu, un tā nekad nevar būt pozitīva. Tomēr nevar arī noliegt, ka krimināLatbildības mērķis ir nodrošināt stāvokli, ka sabiedrība spēj pilnvērtīgi attīstīt indivīda darbībai nepieciešamās civilās, komerciālās un arī citu tiesību garantijas. Lai to veiktu, krimināltiesības nosaka standartus, kas ievērojami ietekmē sabiedrības vērtējumu par to, kas ir labs un kas slikts.[32] Šī vadlīnija ir attīstījusies un pilnveidojusies vēsturiski. Šādas nostādnes mēs varam sastapt gan Hamurapi, gan arī romiešu tiesību normās.[33] Sakotnēji krievu juridiskajā literatūrā nozieguma vietā lietoja iepriekšminēto terminu "krimināLā netaisnība". Ar to apzīmēja apdraudējumu, kas tieši vērsts uz pašu tiesību personisko vai lietisko objektu.[34]

## 2. Noziedzīga nodarījuma jēdziens

Krievijā termins „noziegums", ar kuru sāka apzīmēt ikvienu krimināli sodāmu uzvedību, izplatījās tikai Pētera I valdīšanas laikā. Šī termina izcelsme ir līdzīga terminam "*crime*" - angļu un franču valodā, *Verbrechen*- vācu valodā utt. Literatūrā ar šiem terminiem parasti apzīmēja uzvedību, kas iziet ārpus pieļautajām robežām.[35]

Juridiskajā literatūrā ir plaši pārstāvēts viedoklis, ka nozieguma jēdziens tāpat kā tiesības attīstās atbilstoši sociālās realitātes prasībām.[36] Šāds viedoklis ir pamatots, jo noziedzīgi nodarījumi būtībā ir jebkuri indivīdu nodarījumi, kas ir pretrunā ar sabiedrībā esošajām tradīcijām, parašām un citiem vispāratzītiem uzvedības noteikumiem un būtiski ietekmē sabiedrības drošību.

Krievu zinātnieks N. Tagancevs norāda, lai darbību atzītu par noziegumu, ir nepieciešamas trīs pazīmes: 1) ar likumu noformēta juridiska attiecība, jo pretējā gadījumā nevar pastāvēt nozieguma objekts. Tāpēc par noziegumu nevar atzīt savu

---

[32] Clarkson C.M.V. Understanding criminal law Third ed., London, Sweet& Maxwell, 2001., p.8.;

[33] The Code of Hamurapi. The Avalon Project at Yale Law School www.yale.edu/lawweb/avalon/medieval/hamcode.htm (aplūkots 2003.gada 23. decembrī)

[34] Анализ о преступлении изследование. Изследование П.П.Пусторослева Москва: Университетская типография, 1892.,с.118

[35] Уголовное право Общ. ч. Учебник для вузов.,Москва: ИНФРА· М- НОРМА, 1997.,с 77-78 Par noziegumu vai pārkāpumu atzīstama kā pretlikumīgā darbība, tā arī tās uzvedības, kas aprakstīta likumā kā baiLes no soda, neizpilde. sk.cт.1 Уложения о наказаниях уголовных и исправительных в редакции 1885г.

[36] Уголовное право. Под. ред. Гаухмана, Москва: Юриспруденция, 1999., с. 60

personisko labumu apdraudējumu vai iznīcināšanu, ja netiek pārkāptas citu personu likumīgās intereses; 2) lai pastāvētu noziegums, nepieciešams, lai eksistētu reāla tiesību norma, kas padara attiecīgo interesi, labumu par aizsargājamu; 3) nozieguma esamībai nepieciešams noteiktu, ar likumu aizsargātu interešu reāls apdraudējums, kuram ir krimināpārkāpuma raksturs.[37] Atkarībā no noziedzīgā nodarījuma jēdzienā ietverto pazīmju skaita, teorijā tos iedala formālos, materiālos un materiāli -formālos.

## 2.1. Formālais noziedzīgā nodarījuma jēdziens

Pasaulē krimināltiesību teorijā dominē formālais nozieguma jēdziens. Tas saistīts ar romiešu tiesību lielo ietekmi uz kontinentālās Eiropas un kopējo tiesību sistēmām. Kā norāda profesore S. Brennere, tad, lai gan romāņu –ģermāņu un kopējo tiesību sistēmās ir atšķirīga pieeja juridisko aizliegumu veidošanai, dažādās valstīs un dažādos laikos ir vērojamas arī vairākas svarīgas konsekvences attiecībā uz to, ko valsts nosaka, kāda rīcība ir pasludināma ārpus likuma. Šīs konsekvences izriet no krimināatbildības funkcijas - uzturēt sabiedrībā pienācīgu kārtību.[38]

Formālā nozieguma definīcija izceļ prettiesiskuma un sodāmības pazīmi. Noziedzīgs nodarījums ir nepaklausība kādai tiesiskai normai – aizliedzošai vai pavēlošai. Tas ir vispārējs kritērijs, kuru no tiesiskā viedokļa var attiecināt uz katru noziedzīgu nodarījumu.[39] Tādējādi par noziedzīgu nodarījumu var atzīt tikai prettiesisku, nelikumīgu darbību vai bezdarbību. Piemēram, ASV noziegums (noziedzīgs nodarījums) tiek definēts kā ļaunums, ko Kongress vai štata likumdošana atzinusi par noziegumu vai krimināpārkāpumu.[40] Līdzīga noziedzīga nodarījuma definīcijas interpretācija plaši izplatīta arī juridiskajā literatūrā un lietota daudzu valstu krimināltiesību doktrīnās.

---

[37] Таганцев Н.С. Курсь Русского уголовного права. Часть общая книга 1-я. Учение о преступлении. Санкт-Перербургъ: [b.i]1874.,c.181

[38] Brennere V.S. Kibernoziegumi un tradicionālie noziedzīgie nodarījumi: juridisko problēmu analīze, Likums un tiesības,2002, 4.sēj.,nr.9 (37) 270.lpp. Krimināllikuma mērķis ir definēt sociāli nepieņemamu rīcību un ierobežot rīcību tiktāl, ciktāl tas lietderīgi un pieņemami no sociālā viedokļa. ; Simester A.P. , G.R. Sullivan Criminal law theory and doctrine. Hart publishing , Oxford- Portland Oregon, 2000, p.1

[39] Turpat, Mincs P., 59.lpp.

[40] The electric law library's legal lexicon on crime // http://www.lectlaw.com/def/c330.htm ; [b.a.] Criminal law in England and Wales // http://www.luiss.it/erasmuslaw/uk/lngh8.html#p1 (aplūkots 2003.gada 11.novembrī)

Nosakot formālā noziedzīga nodarījuma definīcijā prettiesiskuma pazīmes prioritāti, mēs atzīstam, ka šāds nodarījuma jēdziens dod krimināltiesisku konstitucionālu garantiju, ka personu nevar saukt pie atbildības par kriminālliku mā neparedzētu darbību vai bezdarbību. Šī krimināltiesiskā konstitucionālā principa garantija izpaužas personu tiesību un brīvību aizsardzībā.[41]

Galvenā formālā nozieguma jēdziena būtība ietverta romiešu tiesību principā "*nullum crimen sine lege*". Šis princips noteic, ka par noziedzīgu nodarījumu var runāt tikai tad, „ja aizrādījums formulēts no varas ;1) tādā veidā nedrīkst uzvesties; 2) kas tā uzvedīsies, saņems sodu".[42] No šī pamatprincipa mēs var atvasināt vairākus apakšprincipus:

1. *Sine lege* - nozīmē, ka atbildība var iestāties tikai uz nodarījuma izdarīšanas brīdī spēkā esoša likuma pamata. Krievu kriminālists P. Osipovs pareizi norāda, ka noziegums ir valstij bīstams noziedzīgs nodarījums. Tāpēc tikai valsts likumdevēja personā var dot tam attiecīgu juridisku novērtējumu.[43]

Ar terminu „likums" vairākas valstīs apzīmē ne tikai parlamenta pieņemtu likumu, bet šajā kategorijā var ietilpt arī normatīvie akti, ko pieņem valdības. Piemēram, Dānijā[44] šādus normatīvus aktus var pieņemt ne tikai ministrija, bet arī zemāki valdības departamenti. Vairākās valstīs izšķiroša nozīme ir kriminālliku ma "*ratio legis*" tulkošanai, kā arī tiesu precedentiem.

Piemēram, Šveices Sodu likuma 251. pants neparedzēja atbildību tieši par elektronisku datu viltošanu, bet 1990.gadā Šveices Federālā tiesa, piemērojot šo normu konkrētā lietā, kas saistīta ar datordatu viltošanu, atzina, ka termins "dokuments" ietver jebkura veida dokumentus, tai skaitā arī tādus, kas izgatavoti ar elektronisko ierīču palīdzību, un par šādu dokumentu viltošanu jāparedz krimināl atbildība.[45]

2. *De lege lata* – ja persona izdara pārkāpumu, kura apraksts precīzi burts burtā nesakrīt ar likumā ietverto noziedzīgā nodarījuma aprakstu, persona ir atbrīvojama

---

41 Егоров В.С. Понятие состава преступления в уголовном праве. Уч.пособие. Москва: Московский психолого социальный институт, 2001.,с.6

42 Turpat, Docents Lejiņš P., 36. lpp.

43 Советское Уголовное право. Общая часть. Москва: Юридическая литература, 1977., с. 68

44 Criminal law in Denmark by Lars Bo Langsted, Van Greve, Peter Garde. Kluwer Law International. The Hague-London-Boston, 1998., pp.55-56

45 Recommendation No R (89)9 on computer related crime report prepared by proffessor Henrik W.K. Kaspersen Computer/law Institute Amsterdam February 1997 CDPC (97)5; PC-CY (97(5) p.91

no atbildības. A. Piontkovskis[46], kritizējot iepriekšminēto principu, min piemēru, ka Vācijas tiesa atteicās saukt pie atbildības personu par elektroenerģijas zādzību tikai tāpēc, ka atbildība par šādu nodarījumu nebija paredzēta Vācijas likumā. Tikai pēc tam, kad Vācijas parlaments pieņēma speciālu likumu un paredzēja krimināLatbildību par elektroenerģijas nelikumīgu piesavināšanos, turpmāk bija iespējams personas saukt pie krimināLatbildības. Jāpiezīmē, ka analoga situācija bija sastopama arī Latvijas tiesu praksē, kad Augstākās tiesas Senāts[47] atzina, ka nav pamata saukt personu pie krimināLatbildības par krāpšanu telekomunikācijās, jo atbildību par šādām darbībām tieši neparedz Krimināllikums.

3. *Nulla poena* – minētais princips nosaka, ka likumam, ar kuru noteikts sods, jābūt skaidri un precīzi formulētam. A. Krugļevskis pamatoti norāda, ka *nulla poena* mērķis ir aizsargāt indivīdu no sabiedrības.[48] Respektējot šo principu, jāatzīst, ka nav pieļaujama Krimināllikuma tulkošana plašāk par tajā ietverto lingvistisko tekstu. Tomēr ir sastopami arī nelieli izņēmumi.

Piemēram, Dānijas Kriminālkodeksa 1.pants atļauj tiesai piemērot ***analoģiju*** pilnīgi salīdzināmos likumos. Dānijā to sauc par *complete statutory analogy*.[49] Analoģiju var piemērot, tulkojot radniecīgi tuvus terminus, bet nekādā gadījumā to nevar attiecināt uz sodu.

Latvijas Sodu likuma 1. pants noteica, „..ka par noziedzīgu atzīstams nodarījums, kurš tā izdarīšanas laikā noliegts ar soda piedraudējumu".[50] Šāds nozieguma jēdziens ir sastopams lielākajā daļā attīstītāko Eiropas valstu krimināllikumu, piemēram, Zviedrijas Sodu likuma 1. pants: "Noziegums ir nodarījums, kas paredzēts likumā vai citā normatīvā aktā ar soda piedraudējumu."

4. Retroaktivitātes princips jeb likuma atpakaļejošs spēks[51]. Saskaņā ar *nullum crimen* principu krimināLatbildība iestājas tikai tad, ja darbība atzīta par noziedzīgu ar soda piedraudējumu jau pirms nodarījuma izdarīšanas. Minētais

---

[46] Пионтковский А.А. Учение о преступлеплении по советскому уголовному праву.: Юридическая литература, 1961,с. 62

[47] Ķinis U. Kibernoziegumi un kriminālprocess. Latvijas Vēstnesis, 2001.gada .20. un 28.februāris.

[48] Turpat, Profesors Krugļevskis A., 203.lpp.

[49] Criminal law in Denmark by Lars Bo Langsted, Van Greve, Peter Garde. Kluwer Law International. The Hague-London-Boston, 1998., pp.58-59

[50] Sodu likums ar komentāriem. Otrais izd. P. Minca un J. Lauva red. Rīga: 1938., Valsts tipogrāfijas izdevums 5.lpp.

[51] Krastiņš U., Liholaja V., Niedre A. Krimināltiesības. Rīga-:TNA, 1999., 16. lpp.; Clarkson C.M.V. Understanding Criminal law. Third edition. London- Swet & Maxwell, 2001., p.14; Criminal law in Denmark by Lars Bo Langsted, Van Greve, Peter Garde. Kluwer Law International. The Hague-London- Boston, 1998., pp.42-43; Criminal law in Denmark by Lars Bo Langsted, Van Greve, Peter Garde. Kluwer Law International. The Hague-London- Boston, 1998., pp.58-59; Курс Уголовного права. Общая часть. Под ред. Н.Ф. Кузнецовой и И.М. Тяжковой. Москва: Зеркало, 1999.,С.192 u.c.

princips ir ietverts arī Krimināllikuma 5. pantā. Saskaņā ar Krimināllikuma 5.panta 3.daļas likumam, kas atzīst nodarījumu par sodāmu, pastiprina sodu vai ir citādi nelabvēlīgs personai, atpakaļejoša spēka nav.

Retroaktivitāte Latvijas krimināltiesībās ir pieļaujama tikai tad, ja tā dekriminalizē noziedzīgo nodarījumu vai mīkstina sodu, vai ir citādi labvēlīga personai. Retroaktivitātes princips ietverts daudzu valstu krimināl kodeksos, kā, piemēram, Vācijas Krimināl kodeksa 1.pantā: "Nodarījums ir sodāms tikai tad, ja sods par to bija paredzēts pirms tā izdarīšanas," analoga definīcija ietverta arī Spānijas, Šveices, Austrijas, Dānijas, Gruzijas, Japānas, Holandes, Beļģijas, Francijas un citu valstu krimināl kodeksos. Kaut arī ASV nav vienota krimināl kodeksa, tomēr arī ASV paraugkrimināl kodeksā ir nostiprināts princips "*nullum crimen sine lege*".[52] Darbība nav atzīstama par noziedzīgu, ja to par noziegumu vai pārkāpumu uz nozieguma izdarīšanas dienu neatzīst šis kodekss vai cits attiecīgā štata likums. Jaunākos ASV autoru[53] darbos par noziegumu atzīst tādu uzvedību, kas tieši, precīzi aprakstīta likumā. Tas nozīmē, ka likumā precīzi ir jābūt noteiktam, par ko iestājas atbildība, un precīzi jānosaka sods. Dānijas Krimināl kodeksa 1.pantā ir ietverts princips „*nulla poena sine lege poenali*"- tikai „likumā" paredzētas darbības ir sodāmas. Ar terminu „likumā" saprotamas precīzas noziedzīga nodarījuma robežas.

Nozieguma formālā definīcija nav visaptveroša. To nereti kritizē ne tikai bijušās PSRS, bet arī daži citu valstu krimināltiesību speciālisti, saucot to par "antizinātnisku tukšu tautoloģiju"[54]. Tomēr, neskatoties uz šo kritiku, minētā pieeja ir vērtējama pozitīvi, jo tā ir nodrošinājusi savu valstu iedzīvotājiem konstitucionālo garantiju, ka nevienu nevar saukt pie atbildības bez tiesiska pamata, un līdz ar to pasargājusi sabiedrību no valsts varas patvaļas. Principa „*nullum crimen sine lege*" rakstura un pazīmju kopsavilkumu precīzi izteicis P. Lejiņš : "*Nullum crimen sine lege* raksturs noteic: 1)ierobežotas likuma tulkošanas iespējas;

---

[52] Уголовное право зарубежных стран. Часть общая. Москва: Издательство Омега-Л, 2003., с.121

[53] Law and disorder: Criminal Justice in America (ed.By Bruce Jackson. University of Illionois Press., 1984.p.11 citēts no Уголовное право зарубежных стран. Часть общая. Издательство Омега-Л, Москва, 2003., С.121

[54] Parker H. The limits of criminal sanction.-Stanford (Cal), 1968.p.5 citēts no Уголовное право зарубежных стран. Часть общая. Издательство Омега-Л, Москва, 2003., С.122; Курс Советского Уголовного права в шести томах , том. II. Общая часть под. ред.Пионтковсковского А.А. Москва: Наука, 1970.,с. 51;

2) nepielaiž analoģiju; 3) Soda likumam nav atpakaļ ejošas nozīmes; 4) tiesnesis nav tiesību radītājs."[55]

## 2.2. Materiālais noziedzīgā nodarījuma jēdziens

Juridiskajā literatūrā plaši ir pārstāvēts viedoklis, piem. ,P. Mincs, H. Meijers[56], ka noziegums vienmēr iemieso kaitējumu tiesiski pamatotām interesēm. Tāpēc valstij ir pienākums kriminalizēt tikai tās darbības, kas būtiski apdraud sabiedrisko kārtību un personu drošību. Nosakot šo darbību aizliegumu vai ierobežojumu ar soda piedraudējumu un iekļaujot konkrētus noziedzīgus nodarījumus krimināllikuma sevišķā daļā, valsts ir novērtējuši šo darbību kaitīgumu un tādējādi materializējusi[57] to saturu. Analogu viedokli pauž arī Š. Dando, A.Simesters un G. Sulivans un citi[58], norādot, ka nozieguma specifiskie materiālie elementi ir cieši saistīti ar konkrētas darbības atzīšanu par nelikumīgu un sodāmu. Pasaulē ir vairāki gadījumi, kad arī daži Rietumu krimināltiesību teorētiķi mēģināja akcentēt noziedzīgā nodarījuma materiālo pazīmi, piemēram, G. Saiks definēja noziegumu kā sabiedrībai kaitīgu nodarījumu, kas ir pretrunā ar sabiedrības labklājību, bet U. Rekliss kā sabiedrības uzvedības normu un sabiedrības garīgo vērtību pārkāpumu[59]. Arī Latvijas krimināltiesību zinātnē[60] ir izteikts viedoklis, ka nozieguma materiālo raksturu noteic princips *„nullum crimen sine poena-* nav nozieguma bez soda, kas izpaužas tā, ka neviens nodarījums, ko sabiedrība izjūt kā noziedzīgu, nedrīkst palikt bez soda. P. Lejiņš, definējot šī principa pazīmes, norāda, ka tā piemērošanu krimināltiesībās raksturo: 1) paplašināta krimināllikuma tulkošanas iespējamība; 2) analoģijas pieļaujamība; 3) Soda likumam var būt atpakaļejošs spēks; 4) tiesnesis ir tiesību radītājs.[61]Tomēr šī teorija atbalstu neguva, jo radās bažas, ka tā valsts ir spējīga realizēt patvaļu pret saviem iedzīvotājiem krimināltiesību piemērošanas jomā. Pareizi norāda A. Krugļevskis, ka analoģijas piemērošana rada kriminālo

---

55 Turpat, Docents Lejiņš P., 39. lpp.

56 Ibid., Shigemitsu Dando, p. 25.

57 Turpat, Mincs P., 59.lpp.

58 Ibid, Shigemitsu Dando, p.57.; Ibid., A.P.Simester, G.R. Sullivan.., p.21.

59 Уголовное право зарубежных стран. Часть общая. Москва: Издательство Омега-Л, 2003., с.122

60 Turpat,Docents Lejiņš P., 36. lpp.

61 Turpat, Docents Lejiņš P., 39.lpp.

normu nenoteiktību: 1) nenoteiktība tiesību prasībās; 2) nenoteiktība tiesību spriedienā[62], līdz ar to tā var pārvērsties par varas patvaļu. Iepriekšminētais tieši parāda šī principa piemērošanas reakcionāro būtību, radot tiesību tiesnesim izlemt, kāda uzvedība ir un kāda nav sodāma, piemērojot likuma analoģiju un paplašināti tulkojot likumus, ko plaši praktizēja PSRS krimināltiesībās laikā no 1920. līdz 1950. gadam.

Pēc Latvijas Republikas okupācijas un inkorporācijas PSRS sastāvā, 1940.gada 25. novembra Latvijas PSR Tautas Komisāru padomes lēmuma 2.p. noteica, ka ".. saukšana pie kriminālatbildības par noziedzīgiem nodarījumiem, kas izdarīti Latvijas teritorijā, izdarāma saskaņā ar KPFSR kodekiem".[63] KPFSR Krimināl kodeka 6. pants noteica: "Par sabiedriski bīstamu atzīstama ikviena darbība vai bezdarbība, kas vērsta pret Padomju iekārtu vai pārkāpj tiesisko kārtību, kuru Strādnieku Zemnieku vara nodibinājusi pārejas laikam uz komunistisko iekārtu". Komentējot šo pantu, toreizējais PSRS Augstākās tiesas priekšsēdētājs I. Goļakovs norādīja, ka minētais pants pretstatā ārzemju kriminālajai likumdošanai, kas definē noziegumu formāli, t.i., kā darbību, par kuru likumā noteikts sods, nepaskaidrojot par kādu darbību īsti ir runa, dod nozieguma materiālo definīciju, norādot nozieguma konkrētas pazīmes kā darbībai, tā bezdarbībai, kas vērsta pret padomju iekārtu vai tiesisko kārtību, kāda noteikta pārejas laikam uz komunistisko iekārtu.

Līdzīgs viedoklis bija plaši pārstāvēts tā laika juridiskajā literatūrā. Piemēram, N. Kuzņecova[64], A. Piotkovskis[65] un citi pamatoja materiālās noziedzīgā nodarījuma teorijas nepieciešamību, lai atklātu krimināl atbildības šķirisko un politisko raksturu, un asi vērsās pret rietumu valstīs pastāvošo formālā noziedzīgā nodarījuma doktrīnu. A. Piontkovskis[66] rakstīja, ka„.. šāda definīcija ir formāla un neatklāj paša noziedzīgā nodarījuma būtību, bet tikai pamato apgalvojumu, ka noziegums ir tad, ja to par tādu atzīst likumdevējs", [67] un secina, ka atbildi uz šo jautājumu var dot tikai **materiāla** nozieguma jēdziena noteikšana, kas cieši saistīts ar politiskā režīma varas nostiprināšanu, proti, saistot to ar valsts šķirisko būtību un šķiru cīņu. Šādu viedokli atbalstīja daudzi PSRS kriminālisti, piemēram, V. Prohorovs P. Osipovs, N.Kuzņecova, M. Tjažkova, N. Beļajevs u.c.[68] Pretstatā

---

[62] Turpat, Profesors Krugļevskis A., 223.lpp.

[63] KPFSR Krimināl kodeks. Komentārs I. T. Goļakova red.- Rīga: Grāmatu apgāds, 1946., 3.lpp.

[64] Советское уголовное право. Общая ч. Москва: изд. Московского университета, 1981., с. 67

[65] Пионтковский А.А. Учение о преступлеплении по советскому уголовному праву. Москва: Юридическая литература, 1961,с. 25

[66] Ibid., А.Пионтковский с. 26

[67] Ibid., А.Пионтковский , с. 26

[68] Прохоров В.С. Преступление и ответственность Ленинград: изд.-во Ленинградского университета.,1984.,с.7; Советское уголовное право. Общая часть. Москва: Юридическая литература,1977.,Советское Уголовное право под.ред. Н.Ф. Кузнецова Общая ч. Москва- изд.-во Московского университета, 1981, с. 67; Курс Советского уголовного права. ч. Общая т.1. Ленинград: изд-во Ленинградского университета,1968, с.147

PSRS krimināltiesību doktrīnai lielākā daļa Rietumu un Latvijas Republikas krimināltiesību teorētiķi noziedzīga nodarījuma materiālo pazīmi vērtē tikai kā formālās pazīmes neatņemamu sastāvdaļu un tāpēc neatbalsta specifisku noziedzīga nodarījuma materializācijas teoriju.

Krievijas juridiskajā literatūrā[69] joprojām ir sastopams viedoklis, kas noziedzīgā nodarījuma materiālās pazīmes izcelšana bija vēsturiska nepieciešamība. Trūkumi šādai pieejai ir acīm redzami, jo, definējot noziegumu kā „.. **sabiedriski** bīstamu darbību vai bezdarbību"[70], tā laika tiesībzinātnieki apzināti izvairījās no šo darbību prettiesiskuma novērtēšanas[71], jo prettiesiska var būt tikai tāda darbība, ko likumdevējs aizliedzis ar soda piedraudējumu.

Šīm bažām bija reāls pamats, jo atteikšanās no nozieguma formālā jēdziena deva iespēju PSRS krimināltiesībās piemērot vienu no visreakcionārākiem krimināllikuma piemērošanas instrumentiem, t.i., analoģiju. A. Piontkovskis, norādīja, ka ".. analoģija deva lielu impulsu padomju krimināltiesību attīstībā, jo tādā veidā tika izveidoti jauni kriminālnoziegumu sastāvi, kas vēlāk tika iekļauti krimināllikumā"[72]. Tas deva iespēju PSRS legalizēt represijas pret savas valsts iedzīvotājiem un okupēto teritoriju iedzīvotājiem. Šodien lielākā daļā pasaules valstu[73] savās krimināltiesību doktrīnās par svarīgāko krimināltiesiskās regulēšanas principu atzīst likumības principu un nepieļauj likuma piemērošanu pēc analoģijas.

Juridiskajā literatūrā autori, piemēram, S. Domatins, V. Prohorovs, V. Kudrjavcevs un citi[74], atbalsta viedokli, ka „...noziegums ir valstij bīstama nodarījuma juridiskais novērtējums"[75], kas arī nosaka nozieguma materiālo

---

[69] Уголовное право. Общая часть. Под ред. З.А.Казаченко и А. Незнамова. Москва: Инфра· М-Норма, 1997. с. 91

[70] Ibid., Пионтковский А.А., с. 26

[71] Уголовное право. Общая часть под. ред. Л.Д. Гаухмана. Москва: Юриспруденция, 1999, с.61

[72] Ibid Пионтковский А.А., с. 51

[73] Ķīnas TR krimināltiesībās ilgu laiku tika atļauta likuma analoģijas piemērošana. Piem., Ķīnas 1979.gada KK 12.p. tieši noteica valstij tiesību piemērot krimināllikuma analoģiju par darbībām, kas tieši nebija atzītas par noziegumu un ietvertas Ķīnas KK. Sk. Ахметин Х. М. , Петухов А.А. Современное уголовное законодательство КНР. Уголовный кодекс КНР. Москва: Изд. дом. "Муравей" , 2000., с. 12-17

[74] Уголовное право. История юридической науки. Под. ред. В.Н. Кудрявцева. Москва: Изд. Наука, 1978, с.15; Уголовное право. Под. ред. Л.Д. Гаухмана, изд. "Юриспруденция" , Москва, 1999.,с. 61-68; Прохоров В.С. Преступление и ответственность. Ленинград: Изд. Ленинградского университета. 1984.,с. 7.

[75] Советское уголовное право. Общая ч. , "Юридическая литература", Москва, 1977, с. 66

raksturu. A. Marcevs norāda, ka valstisko bīstamību raksturo apdraudējums, kas nodara vai var nodarīt kaitējumu ar krimināllikumu aizsargātām attiecībām.[76]

Jēdziens „valsts" šajā gadījumā nav tulkojams tikai kā valsts teritorija un valstī pastāvošā sabiedriski politiskā iekārta. Tas ir tulkojams plašāk un ietver sevī: 1) valsts suverenitāti un citas nacionālās intereses; 2) valstī dzīvojošo iedzīvotāju kopumu; 3) tiem piederošo kustamo un nekustamo mantu un to mantiskās un nemantiskās tiesības; 4) valsts teritorijā reģistrēto juridisko personu kustamo, nekustamo mantu un to tiesības.

### 2.3. Materiāli formālais noziedzīgā nodarījuma jēdziens

Staļinisma perioda beigšanās un Rietumu kritika par PSRS krimināło politiku bija pamats jaunas krimināltiesību politikas un krimināltiesību teorijas izstrādāšanā PSRS. Tāpēc PSRS krimināltiesību teorētiķi izstrādāja jaunu noziedzīgā nodarījuma jēdzienu, savienojot formālo nodarījuma jēdzienu ar materiālo noziedzīga nodarījuma jēdzienu, un izstrādāja no šiem diviem komponentiem jaunu materiāli formālo noziedzīga nodarījuma definīciju. Saskaņā ar materiāli formālo definīciju, noziedzīgu nodarījumu juridiskajā literatūrā definēja kā „.. sabiedriski bīstamu nodarījumu (darbību vai bezdarbību), kas paredzēta krimināłkodeksā un par kura izdarīšanu draud krimināłsods" [77]. Šī definīcija tika ietverta 1958.gadā pieņemtajos PSRS un savienoto republiku Krimināłās likumdošanas pamatos un visu PSRS republiku kriminākodeksos. PSRS Krimināłās likumdošanas pamatu 7. pants noteica, ka „.. par noziegumu atzīst šā kodeksa sevišķajā daļā paredzētu sabiedriski bīstamu nodarījumu". Minētā nozieguma definīcija tika izmantota arī 1961.gada LPSR Krimināłkodeksā. Šā likuma 7. pants noteica, ka „.. par noziegumu atzīstams krimināllikumā paredzēts sabiedriski bīstams nodarījums (darbība vai bezdarbība)." Kopš šī laika PSRS krimināltiesībās līdz pat PSRS iziršanai praksē un teorijā izmantoja noziedzīga jēdziena materiāli formālo definīciju.

---

[76] Марцев А. И. Преступление: сущность и содержание. Омск: МВД СССР Омская высшая шлола милиции, 1986.,с.16

[77] Krastiņš U. Mācība par nozieguma sastāvu. Rīga: Zvaigzne ABC, , 1996., 11.lpp.

Tomēr juridiskajā literatūrā plaši bija sastopams viedoklis, ka „.. krimināltiesību teorijā izstrādātais vispārīgs nozieguma jēdziens aptver vispārīgās kopīgās visu noziegumu pazīmes un izsaka nozieguma juridisko un sociāli politisko raksturu un novērtējumu, īpaši uzverot nozieguma bīstamību un prettiesiskumu"[78].

PSRS Krimināl ās likumdošanas pamatu un KPFSR Krimināl kodeksa komentāros īpaši tika uzsvērts, ka ar „sabiedrisko bīstamību" saprot likumā paredzētā noziedzīgā nodarījuma (darbības vai bezdarbības) objektīvu pazīmi nodarīt reālu kaitējumu KPFSR KK 7.p. uzskaitītiem objektiem: 1) padomju sabiedriskā un valsts iekārta, 2) sociālistiskā saimnieciskā sistēma, 3) sociālistiskais īpašums, 4) pilsoņu personu un viņu politiskās, darba, mantiskās un citas tiesības, 5) kā arī citādi sociālistiskās tiesiskās kārtības apdraudējumi.

Noziedzīgā nodarījuma materiāli formālā definīcija bija solis uz priekšu, jo PSRS uz visiem laikiem atteicās no analoģijas piemērošanas krimināltiesībās, aizstājot to ar principu *non lege sine poena*.

Analoģijas piemērošana krimināltiesībās legalizēja PSRS un citām sociālistiskās nometnes satelītvalstīm, sevišķi Āzijā[79] un Āfrikā, tiesību saukt pie krimināl atbildības jebkuru personu, kas pēc valsts varas domām apdraudēja tautas, proletariāta u. c. diktatūru, sociālistisko sistēmu vai citus analogus KPFSR 7. pantā minētos objektus neatkarīgi no tā, vai likums paredzēja krimināl atbildību.

Aizstāvot noziedzīga nodarījuma materiāli formālo definīciju, lielākā daļa tiesībzinātnieku norādīja, ka „.. saskaņā ar padomju krimināl o likumdošanu nodarījuma sabiedriskā bīstamība atkarīga no konkrētiem vēsturiskiem nosacījumiem"[80]. Nav pamata apstrīdēt tēzes daļu, ka darbība vai bezdarbība atzīstama par krimināli sodāmu tad, ja tā kļūst bīstama sabiedrībai un šo bīstamību nenoliedzami noteic vēsturiskā nepieciešamība, tomēr PSRS tiesību teorētiķi šo vēsturisko nepieciešamību saistīja galvenokārt ar politiskiem, bet ne tiesiskiem kritērijiem. G. Novoselovs pareizi norāda, ka, „.. izstrādājot šī tipa jēdzienu, padomju krimināltiesību zinātne nemainīgi pasvītro viedokli, ka materiālā pazīme (sabiedriskā bīstamība) dominē pār formālo pazīmi (prettiesiskumu)"[81].

---

[78] Turpat, Krastiņš U., 12.lpp.

[79] Piemēram, KTR 1979.gada KK atļāva piemērot KK normas par darbībām, kas tieši nebija atzītas par noziedzīgu nodarījumu un nebija iekļautas KK sevišķajā daļā. Sk. Х.М. Ахметшин, А.А. Петухов Современное уголовное законодательство КНР. Уголовный кодекс КНР. Москва- изд.дом " Муравей", 2000, с. 12

[80] Коментарый к Уголовному кодексу РСФСР ,под. ред. Ю.Д. Северина. Москва: Юридическая литература,1980, с. 18; Коментарый к Уголовному кодексу РСФСР ,под. ред. Ю.Д. Северина. Москва: Юридическая литература,1984,с.15

[81] Новоселов Г.П. Учение об обьекте преступлениюю Методологические аспекты. Москва: Норма, ,2001,с.107

Krievijas Federācijas Krimināl kodeksa 14.pants noteic, ka„.. noziegums ir šajā krimināllikumā paredzēts vainojams sabiedriski bīstams nodarījums ar soda piedraudējumu"[82]. Juridiskajā literatūrā, analizējot darbu pie jaunā KF KK, jau sākotnēji bija piedāvājums definēt noziegumu kā „..likumā aizliegtu nodarījumu (darbību vai bezdarbību), kas rada kaitējumu vai kaitējuma apdraudējumu personai, valstij, sabiedrībai". Šīs idejas piekritēji, piem., Z. Ņeznamovs, A. Kazačenko u.c., savu viedokli pamatoja ar to, ka tā tiktu saglabāta juridiskā pēctecība. [83] Turpretim, A. Naumovs un N. Smirnova, A. Želudkovs u.c. neatzīst šo viedokli un uzskata, ka tiesiskā valstī galvenajai noziegumu raksturojošai pazīmei ir jābūt formālai pazīmei, tas ir, prettiesiskuma pazīmei- ar likumu aizliegtai darbībai.[84]

Autoraprāt, atbalstāms ir G. Novoselova viedoklis, ka jautājums par materiālās un formālās pazīmes attiecību, proti, kurai no tām dot prioritāti noziedzīga nodarījuma jēdzienā Krievijas krimināltiesībās, atkarīgs no tā, ko, atmetot mūsu vēsturisko pagātni, vēlēsimies saprast ar abām šīm pazīmēm pēc būtības. Ja no A. Piontkovska noziedzīgā nodarījuma materiālās teorijas izslēdz norādes par šķiru cīņu un sabiedriskās bīstamības politisko saturu, tad var secināt, ka sabiedriskā bīstamība ir prettiesiskuma ārējā izpausmes forma.[85] Tādējādi jāpiekrīt, ka, pētot padomju laika juridiskajā literatūrā doto prettiesiskuma pazīmes saturu, tā traktējums pēc būtības ne ar ko neatšķiras no šodienas Rietumeiropas vai ASV krimināltiesību teorētiķu traktējuma.

Tā, piemēram, Maskavas universitātes krimināltiesību kursā māca, ka **krimināl ais prettiesiskums** ir pazīme, kas sevī ietver: 1) likumības principu; 2) līdzvērtīga tādām sekām kā sabiedriskā bīstamība un vaina; 3) tā adekvāti norāda uz nodarījuma sabiedrisko bīstamību; 4) krimināl ais prettiesiskums ietver sevī nodarījuma sabiedriskās bīstamības novērtējumu, ko noteicis likumdevējs. Kā

---

[82] Полный сборник кодексов Российской Федерации. Москва: Аст, 1999, с. 209

[83] Уголовное право. Общая часть. Учебник для вузов. Москва: Инфра ·М-Норма, 1997, с. 92; Уголовное право. Общая часть. Учебник. Под. ред. Б.В. Эдравомыслова, Москва: МГУ, 1996, с.59

[84] Наумов А.В. Уголовное право. Общая часть: Курс лекций. Москва: БЕК,1996, с.21; Ветров Н.И. Уголовное право. Общая часть. Москва: Юнити, 2003, с. 111; Смирнова Н.Н. Уголовное право. Учебное пособые. Санкт-Петербург: издательство Мыхайлова, 2002,с. 18; Уголовное право .Общая ч. Пособые для подготовки к экзамену. 2-е изд. Москва: Юрайт, 2001,с.28

[85] Курс Советского уголовного права в шести томах. Т.2.Часть общая. Преступление. Под. ред. А.А. Пионтковского. Москва- Наука, 1970, с. 29

jebkurš politisks novērtējums tas var būt neprecīzs un saistīts ar politisko konjunktūru.[86]. Analogs viedoklis tiek atbalstīts arī Rietumvalstu tiesību teorijā[87]. Rietumu krimināltiesību doktrīnā sabiedriskā bīstamība tiek apskatīta kā nodarījuma prettiesiskuma sastāvdaļa. Piemēram, Dž Fletčers norāda, ka„.. noziegumi vienmēr ir publiski tiesību pārkāpumi, jo tie papildus cietušajam nodarītajam kaitējumam, nodara kaitējumu arī tādām sabiedrības interesēm, kā iedzīvotāju labklājība un drošība"[88]. Līdzīgu viedokli atbalsta arī A. Naumovs[89] un daudzi citi autori, norādot, ka likumdevējs, kriminalizējot to vai citu nodarījumu, dod šī nodarījuma juridisko seku novērtēšanu. Kriminalizācija ir likumdevēja atzinums par noteiktu nodarījumu atzīšanu par krimināls odāmiem. Šāda atzinuma pamats ir nodarījuma sabiedriskās bīstamības izvērtēšana. A. Marcevs pamatoti norāda, ka tiesiskās attiecības apdraud visi pārkāpumi, taču ne katrā pārkāpuma gadījumā var runāt par noziedzīgu nodarījumu, tāpēc viņš „sabiedrisko bīstamību" definē kā tādu tiesību pārkāpuma īpašību, kas būtiski un ievērojami apdraud ar krimināllikumu aizsargātās intereses.[90]

Šim viedoklim var tikai piekrist, jo nav iedomājams, ka likumdevējs atzītu par krimināls odāmu uzvedību, kas nerada būtiskus draudus sabiedrības labklājībai un drošībai. Jāpiekrīt tiem autoriem, kas uzskata, ka sabiedriskā bīstamība ir apskatāma tikai kā viena no krimināli prettiesisku darbību raksturojošām pazīmēm. A. Naumovs norāda, ka faktiski starp ASV un Krievijas krimināltiesību doktrīnu nav būtiskas atšķirības, jo nodarījums ir publisks pārkāpums. Ja tas ir publisks, tad tas vienmēr būs saistīts ar sabiedrisko bīstamību. Taču vai katra sabiedriski bīstama darbība ir noziedzīgs nodarījums? Tomēr gan NVS[91] un dažu Viduseiropas[92] valstu krimināllikumos, gan teorijā joprojām par galveno noziedzīgā nodarījuma pazīmi

---

[86] Курс уголовного права. Общая часть. Учебник для вузов. Под. ред Н.Ф. Кузнецовой и И.М. Тяжковой. Москва: Зеркало,1999.с.; 149 Носелов Г.П. Учение об обьекте преступленияю Методологические аспекты. Москва- Норма, ,2001,с.107

[87] Clarkson C.M.V. Understanding Criminal law. Third edition. London- Swet & Maxwell, 2001, p.244

[88] Флетчер Д., Наумов А.В.Основные концепциии современного уголовного права. Москва: Юристь,1998.с. 218

[89] Ibid., Флетчер Д., Наумов А.В., с. 235

[90] Марцев А. И. Преступление: сущность и содержание. Омск: МВД СССР Омская высшая шлола милиции., 1986.,с.16

[91] Neatkarīgo Valstu Sadraudzibas abreviatūra

[92] Baltkrievijas KK 11.p., , Bulgārijas KK 9.p., Rumānijas KK 17.p. u.c.

atzīst nodarījuma sabiedrisko bīstamību, kas ietver sevī prettiesiskuma pazīmi. ASV krimināltiesību zinātnē ir diezgan izplatīta konsensuss nozieguma (*consensus wiew of crime*) teorija. Saskaņā ar to noziegums ir uzvedība: 1) kas var nodarīt būtisku kaitējumu **lielākai sabiedrības daļai**; 2) ko kontrolē vai aizliedz spēkā esošs krimināllikums.[93] Ar šo teoriju īpaši tiek uzsvērts, ka krimināllikumā noteiktie aizliegumi vai darbības kontrole atbilst lielākās sabiedrības daļas interesēm. P. Pustorosļevs norāda, ka izšķir divu veidu noziedzīgus nodarījumus: 1) tos, kurus, legalizējot tautas paražas, augstākā valsts vara atzinusi par noziedzīgiem nodarījumiem; 2) kurus valsts vara atzinusi par noziedzīgiem, apstiprinot paražas bez vārdiem.[94] Līdzīgs viedoklis nedaudz citā interpretācijā, saistot šo procesu ar dabiskajām tiesībām, ir plaši pārstāvēts daudzu valstu krimināltiesību zinātnē. Piemēram, ASV Deitonas universitātes profesore S. Brennere norāda, ka Rietumu tiesību doktrīnā nereti nodarījumu sabiedriskās bīstamības apzīmēšanai lieto no dabiskām tiesībām atvasināto principu *malum in se* (ļaunums pats par sevi)[95] un no pozitīvām tiesībām atvasināto *mala prohibitia* (aizliegts ļaunums). Ar *mala prohibitia* apzīmē visus tos nodarījumus, ko krimināllikumā ir iekļāvis likumdevējs.

Piemērs. Latvijas radio bija sagatavojis vairākas reportāžas par nekārtībām, kas valda interneta kafejnīcās un interneta klubos. Pēc tam par šo jautājumu tika atklāta sabiedrības diskusija, kas parādīja, ka patiešām esošā visatļautība nodara būtisku kaitējumu sabiedrības drošībai, jo tur vakaros uzturas nepilngadīgi bērni, viņiem tur atļauj darīt visu, tai skaitā iegūt arī erotiska un pornogrāfiska rakstura informāciju, spēlēt vardarbību propogandējošās datorspēles utml. Speciālisti izvērtēja šo problēmu un atzina, ka nepieciešams izstrādāt kvalitatīvi jaunus MK noteikumus, kas noteiktu kārtību erotisko un pornogrāfisko materiālu apritē, tai skaitā arī elektroniskā vidē. Ja MK akceptēs ierosinātos grozījumus, tad paplašināsies iespēja pret vainīgām personām piemērot gan administratīva, gan krimināla rakstura sankcijas. Šobrīd, kaut arī visi atzīst, ka šādas informācijas izplatīšana internetā apdraud bērnu veselību, šīs darbības nevar tikt atzītas par nelikumīgām, jo likumdevējs tām nav devis savu juridisko novērtējumu.

Iepriekšaprakstītā darbība sabiedrības izpratnē var tikt uzskatīta par kaitīgu un morāli nosodāmu. Tomēr tā nav atzīstama par noziedzīgu, jo šādu vērtējumu tai nav devis likumdevējs. Iekļaujot to vai citu nodarījumu (darbību vai bezdarbību) krimināllikumā, likumdevējs to atzīst par bīstamu sabiedrības labklājībai un

---

93 Introduction to Criminal Justice fifth edition by J.J. Senna, L. J. Siegel St. Paul-New York- Los Angeles- Sanfrancisco – West publishing company,[b.g.] p. 36.

94 Анализ о преступлении исследование. Исследование П.П.Пусторослева Москва- Университетская типография, 1892.,с.97

95 Malum in se – ļaunums pats par sevi, parasti apzīmē noziegumu vai darbību, ko raksturo izteikta amoralitāte , kā, piemēram, slepkavība, dedzināšana, izvarošana A handbook of criminal law terms by Bryan A. Garner. St. Paul, Minnesota – West group, 2000,p. 427

personu drošībai un nosaka šādas darbības aizliegumu vai ierobežojumu un sodu par to pārkāpšanu. Īstenojot nozieguma *konsensuss* teoriju, Rietumu krimināltiesību teorētiķi uzskatāmi pierāda, ka demokrātiskā sabiedrībā krimināllikumos noteiktie aizliegumi ar soda piedraudējumu vienmēr atbilst sabiedrības lielākās daļas interesēm.

Mūsdienās lielākajā daļā Eiropas valstu krimināllikumu ir nostiprināta tieši šāda formālā noziedzīgā nodarījuma pazīme. Lemjot jautājumu par tā vai cita nodarījuma iekļaušanu krimināļkodeksā, likumdevēji un eksperti vērtē, cik lielu kaitējums tas var nodarīt valsts vai sabiedrības interesēm un pastāvošajai sabiedriskajai kārtībai.[96] Analogu domu izsaka arī angļu kriminālisti A. Simesters un G. Sullivans, norādot, ka noziedzīgs nodarījums nav tikai personīga lieta, jo personu uzvedību kriminalizē tāpēc, ka tā satur ļaundarību, kas tieši un būtiski apdraud sabiedrības drošību un sabiedrības labklājību.[97]

Piemērs. Diskutējot par jaunā veida noziedzīgiem nodarījumiem, kā, piemēram, kibernoziegumiem, EP Kibernoziegumu komitejas eksperti, izvērtējot pasaules valstu pieredzi, no iesniegtajiem priekšlikumiem kriminalizēt apmēram 15- 20 nodarījumus, atzina, ka tikai 10 no ieteiktajiem var nodarīt būtisku kaitējumu sabiedrības drošībai un personu labklājībai. Tāpēc EP Konvencija paredz krimināltiesisko regulējumu par 10 noziedzīgiem nodarījumiem.

Tas, protams, neliedz EP dalībvalstīm atzīt par noziedzīgiem nodarījumiem arī citas darbības, kas saistītas ar kibertelpas izmantošanu. Krimināļatbildības noteikšana ir katras valsts suverēna tiesība. Tomēr, pieņemot šādu starptautisku Konvenciju, EP neiesaka dalībvalstīm īpaši aizrauties ar citu kibernoziegumu iekļaušanu krimināllikumā.

Piemēram, ieteikums varētu attiekties uz Krimināllikuma 245. panta dispozīcijas pārvērtēšanu, jo šobrīd Latvija ir vienīgā valsts ES, kas bija izstrādājusi vispārobligātus Informācijas sistēmu drošības noteikumus un noteikusi krimināļatbildību par to pārkāpšanu.

Jāpiekrīt izcilajam krievu tiesībzinātniekam N. Tagancevam, ka „ ..vēršanās pret sabiedrisko kārtību kļūst par krimināli sodāmu tikai tad, ja valsts saskaņā ar vēsturiski izveidotiem tautas dzīves nosacījumiem atzīst, kā tā var apdraudēt

---

[96] Уголовный кодекс Грузии. Науч. ред. З.К. Бигвана. Санкт-Петербург: Юридический центр пресс, 2002., с.27, Таганцев Н.С. Руское уголовное право. Лекции.Часть общая. В.2т.М.,1994. Т.2 с.7

[97] Ibid.,Simester A.P. , G.R. Sullivan, p. 2

mierīgu līdzāspastāvēšanu un pareizu valsts attīstību".[98] Tāpēc nenoliedzami krimināltiesības ir valsts politikas instruments, ar kura palīdzību tiek regulēts līdzsvars starp sabiedrībā akceptējamu un noliedzamu uzvedību.

Jēdziena „noziedzīgs nodarījums" analīze parādīja, ka Latvijas krimināltiesību teorija un prakse ir atgriezusies pie tradicionālā formālā uz likumības principu balstītā noziedzīgā nodarījuma jēdziena, kas noteikts Krimināllikuma 6. pantā:

*(1) Par noziedzīgu nodarījumu atzīstams ar nodomu (tīši) vai aiz neuzmanības izdarīts nodarījums (darbība vai bezdarbība), kurš paredzēts šajā likumā un par kura izdarīšanu draud kriminālsods.*

*(2) Par noziedzīgu nav atzīstams nodarījums (darbība vai bezdarbība), kam ir šajā likumā paredzēta nodarījuma sastāva pazīmes, bet kas izdarīts apstākļos, kuri izslēdz krimināllatbildību.*

Kā redzams no iepriekšminētā, tad noziedzīgs nodarījums ir abstrakts jēdziens, kurš pats par sevi krimināltiesiskas sekas neizraisa. Tomēr šim jēdzienam, kas ietverts lielākajā daļā Eiropas valstu krimināllikumu, ir arī praktiska nozīme, proti, tas ietver sevī svarīgāko krimināltiesību principu iemiesojumu, tai skaitā konstitucionālo[99] garantiju.

S. Dando pamatoti norāda, ka termins „noziedzīgs nodarījums"[100] nebalstās uz kriminoloģiju, bet gan uz krimināltiesību teoriju, kur kā galvenā pazīme tiek izcelta tiesiskuma dimensija. Noziedzīgs nodarījums ir pretējība tiesiskai kārtībai, tātad nosodāma, vainojama darbība.

## 3. Kibernozieguma jēdziens

### 3.1. Vēsturiskie aspekti

XXI gadsimts ir atnesis sev līdz jaunas krimināltiesību attīstības tendences, kas ir saistītas ar straujo informācijas tehnoloģiju ietekmi visās dzīves jomās. Mikroelektronika, kas ir visu tehnoloģiju pamatā, būtiski mainījusi ne tikai pašus komunikācijas līdzekļus, bet arī personu attiecības, kas rodas, lietojot šos zinātnes sasniegumus. Eiropas Savienībā un arī Latvijā valsts līmenī ir noteikts mērķis sasniegt informācijas sabiedrību. Informācijas sabiedrības moto: „Informācijas

---

[98] Уголовный кодекс Грузии. Науч. ред. З.К. Бигвана. Санкт-Петербург, Юридический центр пресс, 2002 , с.22, Таганцев Н.С. Руское уголовное право. Лекции.Часть общая. В.2т.М.,1994. Т.2 с.7

[99] Saeimas mājas lapa Latvijas Satversme 92.p.// www.saeima.lv (aplūkots 2004.gada 10. maijā).

[100] Ibid., Shigemitsu Dando.,pp. 1-3

kvalitāte- sabiedrības labklājības sastāvdaļa." Informācijas sabiedrības sasniegšana nav iedomājama bez visas sabiedrības informatizācijas. Juridiskajā literatūrā aizvien biežāk parādās problēmraksti, kas veltīti informācijas sabiedrības izveidošanai, un tāpēc nav pārsteigums, ka tiesību zinātnieki aizvien lielāku vērību pievērš šo procesu pētīšanai.

Šobrīd jau daudzās valstīs juridiskās zinātnes pētīšanas objekts ir informatizācija[101] un ar to saistītie procesi. KF Likuma „Par informāciju, informatizāciju un informācijas aizsardzību"[102] 2.pants noteic: „.. informatizācija ir organizēts sociāli ekonomisks un zinātniski tehnisks process, kura rezultātā cilvēki, valsts varas orgāni, pašvaldības, organizācijas, sabiedriskās apvienības nodrošina savu tiesību realizācijai nepieciešamo informācijas resursu izmantošanu." Juristi definē informatizācijas procesu ar nosacījumu, ka informācijas aprite izveido (mantiskas un nemantiskas) attiecības starp informācijas procesa dalībniekiem, līdz ar to, lai panāktu drošu un efektīvu informācijas apriti, šim procesam ir nepieciešams zināms tiesiskais regulējums.

Jāpiekrīt O. Gavrilovam, kas uzskata, ka ar informatizācijas procesu saistītie tiesiskie jautājumi ir jānodala no termina „datorizācija", kas galvenokārt apzīmē informācijas apritei nepieciešamās tehniskās bāzes radīšanas procesu.[103] Tehnoloģijas attīstās nepārtraukti, un tiesības pēc iespējas vajadzētu nodalīt no šiem tehniskā progresa jautājumiem, jo tiesības vienmēr attiecībā pret tehnoloģijām paliks zaudētājas. Taču tas nenozīmē, ka valsts nevar tiesiski regulēt atsevišķu informācijas sistēmu tehniskās prasības. Tomēr īpaši jāuzsver, ka datorizācijas regulējums nevar būt krimināltiesību regulējuma objekts, jo tas pats par sevi bez cilvēka līdzdalības nevar radīt apdraudējumu personu likumīgām tiesībām un interesēm.

---

101 Latvijā šo zinātni sauc par informātiku (*informatics*). Tā ir zinātnes nozare, kas nodarbojas ar datu vākšanas, organizēšanas, apstrādes un izplatīšanas problēmu izpēti datu apstrādes sistēmās. Vairāku valstu universitātēs juridiskā informātika ir speciāls mācību priekšmets.// http://www.termini.lv/index.php?term=informatics&lang=EN&terms=imformatic (apskatīts 2003.gada 11. novembrī)

102 Федеральный закон " Об информации, информатизации и защите информации" от 25 яфнваря 1995г.

103 Гаврилов О.А. Курс правовой информатики. Учебник для вузов.-Москва: Норма-Инфра·М, 2000, с. 30

Jāpiekrīt D. Haitonam, ka tādējādi krimināltiesību saturā aizvien lielāku nozīmi ieņem sociāli tehnoloģiskais saturs.[104] Lielā mērā šo procesu ietekmē straujā interneta attīstība pasaulē. Internets, protams, ir tikai tehnoloģisks rīks, kas sastāv no n- tajiem datortīkliem, kas savienoti savā starpā. Tie dod tehnisku iespēju pārraidīt jebkuru informāciju uz jebkuru zemeslodes vietu, kur pieejama atbilstoša tehnoloģija. Jo valstī augstāka tehnoloģiskās attīstības pakāpe, jo vairāk personu ir tieši atkarīgas no jaunās komunikācijas kvalitātes. Sabiedrībai kļūstot atkarīgai no šo informācijas un komunikācijas veidu darbības, rodas aizvien jauni globāli apdraudējumi, kuri vienlaicīgi var apdraudēt personu dzīvību, veselību un mantu jebkurā vietā pasaulē. Tāpēc mūsdienu krimināltiesību attīstībā nepieciešams pievērst pastiprinātu uzmanību tām krimināltiesību tendencēm, ko rada tehnoloģiskais progress.

ANO VIII kongresā, kas bija veltīts noziedzības apkarošanas problēmām, tika izstrādāts un pieņemts dokuments „Starptautiskās krimināl ās politikas apskats - ANO rokasgrāmata ar datoriem saistītu noziegumu novēršanā un kontrolē". Tajā norādīts, ka pasaulē pirmais zināmais datornoziegums noticis 1801. gadā Francijā.

Piemērs. Uzņēmējs Džozefs Jagards savā tekstilrūpnīcā izgudroja un ieviesa datorkartes priekšteci, kas prata kopēt sērijveida ražošanā esošu audumu rakstu struktūru. Strādnieki, redzēdami, ka jaunais izgudrojums var apdraudēt viņu darbavietas, sabojāja šo ierīci, tā veicot kaitniecības aktu pret izmantoto tehnoloģisko risinājumu, viņi izdarīja pasaulē pirmo datornoziegumu.[105]

S. Sjolbergs pirms divdesmit gadiem apgalvoja, ka„.. termins „datornoziegumi" tuvākos gados kļūs par vienkāršāko, plašāko un visbiežāk lietoto terminu tiesību speciālistu vidū un sabiedrībā".[106] Tas ir pilnīgi attaisnojies, jo patlaban, kad sabiedrība ir izvirzījusi uzdevumu maksimāli atbalstīt IT attīstību, šī problēma kļūst aizvien aktuālāka. Kopš Havannas VIII ANO Noziedzības novēršanai un krimināl ai tiesvedībai veltītā kongresa regulāri gan ANO, gan Eiropas Padomes un citu starptautisku organizāciju līmenī tiek pieņemtas dažādas rezolūcijas, pasākumu

---

[104] Law's future(s) British legal developments in the 21st Century ed. by David Hayton. Oxford-Portland Oregon – Hart publishing, 2000., p.29

[105] Sk. International review of criminal policy-United nations manual on the prevention and control of computer- related crime http://www.uncjin.org/Documents/EighthCongress.html#congress (aplūkots 2001.gada 21.aprīlī)

[106] Schjolberg Stein Computers and penal legislation A study of the legal politics of a new technology Universitetsforlaget, Oslo, 1983., p. 1.

plāni, kuru uzdevums ir apkarot informācijas tehnoloģiju ļaunprātīgu izmantošanu noziedzīgos nolūkos.

Lielākā noziedzīgo nodarījumu daļa kibertelpā ir cieši saistīta ar informācijas sistēmu drošību. Jo vairāk IS īpašnieki vai turētāji var ieguldīt savu sistēmu drošībā, jo lielāka garantija, ka sistēmas resursi netiks pakļauti apdraudējumiem. Vācijas ISD rokasgrāmatā norādīts, ka cilvēks ar savu darbību tīši var ietekmēt informācijas un tehniskos resursus vairāk kā 60 veidos[107], bet tikpat variantos iespējams pieļaut sistēmas apdraudējumus, rīkojoties neuzmanīgi. No iepriekš teiktā jāsecina, ka ir grūti ir atrast pasaulē tādu nozieguma sastāvu, kuru nevarētu izdarīt ar informācijas tehnoloģiju un komunikāciju palīdzību. Kā norādīts iepriekš pieminētajā rokasgrāmatā, tad datornoziegumi var tikt iesaistīti tādu tradicionālu reālā pasaulē pazīstamu noziegumu izdarīšanā kā, piemēram, krāpšana, zādzība, viltošana, bojājumu nodarīšana u. c.[108]

Sabiedrības un zinātnes attieksme pret datornoziegumiem radikāli mainījās pēc 1980. gada, kad prese publicēja informāciju par pārsteidzošām hakeru, vīrusu un "tārpu" lietām.[109] Tas radīja nepieciešamību atrast piemērotu definīciju jaunajam fenomenam. Viens no ASV pazīstamākajiem datornoziegumu ekspertiem Dons Parkers *(Don Parker)* 1983. gadā datornoziegumu definēja kā „noziegumu, kura sekmīgai izdarīšanai ir nepieciešamas zināšanas datortehnikā".[110] 1983. gadā ANO OECD ekspertu grupa definēja datornoziegumus kā „ikvienu, nelikumīgu, neētisku vai neautorizētu uzvedību, kas saistīta ar automātisko datu procesu un/ vai datu pārraidīšanu".[111] S. Sjolbergs norāda, ka izstrādātajā rekomendācijā OECD ieteica dalībvalstīm iekļaut savu nacionālo valstu krimināllikumos tādas normas, kas satur datornoziegumus.[112]

---

[107] Bundesamt für Sicherheit in der Informationstechnik IT- Grundshutzhandbuch 1997 BSI 7252 CD

[108] Sk. International review of criminal policy-United nations manual on the prevention and control of computer- related crime http://www.uncjin.org/Documents/EighthCongress.html#congress (aplūkots: 2001.gada 21. aprīlī)

[109] Legal aspects of computer- related crime in the Information Society – Comcrime- study - prepared for the European Commission by prof. Dr. Ulrich Sieber University of Wurzburg, Version 1.0 of 1st January 1998., p. 19

[110] Parker D. Fighting Computer crime,[ b.i.] 1983.

[111] Ibid., Dr. Ulrich Sieber., p. 19.

[112] The legal framework - unauthorised access to computer systems, Penal legislation in 37 countries (last updata March 15 1999 by Stein Scjolberg http://www.mossbyrett.of.no/info/legal.html (aplūkots 2003.gada 23. martā)

Kopš tā laika ES Komisijas un EP Komitejas ir organizējušas vairākus pētījumus. Šo un citu pētījumu galarezultātā tika izstrādāta EP Rekomendācija Nr. (89) 9 „Datorsaistīti noziegumi" (*On computer related crime).* Viens no svarīgākajiem starptautisko tiesību dokumentiem datornoziegumu jomā ir Eiropas Padomes 1995. gada 11. septembra Rekomendācija „Par rekomendācijām procesuālajās tiesībās, kas saistītas ar informācijas tehnoloģiju izmantošanu" (95)13 (*Recommendation concerning problems of procedural law with information technology*). Minētais dokuments deva jaunu impulsu Eiropas valstu tiesiskās bāzes nostiprināšanā cīņai ar datornoziegumiem. Ja paraugāmies vēsturē, tad ir redzama ļoti skaidra tendence, kā tehnoloģiskais progress ietekmē noziedzību.

Piemērs. Vācijā 1996. gadā policijā bija reģistrētas 32 128 lietas, ko apzīmēja ar terminu „datornoziegumi". No tām 26 802 lietas bija saistītas ar elektronisko naudas automātu manipulācijām, 3588 ar datorkrāpšanu, 198 lietas par datordatu viltošanu, 282 lietas par datorkaitniecību un 933 hakeru lietas. Nīderlandē no 1981. līdz 1992. gadam bija reģistrētas apmēram 1500 lietas, to skaitā apmēram 10% hakeru lietu, 15% autortiesību pārkāpumu, datorvīrusu - 30%, taču katru gadu šis skaitlis pieaug. Japānā no 1971. gada līdz 1995. gadam bija 14 lietu, kas saistītas ar datora cietā diska sabojāšanu, 12 lietu par datu falsifikāciju, 7 lietas par nelegālu datora izmantošanu, 12 datu zādzības lietu, 1995. gadā parādījās jauna veida noziegumi, kas saistīti ar dažādām elektronisko karšu manipulācijām, kas netika ieskaitīti datornoziegumu statistikā.[113]

No šīs statistikas var izcelt divas tendences:

- nav vienotas politikas, ko uzskatīt par datornoziegumu;
- no 1970. gada līdz 1995. gadam ievērojami un uzskatāmi pieaugusi datornoziegumu izdarīšanas sarežģītības pakāpe.

ASV ģenerālprokurora vietnieks E. Holders (*Eric Holder*) 2000. gada 12. janvārī Kibernoziegumu ekspertu sanāksmē norādīja, ka neviens patlaban nezina, cik lielas var būt augsto tehnoloģiju radītās problēmas. Var tikai aprēķināt ekonomiskos zaudējumus, kas nodarīti datornoziegumu dēļ. Zināms, ka rūpniecībai tie katru gadu rada miljardiem dolāru zaudējumu, bet neviens nevar pateikt, kādas sabiedrības dzīves jomas tie ietekmēs nākotnē.[114]

Kibernoziedzniekam ir vairākas priekšrocības pret noziedznieku, kas nodarījumu izdara tradicionālā veidā : 1) liela peļņa, bet zems risks; 2) nav tieša kontakta ar cietušo; 3) nav jālieto ieroči; 4) nav fiziski jābēg no nozieguma izdarīšanas vietas;

---

113 Ibid., Dr. Ulrich Sieber. p.21

114 Remarks of Deputy Attorney General Eric H. Holder, Jr. High-Tech Crime Summit January 12, 2000, http://www.usdoj-crm/mis/mdf (aplūkots 2003.gada 24. maijā)

5) policija nav sagatavota cīņai ar šādām parādībām; 6) ja arī noķers, tad atbildība par šādiem nodarījumiem ir ievērojami zemāka nekā par tradicionāliem nodarījumiem; 7) laupījums bez fiziskas piepūles tiek nogādāts vajadzīgā vietā.[115] Iepriekšminētās priekšrocības nav vienīgās, bet tās ir pietiekami pievilcīgas, lai veicinātu kibernoziedzību. Tāpēc šobrīd pasaulē pilnīgi atklāti var runāt par ievērojamu kibernoziegumu kvantitatīvo un kvalitatīvo pieaugumu.

Piemērs. CSI/FBI 2003. gada aptauja parādīja, ka katru gadu pieaug to apdraudējumu skaits, ko personas veic izmantojot interneta resursus. 2003. gadā 78% no visiem uzbrukumiem ADAS resursiem tika veikti no interneta.[116] Austrālijā 2003. gadā veiktā kibernoziegumu un drošības aptauja[117] parādīja, ka 54% uzbrukumu saistīti ar internetu.

1997. gadā Latvijas policijas rīcībā bija neoficiāla informācija, ka kibernoziegumu nodarītie zaudējumi Latvijā varētu sasniegt 2 - 3 miljonus dolāru.[118] Taču jāpiebilst, ka šie skaitļi var būt arī pieņēmums, jo IeM statistika līdz šim nereģistrē kibernoziegumus kā atsevišķu noziegumu veidu. To, ka šādu darbību dēļ arī Latvijā rodas zaudējumi, pierāda gadījums ar kaitīgo programmu CIH jeb Černobiļa.

1998.g. 26. aprīlī Latvijas datorlietotāji masveidā pirmo reizi saskārās ar kaitīgo programmu CIH "Černobila".[119] Tā sabojāja lielu daļu Latvijas valsts iestāžu informācijas sistēmas, kas izmantoja Windovs 95., 98, 2000 datorprogrammas. Lieli zaudējumi tika nodarīti valsts iestāžu datorsistēmām, un faktiski līdz šim brīdim neviens nav precīzi uzskaitījis šos zaudējumus, taču to, ka zaudējumi bija milzīgi, apliecina kaut vai tas, ka pēc tam valdība pieņēma lēmumu izstrādāt valstī informācijas sistēmu drošības politiku.

2003.gada septembrī televīzijā ziņoja, ka datortārpa Big one darbība nodarījusi zaudējumus Igaunijas datorsistēmām vairāk kā 3 miljonu Igaunijas kronu apmērā, bet pasaulē šī kaitīgā rīka nodarītā kaitējuma apmērs var sasniegt pat desmitiem miljardu dolāru. Minētie fakti pamato ar kiber-noziegumiem saistīto krimināltiesību normu starptautiskas harmonizācijas nepieciešamību. ES Komisijas veiktajā

---

115 Identity theft law & filings answers by Robert Morgester, Deputy attorney General, [b.i] 2003.

116 2003 CSI/FBI Computer Crime and Security Survey p.8

117 2003 Australian Computer crime and security survey.

118 Some trends of cybercrime under Latvian substantial laws , by Kinis U. PC-CY (97) 17

119 sk. CERT mājas lapa http://www.cert.org/tech_tips/CIH_FAQ.html (aplūkots 2003.gada 7. decembrī)

pētījumā „*Comcrime*" eksperti apstiprināja šādus ar datoriem saistītu noziegumu, kas vērsti pret privāto dzīvi, harmonizācijas principus: [120]

1. ***Ultima ratio* princips**. Privātās dzīves aizsardzība no apdraudējumiem, ko izraisa informācijas un tehnoloģiju nelikumīga izmantošana, galvenokārt ir jāapkaro ar administratīvām un civiltiesiskām metodēm, bet krimināllatbildību piemērot tikai kā galējo līdzekli[121], ja iepriekšminētie pasākumi nevar tikt piemēroti.

2.**Krimināltiesību terminu precīzu formulējumu princips**. Krimināllatbildības pamatam ir jābūt noteiktam precīzi, tas nozīmē, ka ir jāizvairās no neskaidriem un divdomīgiem teksta formulējumiem (*Principle of precision in the wording of criminal law*).

3. **Skaidrības princips**. Krimināltiesību normai ir jābūt izteiktai skaidri un nepārprotamai. Īpaši tas ir jāsaista ar nepieciešamību atturēties no tehnoloģisku terminu iekļaušanas tekstā. Ja norma ir izteikta šauri un precīzi, tad krimināllikums skaidri pasaka, kas ir aizliegts (*Clearness principle*).

4. **Dažādošanas princips**. Nevar savienot vienā vispārējā pantā atbildību par dažāda rakstura privātās dzīves pārkāpumiem, kas izdarīti ar datortehnoloģiju palīdzību. Tāpēc EP eksperti ierosina dažādot šo atbildību atkarībā no personas vainas, apdraudētās intereses un nozieguma izdarīšanas motīviem (*principle of differentation*).

5. **Nodoma princips**. Nodarījumiem, kas saistīti ar datortehnoloģiju izmantošanu, jābūt sodāmiem tikai tad, ja tie izdarīti ar nodomu. Ja šādi nodarījumi veikti aiz neuzmanības, tad krimināllatbildība piemērojama tikai izņēmuma gadījumos. (*Principle of intent*).

6. **Sūdzības princips**. *Ja šāds pārkāpums uzskatāms par mazsvarīgu, pamatojoties uz EP Rekomendāciju R(87)17* „Par dalībvalstu justīcijas vienkāršošanu" 12.b (i) punktu, kas nosaka, ka „..būtu jāpalielina to lietu skaits, kurās tiesvedības ierosināšanai ir nepieciešama noteiktu nosacījumu izpildīšana, piemēram, tajos

---

[120] Ibid., Dr. Ulrich Sieber p. 153.

[121] *Ultima ratio* princips cieši sasaucas ar EP ekspertu ziņojumā „Council of Europe Legal affairs Computer related crime pefased by August Bequai, European by European Committee on Crime Problems, Strasbour 1990. Recommendation No(89)9 on computer related crime and final report of the European Committee on Crime Problems, minēto galējās nepieciešamības principu ,p. 24

gadījumos, kad sabiedrības intereses nav tik svarīgas, par šādu nosacījumu tiesvedības ierosināšanai varētu būt cietušā lūgums vai piekrišana", *tad tādas lietas ierosināmas tikai pēc cietušā sūdzības (principle of complaint).*

Ar datoriem saistītos[122] ekonomiskos noziegumos par prioritātem tika atzītas:

- datorkrāpšanas apkarošana (*fraud*);
- datorviltošanas apkarošana (*forgery*);
- datu un datorprogrammu bojāšana;
- datorsabotāža (*computer sabotage*);
- neautorizēta piekļūšana (*hacking*);
- nelikumīga pārtveršana (*interception*);
- noziedzīgi nodarījumi autortiesību un blakustiesību jomā (aizsargātu datorprogrammu un topogrāfiju reproducēšana).

Iepriekš minētie principi ir pamats, kas jāizmanto, definējot kibernoziegumus. Taču, lai varētu izpildīt šo uzdevumu, nepieciešams konstatēt, vai kibernoziegums ir jauna veida noziedzīgs nodarījums vai arī tam piemīt tradicionālam nodarījumam raksturīgas pazīmes.

### 3.2. E- vide un terminoloģijas problēmas

Realitāte pamet fizisko pasauli un pārceļas uz virtuālo pasauli vai uz to telpu, ko nosacīti pieņemts saukts par "kibertelpu". Kibertelpā kaut ko izdarīt var tikai ar tehnisko resursu palīdzību. Ar datortehnoloģiju atnākšanu radīts elektronisks bits, kuram nav ne smaržas, ne krāsas, ne svara, bet kurš var pārvietoties ar gaismas ātrumu.[123] Vistrāpīgāk šo problēmu ir raksturojis D. Posts: „Ļoti grūti ir saukt pie atbildības un apcietināt elektronu."[124]

Piemērs. Persona, piem., Minskā sēž pie datora un vienkārši pārvieto elektroniskos bitus (vieniniekus un nullītes) savā datorekrāna un īsteno ielaušanos kādā ASV bankā. Šī persona, sēžot savā istabā, no ASV teritorijā esošās bankas konta noņem konkrētu naudas summu un pārsūta to uz citā pasaules malā atrodošos bankas kontu, jo bitus neietekmē ne reālā pasaulē esošās naudas apjoms, ne masa.

---

122 Ibid., Dr. Ulrich Sieber p.159.

123 Why police don't care about computer crime. 10 Harv.J.L.&Tech. 465.(Summer 1997) by Marc D.Goodman http://www.jolt.law.harward.edu/articles/10hjolt465.html (aplūkots 2000.gada 22.augustā.)

124 The cyberspace revolution David G. Post Keynote Address, Computer Policy & Law Conference // Cornell University, July 9. 1997.

Tomēr tradicionālā nozieguma izpratne nevar un nedrīkst būt atšķirīga no kibernozieguma. Neskatoties uz to, ka pasaulē pastāv dažādas tiesību sistēmas, tomēr visās pastāv vienota pieeja, ka noziegumu var izdarīt tikai cilvēks ar savu darbību vai bezdarbību. Neatkarīgi no tā, kāda būs tehnoloģiju attīstība, vainojama būs tikai cilvēka mērķtiecīga darbība. Krimināltiesībās par noziedzīga nodarījuma subjektu nekad nekļūs ierīce vai rīks, bet tikai pieskaitāms, noteiktu vecumu sasniedzis cilvēks. Ierīce jau pati par sevi neveic mērķtiecīgas darbības, bet to vada cilvēka mērķtiecīga rīcība.[125] Šim secinājumam ir liela praktiska nozīme, jo modernajā Rietumvalstu tiesību teorijā jau parādās idejas, ka datori paši spēj domāt[126], līdz ar to paši spēj prognozēt darbības un vadīt tās, un tātad uzņemties arī atbildību. Šīs idejas piekritēji secina, ka mūsdienās dators var darboties neatkarīgi no cilvēka gribas. Programmētājs ar datorprogrammas palīdzību devis iespēju ierīcei patstāvīgi veikt noteikta rakstura darbības, piem., spēlēt šahu, vai arī patstāvīgi veikt dažādas darbības, tai skaitā arī tādas, kas vērstas uz kaitējumu nodarīšanu citu personu likumīgām interesēm. Tomēr atbildīgs vienmēr būs cilvēks, kas radījis mašīnas intelektuālo prātu.

Minētajā ar datoriem saistītu noziegumu novēršanas un kontroles rokasgrāmatā norādīts, ka praksē bieži tiek lietoti šādi termini - datora ļaunprātīga izmantošana, t.i., *computer misuse,* un datora nepareiza ekspluatācija,t.i., *computer abuse.* Šiem abiem terminiem ir principiāli atšķirīga nozīme, jo ne vienmēr, konstatējot šos gadījumus, iestājas krimināalatbildība. Tā iestājas tad, ja darbības ir nelikumīgas vai krāpnieciskas un ja atbildību par tām paredz likums. Jebkurām krimināltiesībām, kas paredz atbildību par datorsaistītiem noziegumiem, ir jānošķir gadījumi, kad datorsistēma tiek nepareizi izmantota gadījuma vai neuzmanības dēļ vai tās

---

[125] Ibid., Флетчер Д., Наумов А.В., с. 136

[126] Grewlich Klaus W. Governance in "cyberspace" access and public interest in global communications. Kluwer law international 1999., p. 50.' Law of International on-line business A. Global perspective general editor Christian Campbel Sweet& Maxwell chapter 8 Finland by Pekka Raatikainen, Ahola& Sokka. - Helsinki Finland, London, 1998., pp. 304. - 306.; Lesigs atsauce uz Joel R. Reidenberg, Governing Networks and Rule-Making in Cyberspace, 45 EMORY L.J. 911, 929 (1996). See also Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 TEX. L. REV. 553 (1998); Rules in the Virtual Society by Mark Gould // http://aranea.law.bris.ac.uk/VirSoc/ (Aplūkots 2000.gada 10. oktobrī).

nepareiza ekspluatācija saistīta ar tīšu, neautorizētu iekļūšanu datorsistēmās, jo visus šos gadījumus var uzskatīt par nepareizu datorsistēmas ekspluatāciju, bet ne katra nepareiza datorsistēmas ekspluatācija (*abuse*) ir noziegums.[127]

Tiesību objekts ir tā informācija, kam tās autors vai īpašnieks ir piešķīris **vērtību**, tas ir, ielicis šīs informācijas radīšanā savu vai citu personu darbu. Informācijas noziegumi ir saistīti ar informācijas vidi.[128] Vairāki kibernoziegumu eksperti savos darbos terminu *„informācijas vide"* identificē ar specifisku apkārtējo vidi, tas ir, ar to apstākļu kopumu, ko veido informācijas un komunikācijas tehnoloģijas. Tas arī noteic to, ka sākotnēji šie noziegumi tika nosaukti par datornoziegumiem.[129]

Attīstoties zinātnei, datori ienāca sadzīvē un daudzi jautājumi kļuva diezgan neskaidri, jo datortehnoloģija bija iebūvēta ikvienā sadzīves priekšmetā, šujmašīnā, veļas automātā, automašīnā. Par datoru pieņemts uzskatīt ierīci, kas var uzkrāt un apstrādāt datus. Tāpēc, kvalificējot šos noziedzīgos nodarījumus, speciālisti izstrādāja citu terminu, proti, „datorsaistīti noziegumi",[130] un definēja šo noziegumu veidu kā *„..jebkuru nelikumīgu darbību, kur datorsistēma ir nozieguma objekts vai nozieguma rīks"*. Ar šo nodarījuma veidu apzīmēja ikvienu darbību, kuras uzdevums ir ietekmēt IS funkcijas. Tomēr arī pie šīs terminoloģijas speciālisti neapstājās, jo EP, pieņemot 1995.gada rekomendāciju Nr. 13,[131] šis termins tika aizstāts ar terminu „noziegumi, kas saistīti ar informācijas tehnoloģiju izmantošanu". Īpaši tika atzīmēts, ka šos noziegumus var izdarīt ar datorsistēmas palīdzību. Šajā gadījumā sistēma var būt gan nozieguma objekts, gan līdzeklis

---

127 Sk. International review of criminal policy-United nations manual on the prevention and control of computer- related crime http://www.uncjin.org/Documents/EighthCongress.html#congress (21.04.2001)

128 Krievijas Federācijas Likumā "Об участии в международном информационном обмене" tiek lietots termins "общественная информационная среда" (sabiedrības informācijas vide), kas definēta kā subjektu darbības joma, kas saistīta ar informācijas radīšanu, pārveidošanu un lietošanu. Sk. Панфилова Е. И., Попов Ф. Н. Компютерные преступления.- Санкт- Петербург: [ b.i.] 1998., c. 21.

129 Schjolberg Stein Computers and penal legislation A study of the legal politics of a new technology Universitetsforlaget, Oslo, 1983., p. 4; Ibid., Dr. Ulrich Sieber, pp.18 - 20.

130 Terminu "*computer related crime*" EP eksperti izmantoja, izstrādājot 1989.gada rekomendāciju Nr. 8 "Datorsaistīti noziegumi"Sk. Council of Europe Legal affairs Computer related crime pefased by August Bequai, European by European Committee on Crime Problems, Strasbour 1990. Recommendation No(89)9 on computer related crime and final report of the European Committee on Crime Problems p. 12.

131 Recommendation Nr. (95)13 of criminal procedurial law cennected with information technology. P. Csonka Council of Europe Activities related to information technology, Data protection and computer crime 5 (1996) Information & Communication technology law, p.186.

nozieguma izdarīšanai. Tā eksperti sekmīgi atrisināja divdomīgo situāciju ar jēdziena „dators" saturu, paplašinot šīs kategorijas noziegumu objektu un līdzekļu loku.[132]

Attīstoties starptautiskajiem datortīkliem, lielākā daļa noziegumu tiek izdarīti no attāluma, vai nu nelikumīgi piekļūstot datorsistēmām, vai arī ievadot sistēmā speciāli veidotu programmu, kuras uzdevums ir manipulēt ar sistēmas resursiem utt. Tāpēc krimināltiesību speciālisti kopā ar datorspeciālistiem meklēja risinājumu šai jaunajai problēmai. Tā radās termini, kuru definējumā bija jāietver prasības, lai tos varētu piemērot saistībā ar jebkuras jaunās tehnoloģijas ļaunprātīgu lietojumu. Tāpēc termins „kibernoziegums" tika atvasināts no Viljama Gibsona zinātniski fantastiskā romāna „*Neiromancer*", kas aprakstīja datorpasauli kā „kibertelpu". S. Brennere raksta, ka kibertelpa ir vide, kas eksistē kopā ar reālo pasauli, bet neatkarīgi no tās. Tā pastāv cilvēku priekšstatos, bet nesatur materiālu substanci. Tā ir jauna telpa, kuras pirmsākumi meklējami reālā pasaulē, bet kura pārsniedz šo realitāti.[133]

Kibernoziegums, ko dažas valstīs sauc arī par „noziegumiem pret informāciju",[134] norāda to, ka šo nodarījumu tiešais apdraudējuma objekts ir informācija. Par kiber-noziegumu var atzīt jebkuru noziedzīgu nodarījumu, ko var izdarīt ar datorsistēmas vai datortīkla palīdzību vai kas vērsts pret datorsistēmu vai tīklu. Citiem vārdiem sakot, kibernoziegums ir jebkurš noziedzīgs nodarījums, kas izdarīts elektroniskā vidē.[135] ANO X kongresā kibernoziegumu semināram sagatavotajā dokumentā norādīts, ka kibernozieguma jēdzienā ietilpst:

- šaurākā nozīmē datornoziegums- jebkura nelikumīga uzvedība,[136] kas izdarīta ar elektroniskiem līdzekļiem pret datorsistēmu[137] drošību un datu apstrādes procesu tajā;

---

[132] Панфилова Е. И., Попов Ф. Н. Компютерные преступления. Санкт- Петербург: [b.i.] 1998., c.10.

[133] Brenner Susan "Is there such a thing as a virtual crime?" California Criminal Law Review Volume 4: June 2001

[134] Ibid., Панфилова Е. И., Попов Ф. Н. c. 10.

[135] Sk. UN Tenth United nations Congress on the Prevention of crime and the Treatment of Offenders Vienna 10-17 Aprill 2000. Crimes related to computer network. background paper for the workshop on crimes related to the computer network A/Conf.187/10, p. 4.

[136] Jēdziens "uzvedība" kibernoziegumu izpratnē ietver sevī subjekta tīšu (dolus eventualis) darbību, bet parasti neietver bezdarbību vai darbību aiz neuzmanības , kā arī to, vai darbība ir tīša vai notikusi aiz neuzmanības.

- plašākā nozīmē (datorsaistīti noziegumi) - jebkura nelikumīga uzvedība, kas saistīta ar vai pret datorsistēmu vai tīklu, ieskaitot tādus noziegumus kā nelegāls informācijas valdījums, reklāma un izplatīšana ar datorsistēmas vai datortīkla starpniecību.[138]

Trīs gadu laikā EP Kibernoziegumu ekspertu komitejai nebija dots uzdevums izstrādāt visiem pieņemamu kibernoziegumu definīciju. Tas ir saistīts ar termina „nelikumīgs" *(without rights)* saturu. Jāatzīst, ka šobrīd nav iespējams atrast vienotus kritērijus, kas dotu pamatu šāda termina vienotai izpratnei.

Piemēram, Kanādas eksperti uzskata, ka šādā terminā ir jāietver arī negodīgums, neētiskums, savukārt citi eksperti uzskatīja, ka pamats konkrētas darbības atzīšanai par nelikumīgu ir kaitējums, kas nodarīts citai personai u.c. Ar negodīgiem noziegumiem vispārējo tiesību valstīs saprot noziegumus, kas vērti pret personu īpašumu.

Diskusijas par kibernoziegumu definīciju pasaulē turpinās. Eksperti uzskata, ka šī nozieguma definīcijas izstrādāšana ir nacionālo valstu tiesība. Tāpēc ikviens starptautisks dokuments, ieskaitot INTERPOL datornoziegumu rokasgrāmatas, atturas no šo darbību definēšanas. Tomēr pasaules krimināltiesību speciālistu sanāksmēs šādas definīcijas tiek apspriestas, bet lielākajā daļā gadījumu diskusija ir par šo noziegumu satura elementiem, bet ne definīciju kopumā.

Daļa ekspertu atbalsta ideju, ka kibernoziegums ir jebkura nelikumīga darbība, kurā dators ir nozieguma rīks vai objekts, kas tiek lietots ar mērķi ietekmēt datorsistēmu vai datortīklu funkcijas. Citi eksperti uzskata, ka krimināli sodāma ir darbība, ja likumpārkāpējs tieši iedarbojas uz informācijas tehnoloģiju ar mērķi nodarīt cietušajam zaudējumus, citiem vārdiem sakot, **iegūt labumu**. Ar zaudējumu nav jāsaprot zaudējums tikai materiālā nozīmē. Tas tikpat labi var būt privātuma aizsardzība, gods, cieņa un reputācija.

Patlaban pasaulē visplašāk lietoto kibernoziegumu vai noziegumu datortīklā *(netcrimes)* definīciju ir izstrādājuši ANO OECD eksperti:

---

137 EP Kibernoziegumu Konvencijas 1. pantā jēdziens "datorsistēma" definēta kā jebkura ierīce vai savstarpēji saistīta ierīču grupa, kas darbojas uz programmas pamata un kas nodrošina datu automātisko apstrādes procesu vai veic citu funkciju. Ar citu funkciju eksperti apzīmē jebkuru sistēmu, kuras darbības pamatā ir telekomunikāciju sistēma, radio vai cits loģisks savienojums.

138 Sk. UN Tenth United nations Congress on the Prevention of crime and the Treatment of Offenders Vienna 10-17 Aprill 2000. Crimes related to computer network. background paper for the workshop on crimes related to the computer network A/Conf.187/10, p. 5.

„Par kibernoziegumu ir jāatzīst ikviena nelikumīga, neētiska vai patvaļīga uzvedība, kas saistīta ar datu automātisko apstrādi un pārraidi."[139] Protams, šī definīcija ir tikai paraugs ANO EDSO dalībvalstīm, tomēr tā satur terminu „neētisks", kas diezin vai ir piemērojams Latvijas krimināltiesību doktrīnā. Jebkurš noziedzīgs nodarījums ir nelikumīga darbība, kas pati par sevi ir negodīga, neētiska. Nevar piekrist, ka ikviena neētiska darbība ir noziedzīgs nodarījums. Kibernoziegums ietver gan pirātismu, gan ielaušanos datorsistēmās, un visi šie noziegumi ir izdarīti augsto tehnoloģiju[140] jomā, tāpēc tos nereti dēvē arī par augsto tehnoloģiju noziegumiem (*high tech crime* - HTC).[141]

Atšķirība šajās definīcijās ir tā, ka šeit uzsvars tiek likts uz tehnoloģiju kā nozieguma rīku vai objektu, kaut gan tiesību speciālisti vēl joprojām strīdas, kas veido HTC. Pie augstajām tehnoloģijām daži speciālisti pieskaita arī vismodernākos zinātnes sasniegumus, kas iegūti ar datoru palīdzību, piemēram, gēnu inženieriju u.c. To pierāda Kalifornijas štata likumos iekļautā definīcija, ka tie ir noziegumi, kuros tehnoloģija izmantota kā nozieguma rīks vai palīglīdzeklis ar mērķi izdarīt noziegumu.[142] Tomēr arī šī definīcija neievieš skaidrību, jo Kalifornijas tiesību speciālisti pie HTC pieskaita mikroshēmu zādzības, datoru un to sastāvdaļu zādzības. Šie noziegumi, kas saistīti ar zināmas materiālas substances (kustamas lietas) nelikumīgu izņemšanu no īpašnieka valdījuma, ir parasta zādzība, kuras izdarīšanā parasti tiek lietotas tradicionālās noziegumu izdarīšanas metodes, kā, piemēram, ielaušanās, iekļūšanas telpā u.c., un to izdarīšana nav saistīta ar augsto tehnoloģiju lietojumu zādzības procesā. Šo viedokli atbalstīja arī Kibernoziegumu komitejas eksperti, jo par kibernoziegumiem nevar atzīt materiālas substances, tas ir, datora, mikroshēmas u.c. zādzību. Kibernoziegumu var raksturot arī citās

---

139 Computer related crimes by Dr. Gulshan Rai, R. K. Dubash, Dr. A.K. Chakravarti Government of India dep. of Electronics New Deli[ b.i][b.g.].; OECD - Computer-Related Crime, Analysis of Legal Policy , Paris, 1986 ; Legal aspects of computer- related crime in the Information Society – Comcrime- study- prepared for the European Commission by prof. Dr. Ulrich Sieber University of Wurzburg, Version 1.0 of 1st January 1998., p.20.

140 Saskaņā ar Eurostat R&D and Innovation Statistics- Eight EEA Working Party Meeting Luxembourg, 22nd-25th November 1999 Doc Eurostat/A/4/REDIS/99/10 pie augstām tehnoloģijam pieskaita izstrādājumus: 1) aviācijā, 2) datoru un biroja tehnikā, 3)elektronisko komunikāciju jomā, 4) farmācijā, 5) bruņojumā. p. 29

141 Remarks of Deputy Attorney General Eric H. Holder, Jr. High-Tech Crime Summit January 12, 2000, http://www.usdoj-crm/mis/mdf (aplūkots 2000.gada 21. oktobrī)

142 [b.a.]High technology crime in California. Annual report on high technology crime in California. Prepared by High tech crime advisory committee, 2000, p. 8.

dimensijās, piemēram, pēc darbības veida vai noziegumu subjekta veida, vai tas ir iekšējais vai ārējais noziegums u. c.

Beidzot kibernozieguma jēdziena apskatu, mazliet paskatīsimies uz to, kas mūs gaida tuvākā nākotnē. Juridiskajā literatūrā, piem., U. Sībers[143], R. Morgesters u.c., plaši izplatīts viedoklis, ka, pieaugot sabiedrības integrācijas pakāpei, pieaugs arī dažādi apdraudējuma riski. Kibernoziegumi kļūs daudz mobilāki un starptautiski. Interneta piedāvātās iespējas noziedzīgos nolūkos izmantos arī organizētā noziedzība. Savukārt tas radīs jaunas diskusijas par kibernoziegumu, augsto tehnoloģiju noziegumu, datortīklu noziegumu, noziegumu informācijas jomā u.c. saturu.

Iepriekšminētais liecina par dziļo pretrunu starp tradicionālo informāciju un elektronisko informācijas – datu, kas ir speciāli IS apstrādei paredzēts informācijas veids, vērtību. Informācijas sabiedrības doktrīnas[144] piekritēji uzskata, ka dati ir brīvi un ka informācija pieder mums visiem. Piederības un īpašuma izpratne informācijas tehnoloģiju laikmetā ievērojami mainās. Informācija, kas ir tikpat visuresoša kā gaiss un lēta kā smilts, tā ir datora izejmateriāls un īpašums pats par sevi.[145]No tā izriet secinājums, ka tas, kas kontrolē informāciju un kuram ir pieeja informācijai, patiesībā valda pār sabiedrību, un šie procesi nav atdalāmi.

Kāpēc juristu sabiedrība pasaulē tomēr ir pieņēmusi savā leksikā šo koplietošanas terminu "kibernoziegums"? Kibertelpa ir nosacīta "telpa", kas veidojas mijiedarbībā starp datoriem, datortīkliem, citiem vārdiem sakot, "kibertelpa ir tas viss, kas ir otrā pusē aiz datora ekrāna".[146] Tātad šajā terminā ir ietverti visi elementi, kas nepieciešami, lai nodrošinātu pārrobežu informācijas plūsmu, izmantojot automātiskās datu apstrādes sistēmas un datortīklus. Līdz ar to vārdu savienojums ar 1.daļu *kiber* -ir visprecīzākais veids, kas attēlo jaunizveidotā

---

[143] Ibid., Dr. Ulrich Sieber, p.64.

[144] Informācijas sabiedrības doktrīna ir saistīta ar informācijas tehnoloģiju izmantošanu kā sabiedrības labklājības sastāvdaļu. Respektīvi, informācijas sabiedrība ir spēja nodrošināt sabiedrību ar kvalitatīvu informāciju. To ietekmē divi faktori, proti, informācijas globālais raksturs un pieaug speciālistu skaits, kas speciāli sagatavoti šīs informācijas apstrādei. Sk. Ķinis U. Tiesības informācijas sabiedrībā. Latvija un Eiropas Savienība Nr. 18. 2000.gada decembris,36.-43.lpp.

[145] Recombinant Culture: crime in the digital network by Curtis E.A. Karnow Landels, Ripley& Diamond Defcon II Las Vegas July 1994 Sk. http://www.cpsr.org/cpsr/privacy/crime/karnow.html (aplūkots 2000.gada 21. oktobrī)

[146] Real law@ virtual space regulation in cyberspace. ed. by Susan J. Drucker, Garry Gumpert, Hampton press Inc.1999.,-p.3.

medija būtību un precīzi parāda šo noziegumu veidu sabiedrisko bīstamību. Zaporožjes milicijas skolas docents V. Golubevs[147] uzskata, ka kibernoziegumu paaugstināto bīstamību nosaka:

- datorsistēmu, kas nodrošina sabiedrības dzīvībai svarīgas funkcijas, vārīgums un atkarība no interneta tīkla;
- pieaugošie izdevumi informācijas sistēmu drošībai, lai nodrošinātu informācijas un tehnisko resursu integritāti jebkurā pasaules valstī;
- starptautiskās likumdošanas nepilnības un starptautiskās sadarbības trūkums.

Šos secinājumus apstiprina vairāki pētījumi kibernoziegumu jomā. Tā, piemēram, Trento Universitātes pētījums liecina, ka ekonomiskie noziegumi var ietekmēt informācijas revolūciju divos veidos.

Pirmkārt, iedarboties tieši uz informāciju kā vērtību, tādā veidā iegūstot peļņu, piemēram, veicot kiberspiegošanu, kaitniecību. Tādā gadījumā likumpārkāpēju darbība ir tieši atkarīga no izmantoto augsto tehnoloģiju sarežģītības pakāpes un to izmantošanas prasmes.

Otrkārt, informācija var būt arī netiešs uzbrukuma mērķis. Tā var tikt izmantota kā dažādu noziedzīgu grupu mācību process, lai sagatavotu liela mēroga, plaši sazarotu noziegumu struktūru, piemēram, starptautisku krāpšanu, netīrās naudas atmazgāšanu. Noziedznieki vispirms uzkrāj informāciju, pēc tam to analizē un, atklājot dažādu valstu likumdošanas vājās vietas, izstrādā rīcības plānu un to īsteno.[148]

Kibernoziegumi juridiskajā literatūrā tiek uzskatīti par jauna veida juridisku fenomenu. Tomēr tiem jābūt aizliegtiem vai ierobežotiem ar krimināllikumu, un par šādu nodarījumu jābūt sodam. Tātad kibernozieguma jēdziena prioritārā pazīme ir prettiesiska darbība vai bezdarbība, kas aizliegta konkrētas valsts krimināllikumā. Visus kibernoziegumus vieno tas, ka tie visi ir izdarīti jaunā vidē- kibertelpā, kas

---

147 Cyber-crime and legal problems of Internet usage by Goubev Vladimir. (wysiwyg://84html://www.networkremotemonitor.com/articles/cyber/cyber.html (aplūkots 2000.gada 2. jūnijā)

148 When economic crime becomes organized: the role of information technologies.A case study. http://www.transcrime.unitnt.it (aplūkots 2001.gada 21. janvārī)

var rasties tikai tad, ja tiek izmantotas informāciju un komunikāciju tehnoloģijas, tai skaitā datori datortīkli, datorprogrammas, telekomunikācijas u.c. Kibernoziegumus atšķirībā no tradicionāliem nodarījumiem raksturo paaugstināta sabiedriskā bīstamība gan nacionālā, gan pārnacionālā mērogā.

Pamatojoties uz iepriekšteikto, kibernoziegumu var definēt, kā

*jebkuru tīšu nelikumīgu, krimināli sodāmu darbību, kur informācijas tehnoloģijas (automātiskās datu apstrādes sistēmas, komunikācijas līdzekļi, t.sk, datu pārraides vai telekomunikāciju tīkli u. c.) izmantoti kā nozieguma priekšmets vai nozieguma rīks ar mērķi ietekmēt informācijas sistēmu tehniskos un informācijas resursus vai arī kā medijs nelikumīgas informācijas aprites procesā.*

Šī definīcija uzskatāmi parāda, ka kibernoziegumi nav principiāli jauna veida noziedzīgi nodarījumi. Tiem piemīt visas tradicionālam noziedzīgam nodarījumam nepieciešamās pazīmes (prettiesiskums un soda piedraudējums). Tomēr minētā definīcija parāda arī principiālu atšķirību no klasiskā noziedzīga nodarījuma jēdziena: 1) par kibernoziegumu var atzīt tikai personas tīšu darbību, izslēdzot atbildību par bezdarbību un nodarījumu aiz neuzmanības; 2) šai darbībai ir jābūt saistītai ar informācijas apriti kibertelpā; 3) šīs darbības var izdarīt, izmantojot vai ietekmējot informācijas sistēmu resursus; 4) šie nodarījumi izdarīti attālināti, tas ir, tieši, fiziski neiedarbojoties uz IS resursiem.

## II nodaļa Kibernoziegumu sastāvs (*corpus delicti*)

### 1. Vispārīgā noziedzīga nodarījuma sastāva analīze

#### 1.1. Jēdziens

Noziedzīgā nodarījuma vispārīgais jēdziens atklāj bīstamās uzvedības sociāli politisko raksturojumu, nosaka, kāpēc tā jāatzīst par noziedzīgu, un palīdz noteikt nozieguma vispārīgās kvalificējošās pazīmes. Juridiskajā literatūrā nav vienota viedokļa par to, ko apzīmēt ar nozieguma sastāva pazīmēm un ko nosaukt par elementiem. Tomēr neapšaubāmi šādai klasifikācijai ir jābalstās uz filozofijas un loģikas likumiem par veselā un atsevišķā attiecību, tas ir, ka elements ir kaut kā vesela sastāvdaļa.[149] Tāpēc juridiskajā literatūrā dominē viedoklis, ka par

---

[149] The Internet Encyclopedia of phylosophy. Category http://www.utm.edu/research/iep/c/category.htm (aplūkots 2003.gada 19. oktobrī)

noziedzīga nodarījuma sastāva elementiem uzskatāmi: 1) objekts, 2) objektīvā puse, 3) subjekts; 4) subjektīvā puse. Ar nozieguma sastāva pazīmēm jāsaprot nozieguma elementu saturs.[150] V. Kudrjavcevs norāda, ka nozieguma sastāva pazīmei ir jābūt apveltītai ar tādām īpašībām kā, piemēram, radniecību, īpatnību, savdabību. Kopumā tām jāatbilst šādām prasībām: 1) kopā ar citām pazīmēm jānosaka nodarījuma bīstamība, prettiesiskums, vainojamība un sodāmība; 2) jāizsaka tā atšķirība no citiem noziegumiem un tiesībpārkāpumiem; 3) jābūt tieši norādītai likumā vai likuma tulkošanas gadījumā nepārprotami jāizriet no tā; 4) tā nevar būt atvasināta no citām pazīmēm; tai jāpiemīt visiem attiecīgā veida nodarījumiem.[151] Nav pamata apstrīdēt iepriekšminēto autoru secinājumus, jo nenoliedzami elements ir veselā sastāvdaļa, bet tā juridiskā nozīme rodas tikai tajā brīdī, kad tā saturu noteic īpašības- pazīmes, kas attiecīgo elementu nošķir no citiem un individualizē.

Juridiskajā literatūrā nav vienota viedokļa par pazīmju iedalījumu, taču dominējošais viedoklis ir, ka pazīmes dalāmas pamatpazīmēs un speciālās pazīmēs.[152] Piem., U. Krastiņš pauž viedokli, ka nozieguma sastāva pamatpazīmes piemīt visiem noziegumu sastāviem neatkarīgi no tā, kādā veidā tie izpaužas. Pie tādām pazīmēm viņš pieskaita ar noziegumu apdraudētās intereses, noziedzīgo darbību vai bezdarbību, vainas formu, krimināllikumā noteikto vecumu personas saukšanai pie atbildības, pieskaitāmību.[153] Ja kādas no šīm pazīmēm nav, tad personas rīcībā nav nekāda noziedzīga nodarījuma sastāva.

Š. Dando secina, ka noziedzīgam nodarījumam piemītošo pazīmju prettiesiskums un vainojamība dod iespēju izveidot „stereotipiskus" noziegumu, piemēram, slepkavība, zādzība u.c., sastāvus.[154] Līdzīgu domu pauž arī V. Jegorovs, norādot, ka „stereotipiskums" jeb „abstraktums" saistīts ar objektīvas realitātes atspoguļojumu, kas atspoguļo kaut ko pastāvīgu, pastāvošu, noturīgumu. Līdzīgu viedokli atbalsta arī P. Lejiņš, norādot, ka dispozīcijā dotajam abstraktajam

---

150 Krastiņš U. Mācība par nozieguma sastāvu. Rīga: Zvaigzne ABC, 1996., 13.lpp.

151 Кудрявцев В.Н. Общая теория класификациии преступлений. Москва: Res cottidiana. Юристь,2001,с. 94-95

152 Уголовное право. Общая часть. Под ред. И.Я. Казаченко, З. А. Незнамова. Москва: Инфра · М- Норма, 1997, с.177

153 Turpat, Krastiņš U., 15. lpp.

154 Ibid., Shigemitsu Dand.op. 3 ;Ibid., Еоров В.С.,с.6

sastāvam piemīt tikai nepieciešamās, bet tai pašā laikā arī pietiekamas pazīmes, lai raksturotu kādu konkrētu gadījumu.[155] Tieši nozieguma sastāva vispārīgais jēdziens dod teorētisko pamatu, lai pilnīgāk atklātu konkrēta noziedzīga nodarījuma saturu. Šādu viedokli, kas noziedzīga nodarījuma sastāvu nosauc par „modeli" vai „abstrakciju", kritizē G. Novoselovs, motivējot ar to, ka neviens juridiskajā literatūrā neraksta, ka nozieguma objekts ir nereāla sociāli - tiesiska parādība, kas izpaužas modelētā vai zinātniski abstraktā personu, sabiedrības, valsts tiesisko attiecību un ar likumu aizsargāto interešu aizstāvībā.[156] Neapstrīdot G. Novoselova argumentus par noziedzīga nodarījuma objekta kā reālas sociālas parādības esamību, nevar piekrist tam, ka objekts un citi noziedzīga nodarījuma elementi bez to konkretizācijas, t.i., apveltīšanas ar tikai tiem raksturīgām pazīmēm, var paši par sevi kļūt par krimināLatbildības pamatu.

Krimināllikumā ietvertais noziedzīgā nodarījuma sastāvs pats par sevi jau nerada krimināltiesisko atbildību. A. Naumovs raksta, ka„.. noziedzīga nodarījuma jēdziens ir ietverts likumā. Tas apzīmē katram noziegumam raksturīgās sociālās un juridiskās pazīmes (prettiesiskumu, sabiedrisko bīstamību, vainojamību un sodāmību), bet noziedzīga nodarījuma sastāvs ir krimināltiesību zinātnes termins, jo tas nav definēts krimināLajā likumdošanā"[157].

Atbildība iestājas tikai tad, ja tiek konstatēts konkrētā nodarījuma sastāvs, tas ir, krimināllikumā paredzēto objektīvo un subjektīvo pazīmju kopums, kas individualizē un raksturo ar pazīmēm konkrētā noziedzīgā nodarījuma elementus, respektīvi, veido šīs tiesiskās parādības veselumu reālā vidē.

Juridiskajā literatūrā dominē viedoklis, ka „.. personas krimināLatbildība iestājas, pastāvot šādiem nosacījumiem: 1) konstatēts bīstamais nodarījums (darbība vai bezdarbība); 2) nodarījumam ir tāda kaitīguma pakāpe, kas raksturīga noziegumam; 3)persona vainīga nodarījumā; 4) nodarījums ir paredzēts krimināllikumā."[158]

---

[155] Turpat, Docents Lejiņš P., 32.lpp.

[156] Уголовное право. Общая часть. Под ред. И.Я.Казаченко, З. А. Незнамовой. Москва: Инфра · М- Норма, 1997, С.179

[157] Ibid., Флетчер Д ., Наумов А.В. с.209

[158] Krastiņš U. Mācība par nozieguma sastāvu. Rīga: Zvaigzne ABC, 1996., 7.lpp.

Analogu domu paužA. Naumovs[159], G. Novoselovs, Klarksons[160], S. Brennere un citi autori.

Neesot kādam no šiem nosacījumiem, krimināatbildība iestāties nevar. No iepriekšteiktā var secināt, ka noziedzīgā nodarījuma jēdziens ir abstrakta kategorija, kura nepieciešama, lai noteiktu krimināltiesību darbības pamatprincipus, tas ir, pamatu, uz kura veidot attiecīgās valsts krimināltiesisko politiku. Krimināllikuma 1.un 6.p. pants noteic, ka pie krimināatbildības ir saucama tikai tā persona, kas izdarījusi krimināllikumā paredzētu nodarījumu, kuram ir **visas noziedzīgā nodarījuma sastāva pazīmes.**[161]

Tātad noziedzīgā nodarījuma jēdzienam ir cieša saikne ar noziedzīgā nodarījuma sastāva (*corpus delicti*) jēdzienu. V. Jegorovs norāda, ka šī saikne ir ļoti svarīga, jo nozieguma jēdzienā atklājas tā materiālās pazīmes, kas izpaužas noziedzīgās uzvedības bīstamībā, tas ir, tajā kaitējumā, ko tā var nodarīt ar likumu aizsargātām sabiedriskām attiecībām[162], bet nozieguma sastāvs- tiesiska kategorija, kas izpaužas Krimināllikuma sevišķās daļas dispozīcijā, kas satur konkrētā ar likumu aizliegtā sabiedriski bīstamā nodarījuma pazīmes.

Ar terminu „pazīme" parasti saprot savrupa priekšmeta vai parādības īpatnības, pēc kurām tos var atšķirt no citiem. Jāpiekrīt V. Kudrjavcevam[163], U. Krastiņam un citiem autoriem, kas pamatoti norāda, ka, „.. izveidojot nodarījuma sastāvu, likumdevējs abstrahējas no konkrētu nodarījumu pazīmēm un noziedzīga nodarījuma sastāvā ietvēris tikai tās pazīmes, kas kopīgas visiem noteikta veida nodarījumiem".[164]

Piemēram, konstruējot Krimināllikuma 241.panta2.daļā.paredzēto noziedzīga nodarījuma sastāvu patvaļīgai piekļūšanai datorsistēmai, likumdevējam jāizceļ tādas pazīmes, kas raksturotu šādu nodarījumu tipiskumu. Piemēram, piekļuvei datorsistēmai ir jābūt patvaļīgai, tā varbūt tikai darbība, darbībai jābūt tīšai ar tiešu vai netiešu nodomu, piekļuvei ir jābūt cēloniskā sakarībā ar radīto iespēju iepazīties ar informāciju vai saistītai ar datortehnikas programmatūras aizsarglīdzekļu pārvarēšanu vai ar pieslēgšanos sakaru līnijām. Respektīvi, krimināprocesa virzītājs, piemērojot šīs tipoloģiskās

---

159 Наумов А.В. Росийское Уголовное право. Общая часть. Курс лекций. издательство БЕК, 1996., с. 135; Учебник Уголовного права. Общая часть. Под. ред. В.Н. Кудрявцева и А.В. Наумова. Москва: Спарк, 1996, с. 35

160 Ibid., Clarkson C.M.V. p. 13

161 Baltkrievijas Republikas Kriminākodeksa 11.p. noziegumu definē kā vainojamu sabiedriski bīstamu nodarījumu (darbību vai bezdarbību) , ko raksturo šajā kodeksā paredzētās pazīmes un kas aizliegtas ar soda piedraudējumu.

162 Ibid., Егоров В.С. с.8

163 Кудрявцев В.Н. Общая теория класификациии преступлений. Москва: Res cottidiana. Юристь,2001, с. 94-95

164 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 13.lpp.,

pazīmes, automātiski atsijās ārpus iepriekšminētajām pazīmēm esošus raksturojošus lielumus, piemēram, bezdarbību, neuzmanīgu rīcību, autorizētu piekļuvi u.c., jo tās neietilpst šī nodarījuma stereotipisko pazīmju kopumā, tādējādi nevar būt par pamatu personas saukšanai pie kriminālatbildības.

Tomēr šāds noziedzīga nodarījuma sastāvs pats par sevi nevar būt par pamatu, lai sauktu personu pie atbildības par patvaļīgu piekļūšanu datorsistēmām, kamēr tā netiek realizēta dzīvē.[165] Līdz ar to jāpiekrīt, ka teorijā nozieguma nodarījuma sastāvs ir tikai zinātniska abstrakcija, kas pati par sevi nerada tiesiskās sekas. Noziedzīga nodarījuma sastāva formulēšanai ir svarīga loma gan krimināltiesību teorijas attīstībā, gan krimināltiesību praktiskā lietojumā. Piemēram, viens no krimināltiesību zinātnes uzdevumiem ir teorētiski konstruēt jauna veida apdraudējumu sastāvus. Tas nozīmē atrast tādas pazīmes, kas vispirms jau ietver visas noziedzīgam nodarījumam raksturīgās pazīmes un papildus tās, kuru intensitātes pakāpe[166] sasniedz vai var sasniegt lielu smagu kaitīgumu jeb ievērojami apdraudēt sabiedrības ar likumu aizsargātās intereses.

Modelējot teorijā kāda nodarījuma sastāvu, krimināltiesību zinātnieki sagatavo likumdevējam ieteikumus par tā vai citu nodarījuma ietveršanu Krimināllikumā. Ja likumdevējs atzīst krimināltiesību teorijā izstrādāto modeli un dod tam sociāli politisku novērtējumu, tad ar likuma spēkā stāšanās brīdi teorētiski modelētais nodarījums no delikta kļūs par noziedzīgu nodarījumu. Diemžēl praksē ir sastopami gadījumi, kad attiecīgās darbības vai bezdarbības kriminalizācija ir saistīta ar politisko konjuktūru un konkrētās darbības vai bezdarbības aizliegums vai ierobežojums Krimināllikumā iekļauts vairāk politisku kā juridisku iemeslu dēļ. Demokrātiskā sabiedrībā konkrētas darbības vai bezdarbības kriminalizēšana ir ekskluzīva likumdevēja tiesība, līdz ar to nenoliedzami politiskās konjunktūras jautājums. Tāpēc izbēgt no šādām kļūdām nav iespējams.

Juridiskajā literatūrā visbiežāk pārstāvēts viedoklis, piemēram, A. Naumovs, U. Krastiņš, K. Klarka, A. Ašvorts V. Jegorovs, G. Novoselovs, u.c. [167], kas par

---

165 Turpat, Krastiņš U., 14. lpp.

166 Кудрявцев В.Н. Общая теория квалификации преступлений. Москва: Res cottidiana.Юристь,2001,с.95

167 Наумов А.В. Росийское Уголовное право. Общая часть. Курс лекций. Москва: издательство БЕК, 1996., с. 135; Учебник Уголовного права. Общая ч. Под. Ред. В.Н. Кудрявцева и А.В. Наумова. Москва: Спарк, 1996. с.136; Krastiņš U. Noziedzīgs nodarījums. Rīga- TNA, 2000.8.lpp.; Catherine Therese Clarke. From criminet to cyber perp: towards an inclusive approach to oicing. The involving criminal means rea on the Internet. Oregon law review, Spring., 1996.; Ibid., A.P. Simester, G.R. Sullivan, p.21;Ibid., Clarkson C.M.V. p. 14; Ibid., Еропов В.С. с.8; Criminal law in Denmark by Lars

nozieguma sastāvu (*corpus delicti*) atzīst konkrētā noziedzīgā nodarījuma objektīvo un subjektīvo pazīmju kopumu. Noziedzīga nodarījuma sastāvs rodas tikai tad, kad abas pazīmes- gan objektīvās gan subjektīvās[168]- sakrīt laikā. Šis viedoklis ir pamatots, un jāpiekrīt, ka „..noziedzīga nodarījuma sastāvs ir krimināllikumā paredzēto visu objektīvo un subjektīvo pazīmju kopums, kas nepieciešams, lai atzītu nodarījumu par noteikta veida noziedzīgu nodarījumu."[169] Iepriekšminētie autori par nozieguma sastāva elementiem atzīst pazīmes: 1) kas raksturo nozieguma objektīvo vai ārējo materiālo izpausmi, tas ir, noziedzīga nodarījuma objektu un objektīvo pusi ; 2) subjektīvo jeb psiholoģisko pazīmju kopumu, tas ir, subjektīvo pusi un subjektu.

### 1.2. Nozieguma sastāva elementu salīdzinošā analīze

Rietumu tiesību doktrīnā nereti *corpus delikti* atzīst par teorijā sastopamo terminu *actus reus* un *mens rea* kopību.

Angļu juridiskajā literatūrā ir sastopamas vairākas pieejas noziedzīgu nodarījumu pazīmju konstatēšanā, piemēram, Lielbritānijas Lordu palāta krimināllietā *House of lords in Miller* (1983)[170] atzina, ka šie latīņu termini *actus reus*, *mens rea* pārsvarā aptver tikai subjekta aizliegto darbību, nodarīto kaitējumu un prettiesiskumu, bet neietver attaisnojošās uzvedības trūkumu. Tāpēc attaisnojošās uzvedības trūkums (*absence of valid defence*) tiek uzskatīts par noziedzīga nodarījuma kvalifikācijas trešo elementu. Šāda likumīgās aizstāvības vai attaisnojošo elementu izcelšana ir sastopama starptautiskās konvencijās un līgumos, kas regulē krimināltiesisko sfēru. To izskaidro ar nepieciešamību aizsargāt indivīdu pret pārmērīgu valsts rīcību, nodrošinot krimināltiesībās garantiju mehānismu, kas izriet no Eiropas Cilvēktiesību konvencijas un citiem starptautiskiem cilvēktiesību dokumentiem.

Analizējot citu valstu krimināltiesību teorijā izmantoto *actus reus* un *mens rea* būtību, jāsecina, ka minēto terminu kopums neatbilst tam saturam, ko mēs saprotam ar noziedzīga nodarījuma sastāvu Latvijas krimināltiesību doktrīnā. Tradicionāli ar *actus reus* saprot tikai nodarījuma objektīvo pusi[171], tas ir, darbību vai bezdarbību,

---

Bo Langsted, Vagn Greve, Peter Garde, The Hague·London·Kluwer law international, 1998., p.76-77. ; Ashworth Andrew Principles of Criminal law.Third edition/ Oxford University Press,[b.g.] p.99

168 Dažu valstu krimināltiesību zinātnē, piemēram, Francijā, un Dānijā, Itālijā, nereti objektīvo un subjektīvo pazīmju vietā tiek izmantots dalījums materiālās ( *elements materiels*) un morālās pazīmes (*elements orals*), kas kopā veido noziedzīga nodarījuma sastāvu (*constitution de l'incrimination*), sk. Уголовное право зарубежных стран Общая часть. под ред. проф. И.Д.Козочкина. Москва: Омега –Л, 2003.,С. 274.,521; Ibid., Shigemitsu Dando. .5

169 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 10.lpp.; Учебник Уголовного права. Общая часть. Под. ред. В.Н. Кудрявцева и А.В. Наумова с.77; Уголовное правою Общая часть. Учебник для вузов. Москва: Инфра· М–Норма, 1997., с.114б,169 Егоров В.С. Понятие состава преступления в уголовном праве. Уч.пособие. Москва: Московский психолого социальный институт, 2001.,с.4

170 Clarkson C.M.V. Understanding Criminal law , London. Sweet & Maxwell, 2001. p. 16

171 Vispārējo un Rietumvalstu tiesību doktrīnā dominē viedoklis, ka *actus reus* sastāv no trīs elementiem : uzvedības, sekām un apstākļiem Criminal law theory and doctrine by A.P. Simester, G.R. Sullivan, p.59.; Criminal law in Denmark by Lars Bo

cēloņsakarību un kaitējumu, bet ar *means rea* personas vainojamību. Tomēr ASV juridiskajā literatūrā ir sastopams arī cits viedoklis, proti, ka *actus reus* ir tikai notikusī darbība vai bezdarbība, bet aizliegtais rezultāts un kaitējums nodalīts atsevišķi.

Uzskatāmi to atklāj K. Klarka, norādot, ka, lai ASV jurisdikcijā personas uzvedību atzītu par noziedzīgu, ir nepieciešami šādi priekšnoteikumi: 1) darbībai ir jābūt notikušai (*actus reus*);2) darbības izdarītājam ir jākonstatē ļauns nodoms (*means rea*);3) *actus reus un means rea* ir jānotiek vienlaikus; 4) notikumam ir jārada kaitējums; 5)\uzvedībai ir jābūt tiešā cēloniskā sakarā ar radušos kaitējumu; 6)personai, kura iesaistīta nodarījumā, ir jābūt krimināltiesību subjektam; 7)uzvedībai ir jābūt izliegtai ar likumu un krimināli sodāmai.[172]

Savukārt profesore S. Brennere norāda, ka „..vispārīgo tiesību doktrīnā noziedzīgs nodarījums sastāv no četriem elementiem: 1) uzvedības –*actus reus* darbība vai bezdarbība (*conduct*); 2) garīgā stāvokļa- *mens rea* (*mental state*); 3) blakus apstākļiem, nepieciešamiem konkrētiem nodarījuma apstākļiem (*attendant circumstances*); 4) aizliegtā rezultāta vai kaitējuma (*forbiden result or harm*). [173] Kaut gan vispārējo tiesību valstīs nav vienota viedokļa par noziedzīga nodarījuma saturu, tomēr praksē dominē Millera[174] lietā pieņemtais tiesu precedents, t.i., *actus reus* un *means rea* kopība papildināta ar trešo elementu, proti, attaisnojošas uzvedības trūkumu.

Rietumvalstu juridiskajā literatūrā[175] pastāv arī viedoklis, kas apšauba zinātnisku nepieciešamību nodalīt noziedzīgā nodarījuma klasifikācijā objektīvos un subjektīvos elementus.

Japāņu profesors Š. Dando uzskata, ka objektīvo un subjektīvo pazīmju nodalījumam krimināltiesību teorijā trūkst racionāla pamata. Savu viedokli viņš motivē ar to, ka nozieguma sastāvs ir „vainojamas darbības stereotips".[176] Viņš

---

Langsted, Vagn Greve, Peter Garde, The Hague·London·Kluwer law international, 1998., pp.83-92; Clarkson C.V. Understanding Criminal law , London. Sweet & Maxwell, 2001. p. 14 u.c.

172 Catherine Therese Clarke. From criminet to cyber perp: towards an inclusive approach to oicing. The involving criminal means rea on the Internet. Oregon law review, Spring, 1996; Analogu viedokli pauž dāņu kriminālisti, ka aizliegtās darbības vai bezdarbības apraksts satur actus reus. Sk. Criminal law in Denmark by Lars Bo Langsted, Vagn Greve, Peter Garde, The Hague·London·Kluwer law international, 1998., p.76-77; Clarkson C.M.V. Understanding Criminal law , London. Sweet & Maxwell, 2001. p. 14

173 Brennere Sūzana Kibernoziegumi un tradicionālie noziedzīgie nodarījumi: juridisko problēmu analīze.// Likums un tiesības 4. sējums Nr. 9 (37), Septembris 2002. ,269.-278. lpp.

174 US Supreme Court. Miller v California 413 U.S. 15. (1973)
http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=413&invol=15 (aplūkots 2003.gada 21. janvārī)

175 Ibid., Simester A.P., Sullivan G.R., p.59; Ibid., Shigemitsu Dando, pp. 6-10

176 Saskaņā ar Japānas krimināltiesību doktrīnu nozieguma sastāvu raksturo: 1) realizētais nodarījums un rezultāts; 2) nozieguma sastāvs ir abstrakts, tipoloģisks noziedzīgā nodarījuma atainojums, kaut kas vispārināts un abstrakts. Sk.

uzskata, ka„.. noziedzīgā nodarījuma sastāvam pietiek, ja konstatē attiecīgam noziedzīgam nodarījumam paredzēto kvalificēto darbību, un nav nepieciešams to sasaistīt ar izdarītāja personību, jo darbība ir individualitātes pazīme."[177] Līdzīgu viedokli paudis arī A. Traiņins, norādot, ka„.. subjekts nav noziedzīga nodarījuma sastāva elements, jo noziedzīgā nodarījuma pazīmes tikai raksturo nodarījumu, t.i, norobežo subjektu loku, kas nevar būt atbildīgi par konkrēto nodarījumu.[178]

Šāds viedoklis PSRS krimināltiesību doktrīnā neguva atbalstu un tika kritizēts, motivējot ar to, ka noziedzīga nodarījuma sastāvu var veidot tikai subjektīvo un objektīvo pazīmju vienotība, jo bez personas- subjekta -nevar būt arī darbības. Zviedrijas Upsalas universitātes profesors N. Jareborgs. raksta: „Zviedru juristi parasti runā par nozieguma objektīvo un subjektīvo pusi, tomēr šāda terminoloģija ir maldinoša, jo mēs varam atrast daudz subjektīvu elementu objektīvajā pusē un subjektīvā puse satur arī objektīvās puses rakstura elementus. Tāpēc nav pareizi runāt par divām nozieguma pusēm, ja šeit pilnīga simetrija divām priekšnosacījumu grupām".[179] N. Jareborgs nenoliedz, ka nozieguma sastāvu veido abu (objektīvo un subjektīvo) pazīmju kopums, bet tikai uzsver, ka nevienu nozieguma elementu nevar apskatīt atrauti no citiem, jo visi tie ir savstarpēji saistīti. Nav šaubu, ka noziedzīga nodarījuma sastāvu nevar apskatīt vai nu tikai no objektīvo pazīmju redzespunkta vai otrādi, t.i., no subjektīvo pazīmju puses. Noziedzīga nodarījuma sastāva analīze būs iespējama tikai tad, ja tiks analizētas abu pazīmju grupas vienlaicīgi un kopsakarībās.

Latvijas krimināltiesību zinātne un prakse vēsturiski atbalsta viedokli, ka noziedzīga nodarījuma sastāvs ir krimināllikumā ietverto noziedzīgo nodarījumu kopīgo stabilo pazīmju un likumsakarību kopums, kas raksturīgs konkrētiem noziedzīgiem nodarījumiem. Tā, piemēram, P. Mincs definē noziedzīga nodarījuma

---

Уголовное право зарубежных страню Общая часть. под ред. проф. И.Д.Козочкина. Москва- Омега –Л, 2003.,с. 438; Уголовный кодекс Грузии. Санкт-Петербург –Юридический центр Пресс,2002.,с.19

177 Ibid., Shigemitsu. Dando p. 5.

178 Citāts no Курс Советского уголовного права в шести томах. Том 2-ой. Часть общая "Преступление" п. ред. А.А. Пионтковского. Москва: Наука, 1970, с. 97

179 Essays in Criminal law Nils Jareborg Iustus Förlag. Juridiska Förennigen i Uppsala,[b.g.] p. 11

sastāvu kā „..pretlikumīgu, vainojamu, sodāmu cilvēka uzvešanos, kas atbilst vienam no tipiskiem sastāviem".[180]

Tādējādi jau vēsturiski Latvijas krimināltiesību teorijā un praksē par noziedzīga nodarījuma sastāva elementiem atzīst objektīvās pazīmes- nodarījuma ārējo izpausmi (objektu un objektīvo pusi) un nodarījuma iekšējo jeb subjektīvo pusi (subjektu un subjektīvo pusi nodoma vai neuzmanības formā), un šī viedokļa pārvērtēšanai un jaunu teoriju radīšanai nav pamata.

## 2. Noziedzīga nodarījuma objekts

### 2.1. Jēdziens

Katram noziedzīgam nodarījumam ir jāsatur apdraudējuma objekts. Jautājums par noziedzīgā nodarījuma objektu tiesību zinātnē ir aktuāls kopš XVIII gadsimta, kad tika veikti pirmie mēģinājumi noziedzīgo nodarījumu grupēšanā. Juridiskajā literatūrā nav vienotas pieejas noziedzīgo nodarījumu klasificēšanā. Rietumeiropā plaši lietota noziedzīgu nodarījumu dalīšana 5 grupās: 1) sabiedriskie noziegumi, 2) ģimenes noziegumi, 3) noziegumi pret atsevišķu fizisku un juridisku personu tiesībām, 4) noziegumi pret personu; 5) mantiskie noziegumi. Šādu noziegumu dalījumu ar nelielām atšķirībām izmantoja gan Francijā, gan Krievijā, Vācijā, Itālijā un citās valstīs.

Ja salīdzinām Latvijas krimināltiesību zinātnē pieņemto noziedzīgā nodarījuma definīciju ar vispārējo valstu krimināltiesību doktrīnā pieejamo, tad redzams, ka šajās valstīs ne praksē, ne arī teorijā faktiski terminu "noziedzīga nodarījuma objekts" nepiemēro. Spriežot pēc Vispārīgo tiesību un Rietumvalstu krimināllikumiem, šajās valstīs tiek izšķirti šādi objekti: noziegumi pret valsti, noziegumi pret sabiedrību un noziegumi pret personu. Tā, piem., ASV Deitonas Universitātes rīkotajā virtuālajā kibernoziegumu kursā klausītāji sagatavoja Kibernoziegumu paraugkodeksu, kurā tika izmantots šāds iedalījums: 1) noziegumi pret personu (slepkavība, virtuālā uzmākšanās, nonāvēšana aiz neuzmanības, virtuālais vojerisms u.c.); 2) seksuālie noziegumi (noziegumi pret nepilngadīgiem, neķītru materiālu publicēšana, prostitūcija un ar to saistītie nodarījumi, virtuālā

---

[180] Turpat, Mincs P., 61. lpp.

izvarošana u.c.); 3) noziegumi par personu mantisko tiesību traucēšanu un bojāšanu (noziegumi pret informācijas sistēmu drošību, datorvandālisms u.c.); 4) zādzība un krāpšana (datorkrāpšana un datorzādzība, identitātes zādzība, datorinformācijas zādzība u.c.); 5) noziegumi pret morāli (azartspēles, alkohola un tabakas piedāvājums internetā); 6) noziegumi pret valdību (terorisms, pretdarbība varas iestādēm u.c.).[181] Teorijā ir aplūkoti arī citi sadalījuma veidi, piemēram, vairākās Lielbritānijā izdotajās krimināltiesību teorijas grāmatās noziedzīgie nodarījumi pret personu mantu apzīmēti kā negodīgi noziegumi. Jāpiekrīt S. Brenneres viedoklim, ka Rietumvalstīs ar atsevišķām niansēm noziegumus parasti iedala četrās pamatgrupās: 1) noziedzīgi nodarījumi pret personu; 2) noziedzīgi nodarījumi pret īpašumu; 3) noziedzīgi nodarījumi pret valsti; 4) noziedzīgi nodarījumi pret morāli.[182]

Noziedzīgo nodarījumu grupēšana radīja nepieciešamību attīstīt teorijas par noziedzīga nodarījuma objektu. Definējot noziedzīga nodarījuma objektu, vienprātība valda tikai jautājumā, ka nozieguma objekts ir tikai tas, uz ko vērsts apdraudējums, un ka šim apdraudējumam (konkrētam vai abstraktam) ir jāaizskar konkrētu personu vai personu grupu (indivīda, sabiedrības vai valsts) likumīgās tiesības un intereses. Taču uz ko tas ir vērsts un kas ir šī konkrētā vai abstraktā apdraudējuma saturs, viedokļi dalās.

G. Novoselovs[183] uzskata, ka nozieguma objektu nevar definēt, to cieši nesaistot ar kaitējuma būtību un mērķi. Ja konstruktīvi analizē nozieguma objektu, tad vienlaicīgi jāievēro tas, kas ar noziegumu tiek pārkāpts, kas nozieguma izdarīšanas brīdī tiek ietekmēts; kas izmainās šīs darbības ietekmē un kurš cieš kaitējumu. Visas šīs raksturiezīmes ir cieši saistītas. Pirmsrevolūcijas Krievijas perioda krimināltiesību teorijā tika izvirzītas vairākas nozieguma objekta teorijas, bet, kā norāda G. Novoselovs, tad juridiskajā literatūrā dominēja viedoklis, ka noziedzīga

---

[181] The University of Dayton School of law. Cybercrimes. Cybercrimes model state computer crimes code. Fall. 1999.

[182] Brenneres Sūzana Kibernoziegumi un tradicionālie noziedzīgie nodarījumi: juridisko problēmu analīze. Likums un tiesības 4. sējums Nr. 9 (37), Septembris 2002. ,269.-278. lpp.

[183] Новоселов Г.П. Учение об объекте преступления. Методические аспекты. Москва: Норма, 2001,с. 44-45

nodarījuma objekts ir "noteikta veida labums".[184] Ar noteikta veida labumu saprot tiesību apsargātu labumu.[185]

Patlaban juridiskajā literatūrā ir pārstāvētās četras noziedzīga nodarījuma objekta teorijas:

1.Teorija, kas par nodarījuma objektu atzīst sabiedriskās attiecības.

2.Teorija, kas par noziedzīga nodarījuma objektu atzīst tiesiski aizsargātu labumu.

3. Teorija, ka noziedzīgā nodarījuma objekts ir apdraudētās intereses.

4. Teorija, kas par noziedzīga nodarījuma objektu atzīst konkrētus cilvēkus vai cilvēku grupas, kam noziedzīgā nodarījuma rezultātā nodarīts kaitējums.

## 2.2. Sabiedriskās attiecības kā noziedzīga nodarījuma objekts

PSRS krimināltiesību zinātnē pastāvēja viedoklis, ka iepriekš paustās krimināltiesību zinātnes atziņas, ka nozieguma objekts ir ar tiesību aizsargāts labums, ir nepareizas. Tāpēc tika izstrādāta jauna teorija, kuras bāze bija marksistiski – ļeņiniskā filozofija, kas atzina par noziedzīga nodarījumu objektu ar krimināllikumu aizsargātās sabiedriskās attiecības. Analizējot tā laika juridiskās publikācijas, jāatzīst, ka lielākā daļa autoru, piemēram, A. Piontkovskis, N. Beļajevs, M. Tjažkova, V. Kudrjavcevs, M. Žuravļovs, N. Kuzņecova u.c. [186] nemainīgi aizstāvēja šo viedokli. Tomēr zinātnieku viedoklis bieži vien atšķīrās par to, kas veido sabiedrisko attiecību saturu. Piemēram, V. Prohorovs sabiedriskās attiecības raksturo kā tipizētu sakaru formu, ko izveido cilvēku darbība, to raksturo: 1) sabiedriskā saikne- attiecības pret citiem sabiedrības indivīdiem; 2) cilvēku darbības praktiskā uzvedībā.[187]Vairāki autori, piemēram, D. Koržanskis un B.

---

184 Ibid., Новоселов Г.П. с.7

185 Turpat, Mincs P.,75.lpp.

186 Пиотковский А.А. Учение о преступлении по советскому уголовному праву. Москва: Юридическая литература, 1961,с. 117; Курс советского уголовного права в шести томах. Том. II часть Общая " Преступление" под. ред. А.А. Пионткоʏского . Москва : Наука, 1970, с. 119.; Курс Советского уголовного права. Часть общая. Т. I. Издательство Ленинградского университета, 1968, С 263; Советское уголовное право. Общая часть. Москва : издательство Московского университета, 1981,с.114.; Советское уголовное право. Общая часть. Москва : издательство Юридическая литература, 1977,с.108; Росссийское уголовное право. Общая ч. Учебник Под Ред. М.П. Журавлева. 1999. Москва: издательство "Щит-М" 1999, с.54-59; Уголовное право Росийской федерации Общая часть. Под. Ред. Б.В. Здравомыслова Москва : Юристь.1999, с.106; Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва: Юриспрудения. 1999, с. 86; Kuznetsova N.F Selected works. Saint Petersburg: Yuridichesky Center Press, 2003, p.404

187 Прохоров Преступление и ответственность. Ленинград: издательство Ленинградского университета, 1984.с.47

Ņikiforovs[188], uzskatīja, ka nozieguma objekta kā sabiedrisko attiecību galvenā sastāvdaļa ir ar krimināllikumu aizsargātā interese. Interesi kā zināmu sabiedrisko attiecību sastāvdaļu atzīst arī V. Tacijs. Viņš norāda, ka„.. interese ir zināma veida sociāls fenomens, kas ir sabiedrisko attiecību darbības produkts vai rezultāts. Terminu „interese" nozieguma objekta apzīmēšanai var izmantot tikai tad, kad likumdevējs kā nozieguma objektu ir atzinis *neredzamās sabiedriskās attiecības*, t.i., tādas sabiedriskās attiecības, kuras pēc savas dabas nav tieši uztveramas". [189] Līdz ar to viņš izdara secinājumu, ka jebkura noziedzīga nodarījuma objekts, kā vispārīgais, tā grupas, ir ar krimināllikumu aizsargātas sociālistiskās sabiedriskās attiecības, jo ar interesi šajā gadījumā saprot krimināllikumā aizsargātu „neredzamo" sabiedrisko attiecību, kas stāv aiz konkrētās intereses. Savukārt citi autori, piem., V. Glistins,[190] kritizē šo viedokli, norādot, ka tieši nav iespējams vērsties pret interesi tāpat kā pret tiesībām vai tiesisku labumu. Viņš uzskata, ka nozieguma izdarīšanas brīdī noziedznieks vienmēr iedarbojas uz kaut kādiem sabiedrisko attiecību elementiem, piem., uz sabiedrisko attiecību subjektu vai arī uz konkrēto sabiedrisko attiecību priekšmetu.

Arī mūsdienās daudzi autori[191] atbalsta noziedzīgā nodarījuma objekta apzīmēšanu ar sabiedriskām attiecībām. Piemēram, B. Zdravomislovs nozieguma objektu definē kā sabiedrisku attiecību, kurā iekļaujami šādi elementi: subjekts un sociālā saikne; subjektu intereses, ko aizsargā likums, un priekšmets, ja tas sakrīt ar nodarījuma priekšmetu.[192] V. Krilovs norāda, ka„.. noziedzīgu nodarījumu noziegumu datorinformācijas jomā objekts ir sabiedriskās attiecības, kas nodrošina

---

188 Коржанский Н.И. Обьект преступления и предмет уголовно – правовой охраны. Москва: Академия МВД СССР, 1080.с. 43 Никифоров Б.С. Обьект преступления. Москва, 1960. с. 29-Citēts no Новоселов Г.П. Учение об обьекте преступления. Методические аспекты. Москва: Норма, 2001, с.35-37;

189 Таций В.Я. Обьект и предмет преступления в советстком уголовном праве. Харьков, 1988. с.77 Citēts no Новоселов Г.П. Учение об обьекте преступления. Методические аспекты. Москва: Норма, 2001, с.36

190 Глистин В.К. Проблема уголовно- правовой охраны общественных отношений. Ленинград: издательство Ленинградского университета, 1979. с. 30-35;80-84

191 Ветров Н.И. Уголовное право. Общая часть. Москва : Юнити, 1999, с. 111; Смирнова Н.Н. Уголовное право Учебное пособие. Санкт-петергург – издательство Михайлова, с.28; Кудрявцев В.Н. Общая теория квалификации преступлений. Москва: Юристь, 2001,с.130

192 Уголовное право Росийской федерации Общая часть. Под. Ред. Б.В. Здравомыслова Москва – Юристь.1999 с. 109

informācijas aprites procesu drošību un noteiktās kārtības ievērošanu.[193] Līdzīgi viedokļi ir izteikti arī citu autoru darbos.[194]

Tas, ka teorijā joprojām daudzi juristi palikuši pie ierastā nozieguma objekta definējuma, ir pilnīgi saprotams. Kā norāda A. Ignatovs, tad centieni šobrīd pilnīgi aizvietot nozieguma objekta sabiedrisko attiecību saturu ar tiesiska labuma (intereses) apzīmējumu pagaidām vēl nav spējuši attīstīties kā jauna teorija. Tas ir saistīts ar mazo laika sprīdi, kopš šī teorija atdzīvināta. Tāpēc daudzi krimināli pret to izturas pietiekami piesardzīgi.[195] Šāds arguments ir pamatots, jo teorija par noziedzīga nodarījuma objekta saistīšanu ar tiesiski aizsargātu labumu vai interesi ir pietiekami jauna, lai varētu spriest par tās lietderību krimināltiesību doktrīnā.

Iepriekšējos gados, pētot nozieguma objektu, netika noliegta ne tiesiska labuma, ne arī interešu aizskaršana, taču tobrīd, ievērojot vadošās marksisma un ļeņisma filozofijas nostādnes, visas iepriekšminētās pazīmes tika ietvertas sabiedrisko attiecību saturā. G. Novoselovs norāda, ka jautājums par nozieguma objekta saistību ar sabiedriskām attiecībām ir kļūdains. Viņš uzskata, ka par nozieguma objektu var atzīt tikai to, kam var tikt nodarīts kaitējums. Parādībai, kurai nevar nodarīt kaitējumu, nav nepieciešama krimināli tiesiskā aizsardzība. Ievērojot iepriekšminēto autoru viedokļus, nāktos atzīt, ka kaitējumu var nodarīt tikai sabiedriskām attiecībām, bet nevis tiesiskam labumam, mantai u.c.[196] Šim viedoklim var piekrist, jo nozieguma objekts un nodarītais kaitējums ir savstarpēji saistīti. Tomēr jāpiekrīt arī tiem autoriem, kas uzskata, ka kaitējums nedrīkst būt atkarīgs no tā, kā mēs interpretējam noziedzīga nodarījuma jēdzienu, bet gan objekta izpratnei jābūt pamatotai ar to, ko mēs saprotam kā kaitējumu.[197] Šāda teorija dominē arī vispārējo tiesību valstīs. Piemēram, S. Brennere uzskata, ka

---

193 Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва- Юриспрудения. 1999,с.653

194 Kacman A.Computer crimes Disertation to come forward as candidate of legal sciences. Authors summary .Tbilisi: State University of Tbilisi: 2004. ,p.53.

195 Уголовное право Росиии. Учебник для вузов. В 2- х томах. Т.1. Общая часть. Под. ред. А.И. Игнатова и Ю. А. Красикова. Москва: Норма- Инфра· М, 1999, с.97

196 Ibid., Новоселов Г.П. с.39

197 Ibid., Новоселов Г.П. с.46

noziedzīga nodarījuma objekts ir noziedzīgas darbības rezultāts, kaitējums.[198]D. Fletčers šo domu papildina, ka „... kaitējums tiek nodarīts tieši upura interesēm"[199].

Visām teorijām ir tiesības pastāvēt, jo teorija nav dogma, tā pastāvīgi pilnveidojas un attīstās. Pirmās teorijas piekritēju viedokli autors ir aprakstījis iepriekš, tāpēc turpmāk pievērsīsies teorijām par objektu - tiesisku labumu, objektu - apdraudētu interesi, objektu- cilvēkiem.

## 2.3.Objekts kā tiesisks labums

Viedokli par to, ka objekta apzīmēšana ar sabiedriskām attiecībām ir pārāk vispārēja un virspusēji raksturo nozieguma objektu, juridiskajā literatūrā ir izteikuši vairāki autori, piemēram, U. Krastiņš,[200] A. Naumovs, I. Tjažkova u.c. Piemēram, I. Tjažkova par objektiem atzīst svarīgākās sociālās vērtības, intereses, labumus, ko aizsargā krimināllikums, savukārt V. Naumovs savos sākotnējos darbos pieļauj tikai daļēju atteikšanos no objekta apzīmēšanas ar sabiedriskām attiecībām, norādot, ka nozieguma objektu nevar identificēt ar sabiedriskām attiecībām tad, kad runā par noziegumiem pret personu, bet citos gadījumos tas ir pieļaujams, bet vēlākos darbos viņš runā gan par nozieguma objektu kā (tiesisku labumu) (interesi), bet citos darbos objektu apzīmē tikai ar interesi.[201]

J. Krasikovs pamatoti norāda, ka „... neatkarīgi no valodas barjerām visiem nodarījumiem ir kopīgi šādi apstākļi: a) noziegumam kā jebkurai darbībai ir savs mērķis. Tas apzināti vai ne, bet vienmēr ir vērsts pret kaut ko konkrētu- ārējo fenomenu, kas sastopams reālā pasaulē; b) ārējais fenomens-vienmēr pastāv realitātē. Tas var būt bioloģisks, informatīvs, materiālas un nemateriālas dabas. Tas var izpausties kā mākslīgs fakts, virtuālā realitāte (artifakts), piemēram, sakari, procesi, organizācija, tiesības, iespējas, citi domāšanas rakstura fenomeni, kas izpaužas šī objekta noteiktā vērtībā (reālā vai iedomātā); c) ārējās pasaules fenomeniem pastāvīgi nepieciešama aizsardzība, lai aizsargātu tos no

---

198 "Some question of criminal law theory" by S. Brenner . Autora privātā elektroniskā pasta sarakste

199 Ibid., Флетчер Д., Наумов А.В. с.170

200 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000, 32.lpp.; Наумов А.В. Уголовное право. Общая часть. Курс лекций. Москва: БЕК, 1996,с.147; Курс уголовного права. Общая часть. Под. Ред. Н.Ф. Кузнецовой, И.М. Тяжковой Москва: Зеркало, 1999, с.197;

201 Ibid., Флетчер Д., Наумов А. В. с.218.

pārkāpumiem, pašiznīcināšanās un citām izmaiņām. Šīs aizsardzības iespējas nosaka ārējā vides parādības un to saistība ar apkārtējo darbību. Līdz ar to objekts vienmēr nes sev līdz zināmu krimināltiesiskās aizsardzības nepieciešamību. Šī fenomena apzīmējums var būt dažāds, tur, kur nepiemēro nozieguma objektu, tos sauc par tiesiskiem labumiem vai aizsargājamiem tiesiskiem labumiem"[202]. Viņš neatbalsta objekta apzīmēšanu ar terminu "sabiedriskās attiecības", jo tas ir pārāk abstrakts reālās parādības modelis. Tāpēc J. Krasikovs atbalsta objekta satura apzīmēšanu atkarībā no konkrētās valsts tiesību doktrīnas vai kā tiesisku labumu vai arī aizsargājamo interesi.[203]

Japānas krimināltiesību teorijā ar noziedzīga nodarījuma objektu saprot ar tiesībām aizsargāto interesi (tiesisko labumu).[204] Kā redzams iepriekš, tad daudzi autori, abus terminus lieto kā sinonīmus.

### 2.4.Objekts - tiesiski aizsargāta interese

U. Krastiņš uzskata, ka jēdzieni tiesisks labums un interese nav identiski jēdzieni.[205] Modernajā krimināltiesību teorijā aizvien biežāk, raksturojot konkrētā noziedzīgā nodarījuma apdraudējuma faktorus, tiek lietots termins "intereses". Piemēram, apspriežot nepieciešamību pieņemt visām ES dalībvalstīm saistošu *Corpus Juris*, kā galvenais mērķis tiek izvirzīts specifisku Eiropas interešu aizstāvēšana.[206]

Starptautiskās konvencijas, kas dalībvalstīm uzliek pienākumu kriminalizēt konkrētus sabiedriskus apdraudējumus, piem., Kibernoziegumu konvencija, noteic, ka nodarījums, piemēram, patvaļīga pieeja informācijas sistēmai, apdraud organizāciju un indivīdu intereses netraucēti lietot, vadīt un kontrolēt savu sistēmu darbību[207]. Līdzīgi izskaidrojumi doti arī citiem pantiem, piem., datu traucēšanas

---

202 Уголовное право Росиии. Учебник для вузов. В 2- х томах. Т.1. Общая часть. Под. ред. А.И. Игнатова и Ю. А. Красикова. Москва: Норма- Инфра· М, 1999, с.99-100

203 Ibid., с. 104

204 Уголовное право зарубежных стран.Общая часть.Под. ред. И.Д. Козочкина. Москва: Омега-Л,2003, с.452

205 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 32.lpp

206 The implementation of the Corpus Juris in the member States. Vol. 1. Prof. M. Delmas- Marthy and prof. J.A.E. Vervaele. Antwerpen-Groningen-Oxford- Insersentia, 2000., p.11.

207 ConfCy (2001) Exp.Mem. Explanatory Report to the Convention on Cybercrime.p. 15.

gadījumā tiek apdraudēta datorsistēmu un datorprogrammu integritāte un funkcionēšana u.c.

Līdz ar to jāpiekrīt U. Krastiņam, ka interese ir plašāks jēdziens par tiesisko labumu un sabiedriskām attiecībām, jo tā ir sociāla kategorija, kas ietver sevī vienlaikus gan subjektīvus, gan arī objektīvus kritērijus, tā nav abstrakta, jo vienmēr vērsta uz to, lai apmierinātu personas garīgās un materiālās vajadzības. Intereses nesējs vienmēr ir subjekts, kurš tās realizācijas procesā nonāk zināmās sabiedriskās attiecībās. Tādējādi interese ietver sevī gan tiesisko labumu, mantiskas, nemantiskas vērtības, gan arī sabiedriskās attiecības. Tikai tad, ja šo interešu aizskārums ir krimināli prettiesisks, tad vainīgās personas ir krimināli sodāmas un apdraudētā interese kļūst par noziedzīgā nodarījuma objektu.[208]

### 2.5. Noziedzīga nodarījuma objekti- cilvēki

Kā jauns pagrieziens un tāpēc daudziem autoriem nepieņemama ir G. Novoselova izstrādātā teorija par cilvēku kā nozieguma objektu. Vairākās valstīs par kaitējumu atzīst fizisku personu- upuri. Piemēram, Japānas tiesību teorija izvirza tēzi, ka tiesiskā interese ne vienmēr sakrīt ar nozieguma objekta jēdzienu. Saskaņā ar šo teoriju Japānā un ASV par slepkavības nozieguma objektu atzīst cietušo cilvēku, taču noziegumos pret īpašumu par apdraudējuma objektu tiek uzskatīts tiešais kaitējums, bet nevis interese.[209]

Līdzīga izpratne par kaitējumu kā noziegumu objektu ir sastopama daudzu Rietumvalstu krimināltiesību zinātnē. Ar kaitējumu juridiskajā literatūrā saprot ne tikai nodarījuma fiziskās sekas, bet gan to sociālo nozīmību. Līdz ar to noziedzīga nodarījuma objekta identificēšana ar sabiedriskām attiecībām ne vienmēr ietver visus nozieguma objektu raksturojošos faktorus, piemēram, cilvēkus kā noziedzīga nodarījuma objektus.[210] Viedokli par cilvēku atzīšanu par noziedzīga nodarījuma objektiem padomju krimināltiesību doktrīnā noraidīja lielākā daļa zinātnieku. Piemēram, N. Beļajevs rakstīja, ka cilvēkus nevar atzīt par pastāvīgu nozieguma

---

208 Krastiņš U., Liholaja V. Niedre A.Krimināltiesības Vispārīgā un sevišķā daļa. U. Krastiņa redakcijā. Rīga: TNA,1999., 28.lpp.

209 Уголовное право зарубежных стран.Общая часть.Под. ред. И.Д. Козочкина. Москва: Омега-Л,2003, с.452

210 Ibid., Новоселов Г.П. с.43

objektu, kamēr tie nekļūst par sabiedrisko attiecību sastāvdaļu.[211] Savukārt G. Novoselovs secina, ka „.. jebkura nozieguma objekts, ne tikai tā, kas vērsts pret personu, ir cilvēki, kuri vienā gadījumā ir atsevišķas fiziskas personas, citā kā noteikts cilvēku kopums, bet citā kā sociums (sabiedrība)"[212], jo noziedzīga nodarījuma rezultātā nav iespējams nodarīt kaitējumu nevienam citam kā tikai cilvēkiem.

Turpinot G. Novoselovs polemizē, kas ir svarīgāks noziedzīgos nodarījumos, kas vērsti pret sabiedrisko kārtību, vai cietušā, piem., personas, kas izpilda apsarga pienākumus personīgā interese, vai tā, kuru viņš aizsargā. Protams, ka no sabiedrības drošības viedokļa svarīgāka ir tā interese, ko cietušais aizstāv sabiedrības interesēs, bet no personiskā viedokļa, vienmēr svarīgāka būs viņa personiskā aizskārtā interese. Tāpēc G. Novoselovs uzskata, ka, apskatot jautājumu par nozieguma objektu, nevar nerunāt arī par cietušo. Viņš norāda, ka cietušais nav tikai procesuāls jēdziens, bet nereti cietušais un nozieguma priekšmets savienots vienā personā, līdz ar to viņš secina, ka cietušais kā persona vienlaicīgi ir arī nozieguma objekts.[213] Tādējādi, pēc viņa domām, nozieguma objekts ir tas, pret ko tiek vērsts noziegums.

Analizējot teoriju nozieguma objekts- cilvēks, jāatzīst, ka G. Novoselovs savā monogrāfijā ir sniedzis pietiekamus argumentus, lai to dažu zinātnieku, piem., I. Tjažkovas, kritika būtu mazpārliecinoša. Tomēr šī teorija ir ļoti jauna, tai nav piemērošanas prakses, un turklāt šeit ir vairāki vispārfilozofiski kritēriji, kas padara šo teoriju, tieši no teorētiskā izpētes viedokļa par mazāk pievilcīgu. Pamatots ir Dž. Fletčera viedoklis, ka pret objektiem mums ir jāizturas kā pret lietām, vērtībām, interesēm, labumiem, bet cilvēks ir jāciena kā subjekts, vispirms jau pašam sevī. Ja mēs par nozieguma objektu atzīsim cilvēku, tad kā objektam viņam var aizsargāt cilvēka godu, cieņu. Minētā sentence balstās uz Kanta filozofiju, kas uzskatīja, ja ar

---

211 Курс советского уголовного права. ч. Общая Т.1 издательство Ленинградского университета, 1968,с.292

212 Ibid., Новоселов Г.П. с.60

213 Ibid., Новоселов Г.П. с.66

cilvēku rīkojas kā ar lietu, tas kalpo kā atbaidīšanas idejas atspoguļojums, kā pietiekams pamats, lai sodītu.[214]

### 2.6. Noziedzīga nodarījuma objekta klasifikācijas problēmas

Jebkurai klasifikācijai vai grupēšanai ir jānotiek pēc noteiktām likumsakarībām. Tradicionāli juridiskajā literatūrā tiek izmantota trīspakāpju noziedzīgu nodarījumu objektu klasifikācija pa vertikāli (vispārīgais, grupas un tiešais). Šī klasifikācija tiek pamatota ar filozofijas likumiem par vispārīgā, sevišķā un atsevišķā attiecībām.

PSRS krimināltiesiskajā zinātnē un arī Latvijā[215] noziedzīga nodarījuma objektus pārsvarā iedalīja trīs pakāpēs: 1) vispārīgais objekts; 2) grupas objekts; 3) tiešais objekts. N. Beļajevs atzīst, ka sabiedrisko attiecību kopums ir noteikta parādību vienotība ar kopīgu būtību. Līdz ar to viņš izdara secinājumu, ka objektu dalījums vispārējā, grupas un tiešajā pilnīgi atbilst loģikas prasībām.[216] Padomju juridiskajā literatūrā pastāvēja vairākas nozieguma objekta dalījuma teorijas, piemēram, A. Piotkovskis uzskatīja, ka ar sabiedriskām attiecībām ir jāapzīmē tikai vispārīgais un grupas noziedzīga nodarījuma objekts, bet tiešais objekts ir tas priekšmets, uz ko iedarbojas noziedznieks, tas ir saistīts ar sabiedriskām attiecībām.[217] Savukārt V. Prohorovs norāda, ka „atsevišķais ietilpst kopējā un raksturo to"[218], tādējādi uzsverot, ka sabiedriskās attiecības raksturo gan vispārīgo, gan arī tiešo nozieguma objektu, taču tai pašā laikā viņš atzīst, ka noziedzīga nodarījuma objekts ir tiesiskā kārtība kā sociālo tiesisko attiecību sastāvdaļa. G. Novoselovs secina, ka padomju krimināltiesību teorijā ar sabiedriskām attiecībām kā nozieguma objektu saprata tiesību normu, tiesisko attiecību, tiesisko kārtību un subjektīvās tiesības.[219]

---

214 Ibid.,Флетчер Дж.и Наумов А. В. с.125

215 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000, 37-41lpp.

216 Курс Советского уголовного права. Часть общая. Т. I. Издательство Ленинградского университета, 1968, с.291

217 Курс советского уголовного права. Часть общая т. 2 с. 119-120

218 Прохоров Преступление и ответственность. Ленинград: издательство Ленинградского университета, 1984 с.47

219 Ibid.,Новосеов Г.П.с.33

Iepriekšminētais pierāda, ka krimināltiesību teorijā nav vienota viedokļa par noziedzīga nodarījuma objektu klasifikāciju, tā, piemēram, A. Naumovs[220], I. Tjažkova[221] uzskata, ka noziedzīga nodarījuma objekti ir jāklasificē trīs grupās: 1) vispārējais noziedzīga nodarījuma objekts- ar krimināllikumu aizsargāts labumu (interešu) kopums; 2) grupas objekts, kas ir daļa no vispārējā tiesību objekta, kas sastāv no vienveidīgiem labumiem ( interesēm), pret ko vēršas vienveidīga noziegumu grupa; 3) tiešais objekts, vispārīgā objekta speciāla daļa, interese (labums), kuram tiek nodarīts vai var tikt nodarīts kaitējums noziedzīgu nodarījumu rezultātā.

Aprakstot nozieguma objektu krimināltiesību vārdnīcā, A. Naumovs papildus iepriekšminētajam dalījumam pievieno šķiras, sugas objektu (*видовой*). Ar to apzīmē tos labumus (intereses) gadījumos, ja vienā Krimināllikuma nodaļā ietilpst apakšnodaļas, piem., KF KK VII sadaļā „Persona" ietvertas apakšnodaļas, piem., „Nodarījumi pret dzīvību un veselību, dzimuma neaizskaramību" u.c.[222] Analogu objektu dalījumu ir apskatījis N. Koržanskis u.c. autori.[223]

Citu viedokli izsaka G.Novoselovs.[224] Viņš klasifikācijai izdala šādas pamatprasības: 1) vispirms jāatšķir, ko teorijā sauc par pazīmēm un ko par to nesējiem (lietām); 2) atšķirībā no nesēja pazīme ir rādītājs, pēc kura var kaut ko noskaidrot, bet kas nevar pastāvēt atrauti no nesēja. Viņš uzskata, ka iepriekšminētā pazīme netiek ņemta vērā, klasificējot objektus pa vertikāli, iedalot tos vispārīgā, grupas un tiešajā objektā. G. Novoselovs uzskata, ka minētais iedalījums, kas balstīts uz filozofijas likumsakarībām, nav pareizs, jo vispārīgā, atsevišķā un sevišķā attiecībām filozofijā ir pilnīgi cits raksturs, proti, nevis atsevišķais iekļaujas sevišķajā un vispārīgajā, bet tieši otrādi -vispārīgais un sevišķais ir atsevišķā sastāvdaļa, līdz ar to viņš izdara secinājumu, ka juristu argumenti par minēto kategoriju izmantošanu kā nozieguma objekta vertikālās klasifikācijas pamatu ir

---

220 Учебник уголовного права. Общая часть. Под ред. И.Н. Кудрявцева и А.В. Наумова. Москва: издательство Спарк, 1996, с. 86-87

221 Курс уголовного права. Общая часть. Т.1.Учение о преступлении. Под ред. Н.Ф. Кузнецовой, И.М. Тяжковой. Москва- Зеркало, 1999, с.207-209

222 Словарь по уголовному праву. Под ред. А.В. Наумова. Москва: Издательство -БЕК, 1997, с.308-309

223 Коржанский Н.И. Обьект преступления и предмет уголовно правовой охраны. Москва. [b.i.] 1980, с. 74

224 Уголовное право. Общая часть. Под ред. И.Я.Казаченко, З. А. Незнамова. Москва- Инфра · М- Норма, 1997, с.137

neatbilstoši filozofijā pastāvošajiem likumiem. Viņš secina, ka klasifikācijas pamatā jābūt filozofijas likumiem par elementa, apakšsistēmas un sistēmas attiecībām. Tāpēc viss noziedzīgo nodarījumu objektu kopums veido zināmu (veselu) sistēmu, kuras ietvaros var tikt izdalītas atsevišķas apakšsistēmas un elementi (daļas). Tādējādi G. Novoselovs secina, ka nav pamata runāt par nozieguma objektu klasificēšanu vispārīgos, grupas un tiešos, bet iesaka vispār atteikties no nozieguma objektu klasifikācijas, jo sistēmas, apakšsistēmas un elementa analīze paredz nevis nozieguma objektu veidu pētīšanu, bet gan to hierarhiju, kuras galvenā pazīme ir vertikālo saišu – veselā attiecības pret daļu- raksturojums. Viņš uzskata, ka ar atsevišķo ir jāsaprot paši objekti, bet ar vispārīgo, sevišķo un individuālo nevis paši objekti, bet tiem piemītošās pazīmes. Līdzīgu viedokli padomju krimināltiesību teorijā aizstāvēja A. Piontkovskis, norādot, ka nozieguma objekts ir sociālistiskās tiesiskās attiecības, bet tiešais objekts ir šo attiecību elements.[225] Juridiskajā literatūrā pastāv arī viedoklis, ka faktiskais objekts ir tieši tas reālais priekšmets, pret ko vērts apdraudējums, bet pārējā objektu klasifikācija tikai raksturo ar konkrētām pazīmēm konkrēto nodarījuma objektu, bet nevis otrādi, konkrētais nodarījuma objekts iestājas kā grupas un vispārīgā objekta sastāvdaļa.

G. Novoselovs iedala pazīmes šādās kategorijās: 1) **vispārīgās**- apzīmē tās pazīmes, kas bez izņēmuma atkārtojas katrā apdraudējuma objektā; 2) **sevišķās**- pazīmes, kas piemīt kaut kādai nozieguma objektu daļai; 3) **individuālās** – pazīmes, kas raksturīgas tikai vienam objektam un nepiemīt citiem.[226] Ievērojot sistēmas, apakšsistēmas un elementa likumsakarības, sistēmas sadalīšanai pa vertikāli nav nekā kopīga ar klasifikāciju kā zinātniskās izziņas metodi, jo tās interese ir atklāt starp vertikālā dalījuma dalībniekiem pastāvošās likumsakarības. Sistēma kopumā apakšsistēmu pret nekad nav nosaukta par sugu, bet apakšsistēma par sugu pret elementu. Līdz ar to viņš secina, ka nozieguma objektu grupēšanai

---

[225] Курс советского уголовного права в шести томах. Т. II. Часть общая " Преступление"ю Под. ред. А.А. Пионтковского. Москва: Наука, 1970, с. 116-117

[226] Уголовное право. Общая часть. Под ред. И.Я.Казаченко, З. А. Незнамова. Москва: Инфра · М- Норма, 1997, с.137

nav pamata.[227] G. Novoselovs secina, ka noziegums nav jēdziens, bet gan konkrēta parādība. Noziegums nevar būt ne sugas, ne grupas vai vispārīgs, tāpēc tā objekts vienmēr ir konkrēts un reālā vidē pastāvošs, līdz ar to pastāv tikai viens objekta veids, tas, ko objektu klasifikācijas piekritēji sauc par tiešo objektu.[228]

Minētais viedoklis nav plaši pārstāvēts juridiskajā literatūrā. Ja iedziļināmies G. Novoselova teorijā, tad jāatzīst, ka juridiskajā literatūrā nav iespējams atrast precīzu izskaidrojumu, kāpēc ir nepieciešama noziedzīgu nodarījumu objektu klasifikācija. Vienīgais izskaidrojums ir atsauce uz Hēgeļa triādi par vispārīgo, sevišķo un atšķirīgo, kas izskaidro objektu trīspakāpju iedalījumu.[229] Tomēr nevar piekrist U. Krastiņa un citu autoru viedoklim, kuri pamato šo iedalījumu ar Hēgeļa filozofisko triādi, kas apzīmē vispārīgo, sevišķo un atšķirīgo, jo šī triāde apzīmē spriedumu kvantitatīvo dimensiju, kuras pamatā ir skaitīšana, tātad secība laikā[230]. Hēgeļa triādes galvenā būtība ir esamības (tēzes), neesamības (antitēzes) un nākotnes, kas saistīta ar kaut kā jauna, tikai sev piemītošas esības, radīšanu (sintēze). Autori, kas atbalsta objektu dalījumu trīs vai četrās pakāpes, faktiski to dala pa vertikāli, tas ir, no augšas uz leju, tādējādi šajā dalījumā netiek radīts nekas jauns, atšķirīgs.

Pamatots ir viedoklis, ka objektu klasifikācijai pēc vertikāles ir jābalstās uz sistēmas, apakšsistēmas un elementa savstarpējām attiecībām, kur vispārīgais objekts atspoguļotu visu apdraudēto interešu kopumu- veselumu, savukārt grupas objekts kā apakšsistēma, kurai piemīt radniecīgas pazīmes, apvieno radniecīgas intereses, ko var aizskart ar noziedzīgiem nodarījumiem. Apakšsistēma ir veselās sistēmas sastāvdaļa un sistēmas elements kā apakšsistēmas sastāvdaļa ir noziedzīgā nodarījuma tiešais objekts. Objektu klasifikācija pēc vertikāles pastāv tikai padomju krimināltiesību teorijā un pārmantota juridiskās pēctecības ceļā neatkarīgu ieguvušās valstīs, tai skaitā arī Latvijā. Savukārt Rietumvalstu tiesību doktrīnas par apdraudējuma objektu atzīst tikai tiešo kaitējumu. Atsevišķas valstis grupas objektu

---

[227] Ibid., Новоселов Г.П. с.20-21

[228] Ibid. Новоселов Г.П. с. 22

[229] Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 37.lpp.

[230] Filozofijas atlants attēli un teksti. Rīga: Zvaigzne ABC , 1999., 138 lpp.

izmantoja savu nacionālo krimināl kodeksu konstruēšanā, bet teorijā tas vispār netiek pieminēts.

### 2.7. Vispārējā objekta jēdziens

Latvijā no 1920. līdz 1940. gadam nepastāvēja šāds trīspakāpju noziedzīga nodarījuma objektu iedalījums pa vertikāli. Soda likumā noziedzīgi nodarījumi ir izkārtoti nodaļās, taču tās ir stipri sadrumstalotas, līdz ar to labākajā gadījumā var piekrist, ka šeit ērtības labad tika izdalīti divu veidu objekti, tas ir, grupas un tiešais.

Veicot dažādu valstu krimināllikumu salīdzinošo analīzi, jāsecina, ka Rietumeiropas valstis, piem., Zviedrija, Norvēģija, Dānija, Somija[231] Vācija, Francija, Nīderlande, Itālija, Jāpāna[232] u.c., nepiemēro vispārējo noziedzīgā nodarījuma klasifikāciju, bet galvenokārt ar dažām niansēm izmanto noziedzīgu nodarījumu klasifikāciju pēc grupas pazīmes un tiešā nodarījuma objekta. Tas tikai pierāda, ka Novoselova teorija ir tuva Rietumvalstīs pieņemtajām krimināltiesību teorijas nostādnēm, bet šobrīd tās izmantošana Latvijas krimināltiesību teorijā nav pieņemama.

Pamatots ir J. Krasikova viedoklis, ka šāda objektu klasifikācija pēc vertikāles jāveic, ievērojot to sociālo vērtību apjomu: 1) vispārējo kā visu vērtību kopumu, kuru aizsargā krimināllikums un pret kuru var tikt vērts apdraudējums; 2) grupas objektu kā noteiktu vērtību grupu, pret kurām var tikt vērsti apdraudējumi; 3) tiešo kā interesi, pret kuru tiek vērts apdraudējums.[233] Uzsverot šajā vertikālajā sadalījumā sociālo nozīmīgumu, atsevišķa objekta vārīgumu, aizsardzības pakāpes intensitāti, faktiski vertikālo noziegumu objektu sadalījums tiek nostādīts jaunā kvalitātē. Tāpēc jāpiekrīt tiem autoriem, kas norāda, ka grupas objekta izveidošanas mērķis ir: 1) dažādu grupu labumu salīdzinošā sociālās vērtības, tai skaitā aizsardzības nepieciešamības pakāpes izzināšana; 2) šīs pazīmes likumdevējs izmanto, lai izveidotu krimināllikuma sevišķo daļu.[234] Tādā veidā, balstoties uz

---

231 Criminal law in Danmark by Lars Bo Langsted, Van Greve, Peter Garde. Hague- London-Boston- Kluwer law international, 1998. pp.177-205.

232 Ibid., Shigemitsu Dando. p. 136.

233 Уголовное право Росиии. Учебник для вузов. В 2- х томах. Т.1. Общая часть. Под. ред. А.И. Игнатова и Ю. А. Красикова. Москва- Норма- Инфра- М, 1999. с.100-102

234 Ibid..c.106

tiesisko tradīciju pēctecību, arī likumdevējs, kriminalizējot tos vai citus nodarījumu sastāvus, tos iekļauj sadaļās, kas dod iespēju izvērtēt to salīdzinošo sociālo vērtību un tai skaitā arī aizsardzības nepieciešamo pakāpi.

Objektu dalījums par vertikāli ir dziļi iesakņojies teorētiķu apziņā, un šī teorija ir pieņemta praksē un saprotama gan teorētiķiem, gan praktiķiem, ka vispārīgais objekts ir visu ar krimināllikumu apdraudēto interešu kopums, ka grupas objekts ir vispārējā objekta sastāvdaļa, kas apvieno vienveidīgu apdraudēto interešu grupu. Tieši grupas objektam ir būtiska nozīme Krimināllikuma sevišķās daļas uzbūvē un noziedzīgo nodarījumu izkārtošanā pēc vienveidīgām apdraudēto interešu grupām, un tiešais objekts ir speciālā objekta sastāvdaļa.

*Vispārīga drošība kā noziedzīgu nodarījumu objekts*

Padomju krimināltiesību doktrīna jēdziens „sabiedriskā drošība" pirmo reizi tika izmantots 1922. gada Krievijas Federācijas Kriminālkodeksa 8. nodaļā „Noteikumu, kas aizsargā tautas veselību, sabiedrisko drošību un publisko kārtību, pārkāpšana" , taču līdz pat 90 gadiem teorijā nebija dots termina „drošība" saturiskais skaidrojums. Tieši pēc PSRS sabrukuma neatkarību atguvušās un jaunizveidotās valstis sāka attīstīt savu nacionālo drošības politiku. Tā Krievijas Federācija 1992.gada 15. marta likuma „Par drošību" 1. pantā definēja drošību,.. kā valsts, sabiedrības un personu dzīvei svarīgu interešu aizsardzības stāvokli no iekšējiem un ārējiem apdraudējumiem"[235]. 2000.gada 14. decembrī Saeima pieņēma Nacionālas drošības likumu. Šā Likuma 1. pantā termins „nacionālā drošība"definēta kā „.. valsts un sabiedrības īstenotu vienotu, mērķtiecīgu pasākumu rezultātā sasniegts stāvoklis, kurā ir garantēta valsts neatkarība, tās konstitucionālā iekārta un teritoriālā integritāte, sabiedrības brīvas attīstības perspektīva, labklājība un stabilitāte."[236] 2002.gada 24. janvārī Saeima apstiprināja „Nacionālās drošības koncepciju". Minētā dokumenta 1.1. punktā nacionālā drošība definēta kā „ .. valsts un tās sabiedrības spēja aizsargāt un nodrošināt nacionālās intereses un pamatvērtības. Tās ietver Latvijas Republikas valstiskās neatkarības, teritoriālās nedalāmības un Satversmē noteiktās demokrātiskās iekārtas

---

[235] Закон о безопасности //Ведомости Съезда Народных Депутатов Российской Федерации 1992. Nr. 15. Ct. 769

[236] http://www.likumi.lv/doc.php?id=14011 (aplūkots 2005.gada 27. martā)

pastāvēšanu, kā arī valsts iekšējās drošības nodrošināšanu, garantējot cilvēka tiesību ievērošanu, iedzīvotāju drošību un aizsargātību."[237] Šīs koncepcijas 2.2.2. punktā dots termina „iekšējā drošība" saturiskais skaidrojums: „Sabiedrības drošību un katra sabiedrības indivīda drošību ietekmē un raksturo noziedzības stāvoklis valstī. To ietekmē ne tikai iekšējie procesi (politiskie, ekonomiskie, sociālie un tiesiskie), bet arī noziedzības tendences pasaulē." Šī dokumenta 3.1. punktā dots termina „apdraudējums nacionālai drošībai"skaidrojums. Ar apdraudējumu saprot darbības, kas vērstas pret Latvijas nacionālajām interesēm un pamatvērtībām, kā arī ekoloģisku, tehnisku un cita rakstura faktoru radītas situācijas, kas nelabvēlīgi ietekmē iespējas realizēt nacionālās intereses. Tādējādi Latvijas nacionālā drošība ir valsts un sabiedrības spēja aizsargāt un nodrošināt tās nacionālās intereses un pamatvērtības. Tas ir arī Krimināllikuma uzdevums ar tajā noteikto aizliegumu vai ierobežojumu palīdzību nodrošināt valsts un sabiedrības spēju aizsargāt Latvijas tautas kā Latvijas suverēnās varas nesēja[238] tiesiskās un likumīgās intereses.

Krievijas krimināltiesību zinātnieki noziedzīgus nodarījumus, kas apvienoti Krievijas Federācijas Krimināl kodeksa IX nodaļā „Noziedzīgi nodarījumi pret sabiedrisko drošību un sabiedrisko kārtību", definē, kā krimināl kodeksā iekļautus noziedzīgus nodarījumus, kas nodara būtisku kaitējumu sabiedrības dzīves drošības nosacījumiem, iedzīvotāju veselībai un sabiedriskai tikumībai, apkārtējai videi, datorinformācijas saglabāšanai un neaizskaramībai vai rada reālus šāda kaitējuma draudus.[239] Līdzīgs iedalījums ir arī Krimināllikumā. Krimināllikuma XX nodaļā „Noziedzīgi nodarījumi pret vispārējo drošību un sabiedrisko kārtību" vienā grupā apvienoti pēc sava rakstura dažādi nodarījumi. Likumdevējs paredzējis, ka vienojošais elements šās nodaļas noziedzīgiem nodarījumiem ir vispārējās drošības un sabiedriskā kārtības intereses apdraudējums.

Krievijas kriminālisti sabiedrisko drošību atzīst par vienu no grupas objekta elementiem un definē kā noteikta apjoma sabiedrisko attiecību kopumu, kas regulē

---

[237] Nacionālās drošības koncepcija. Latvijas Ārlietu ministrijas mājas lapa// http://www.am.gov.lv/lv/nato/Pamatdokumenti/4120/#1 (aplūkots 2005.gada 26. martā).

[238] Satversme. Saeimas mājas lapa// http://www.saeima.lv/Likumdosana/likumdosana_satversme.html (aplūkots 2005.gada 26. martā)

[239] Курс Уголовного праваю Том 4. Особенная часть. Под ред. Г.Н. Борзенкова и В.С. Комисарова, Москва, Зеркало-М, 2002, с.169

drošus sabiedrības dzīves nosacījumus. Tai pašā laikā arī viņi atzīst, ka drošības un kārtības panākšana ir viens no galvenajiem krimināllikuma uzdevumiem. Tādējādi nav skaidrs, kāpēc tieši sabiedriskā drošība tiek izvēlēta par grupas objektu. Lai rastu atbildi uz šo jautājumu, nepieciešams veikt vārda un termina „drošība"semantisko un saturisko analīzi.

Drošība ir tad, ja „kaut kas nav pakļauts zaudējumam vai neveiksmei".[240] E. Grīnbergs (*Eric Greenberg*) raksta: „Drošība nav tikai produkts vai pazīme, ko viegli var iegūt. Drošība ir domāšanas veids- tā nekad nebūs absolūta, un tā nav tikai tehniska problēma. Mums tāpēc ir labāk jādomā par tiem, kas stāv pretējā pusē."[241] Patiesībā šeit nav ko piebilst, taču nevar runāt par drošību kā pazīmi vai kā domāšanas veidu, jo par nepareizu domāšanu, kā zināms, nevienu sodīt nevar. Šeit ir ļoti svarīgi nodalīt divus jautājumus, proti, termina „drošība" kā lietvārda lietošana un vārda „drošība" lietošana īpašības vārda kontekstā, piem., droša darba vide, droša informācijas vide u.c. Vārdu kopa „vispārīgā drošība" jau pati par sevi norāda, ka likumdevējs ar šo jēdzienu neapzīmē neko konkrēti, tas ir, šo jēdzienu aplūko vispārēji, bez piesaistes speciālai videi pretēji tām krimināllikuma nodaļām, kur izcelta specifiskas vides drošība, piemēram, XXI nodaļa „Noziedzīgi nodarījumi pret satiksmes drošību". Ja terminu „drošība" lieto vispārīgā nozīmē, tad tas vairāk akcentē īpašības vārda formu „drošs" kā lietvārdu. Bet, ja termins „drošība" netiek saistīts ar konkrētu vidi, tad tas ir lietojams tikai kā vispārīgs apzīmējums, piemēram, valsts pienākumu nodrošināt apstākļus, ka indivīds var dzīvot drošā vidē. Tā ir vispārīga cilvēka interese- vēlme dzīvot bez jebkādiem apdraudējumiem. Tas nozīmē, ka „drošība"pēc sava rakstura ir multifunkcionāla parādība, kuras tiesisko pamatu nodrošina Latvijas valsts normatīvo aktu sistēma, tai skaitā Krimināllikums, kuras uzdevums ir ar tiesiskām metodēm vispārīgi nodrošināt Latvijas valsts (cilvēku, sociālo grupu, valsts teritorijā esošo mantisko vērtību) interešu aizsardzību. Ja likumdevējs par grupas objektu izvēlējies vispārējo

---

240 Cambridge advanced learner's dictionary // http://dictionary.cambridge.org/define.asp?key=71111&dict=CALD&desc=secure (aplūkots 2001.gada 21. janvārī) ; The Wordsmyth English Dictionary-Thesaurus // http://www.wordsmyth.net/live/home.php?script=search&matchent=security&matchtype=exact (aplūkots 2003.gada 20. martā) u.c.

241 Mission Critical Security Planner. Creating Custumised strategies by Eric Greenberg. Indianpoliss-Wiley publishing Inc. 2003, pp. 1-2;

drošību, tad uzreiz kļūst skaidrs, ka ar terminu vispārīgs netiek domāts nekas konkrēts, respektīvi, šādu apzīmējumu ar tikpat lielu pamatojumu var attiecināt uz jebkuru citu Krimināllikuma sevišķajā daļā iekļauto nodaļu.

Ja krimināltiesību teorijā un praksē jāapvieno noziedzīgi nodarījumi, kas vērsti pret noteiktu specifisku vidi, tad ir jārunā par konkrētu personas intereses apdraudējumu, un šim apdraudējumam ir jābūt saistītam ar konkrētu darbību, kas kavē vai traucē personai realizēt savas tiesības. Drošību kā rezultātu apraksta ASV Aizsardzības departamenta Militāro un saistīto terminu vārdnīca, kur tā ir definēta, kā „.. aizsardzības līdzekļu, kas nodrošina valsts neaizskaramību no ienaidnieka darbībām vai ietekmes, piemērošanas un uzturēšanas rezultāts"[242]. Tātad, lai identificētu drošību, ir jārunā par kaut kā gala produktu, kas mūs pasargātu no apdraudējumiem. Tādējādi drošību varam identificēt ar šādām vispārīgām pazīmēm:

1. Drošība ir iespējams konkrēta objekta minimālā apdraudējuma stāvoklis konkrētā brīdī. Tas nozīmē, ka par drošību nevar runāt abstrakti, bet vienmēr tā ir jāsaista ar konkrētu objektu. Šīs tēzes oponenti var izvirzīt argumentus, ka praksē runā arī par valsts drošību, par informācijas drošību un sociālo un cita rakstura drošību, kur terminu „drošība" ne vienmēr attiecina uz personu grupām, valsts aizsardzību u.c. jomām.

2. Drošība nekad nav absolūta. Riskus un apdraudējumus ir iespējams samazināt, bet ne pilnīgi novērst. Precīzi alegorijā šo stāvokli ir definējusi D. Deninga (*Doro:hy E. Denning*), ka „.. drošība ir bedre bez dibena, tāpēc sasniegt 100% drošību nav iespējams".[243]

3. Drošība vienmēr ir saistīta ar pasākumu kompleksu, bez kura nav iespējams panākt šo *status quo*. Šo pasākumu kompleksu sauc par drošības politiku. [244] Viens no šādas politikas pilāriem ir arī valsts krimināltiesiskā politika.

---

242 FEDERAL STANDARD Telecommunications: GLOSSARY OF TELECOMMUNICATION TERMS http://www.its.bldrdoc.gov/fs-1037/dir-032/_4740.htm (aplūkots 2003.gada 23. oktobrī)

243 Cybercrime & Secyrity. Compiled & edited by Alan E. Brill, Fletcher N. Baldwin, Jr. Robert J. Munro. II. Infrastructure protection & management solutions. Booklet II.6 Protection and defence of intrution by Dorothy E. Denning Georgetown university, March 5 1996. issued September 1998. Oceana publications, Inc., Dobbs Ferry, Ny., II.6-1.

244 sk. LVS ISO/IEC 17799:2002 A 4.1.3. , 3.lpp.

No iepriekš teiktā var secināt, ka „drošība" ir atzīstama par vienu galvenajām vērtībām, ko aizsargā krimināllikums. Tas, ka attiecīgā krimināllikuma nodaļas nosaukums tieši nesatur šo terminu, nenozīmē, ka šāda interese netiek apdraudēta. Analizējot Krimināllikuma sevišķo daļu var secināt, ka tieši vispārējā drošība ir tas dzinulis, kas liek iekļaut to vai citu normu krimināllikuma sevišķajā daļā. Tāpēc „vispārējā drošība" faktiski ir atzīstama par *sui generis* apzīmējumu visu apdraudējumu kopumam un kā tāda var tikt atzīta tikai par vispārīgo objektu. Tā ietver sevī valsts militāro, ekomisko, ekoloģisko, fizisko, satiksmes, darba, mantisko, informatīvo un cita veida drošību, tai skaitā arī informācijas sistēmu drošību. Tādējādi informācijas sistēmu drošība ir vispārējās drošības apakšsistēma un atbilstoši krimināltiesību objektu klasifikācijai pa vertikāli atzīstama par grupas objektu, kas apvieno noziedzīgus nodarījumus, kuri pēc savas dabas ir radniecīgi un kuriem ir kopīga apdraudētā interese.

## 3. Kibernoziegumu klasifikācija pēc grupas objekta

### 3.1. Vispārīgie nosacījumi

Saskaņā ar Eiropas Padomes Kibernoziegumu konvenciju un tās papildus protokolu kibernoziegumi klasificēti piecās grupās: 1) noziedzīgi nodarījumi pret informācijas sistēmu drošību; 2) datorsaistīti noziegumi (krāpšana, viltošana); 3) noziegumi, kas saistīti ar bērnu pornogrāfiju; 4) noziedzīgi nodarījumi, kas saistīti ar autortiesību un blakustiesību pārkāpšanu; 5) noziedzīgi nodarījumi, kas saistīti ar rasismu un ksenofobiju un genocīdu propagandējošu materiālu izplatīšanu automatizētās datu apstrādes sistēmās. Lai kvalificētu noziedzīgos nodarījumus pēc grupas objekta, nepieciešams konstatēt tikai konkrētai noziedzīgo nodarījumu grupai raksturīgas vispārīgas un speciālas pazīmes, kas dod pamatu tos grupēt pēc vienveidīgām apdraudēto interešu grupām. Visus kibernoziegumus vieno tikai tas, ka tie ir izdarīti kibertelpā un *modus operandi*, ka tie visi var tikt izdarīti ar darbību un tiešu vai netiešu nodomu. Taču minētās pazīmes ir nepietiekamas, lai gan teorētiski, gan arī praktiski veiktu šo noziedzīgo nodarījumu grupēšanu un atrastu vienotu aizskarto tiesisko interesi. Katrai no iepriekšminētajām kibernoziegumu grupām ir savas aizskartās tiesiskās intereses, piemēram, krāpšanas automatizētās datu apstrādes sistēmās aizskartā interese ir mantiskās tiesības, tāpēc šāds

nodarījuma sastāvs iekļaujams Krimināllikuma XVIII nodaļā „Noziedzīgi nodarījumi pret īpašumu", viltošana automatizētās datu apstrādes sistēmās var tikt iekļauta Krimināllikuma XXII nodaļā „Noziedzīgi nodarījumi pret pārvaldības kārtību", kur 275.pantā paredzēta krimināalatbildība par dokumenta, zīmoga un spiedoga viltošanu un viltota dokumenta, zīmoga un spiedoga realizēšanu un izmantošanu, jo viltošana automatizētās datu apstrādes sistēmās pēc savas būtības atšķiras no 275. panta paredzētā noziedzīgā nodarījuma tikai ar to, ka mainās dokumenta viltošanas vide un darbības veids, bet apdraudētā interese- valsts noteiktās dokumentu aprites kārtības ievērošana- saglabājas.

Noziedzīgi nodarījumi, kas saistīti ar automatizēto datu apstrādes sistēmu izmantošanu kā mediju nelikumīgas informācijas (bērnu pornogrāfija, rasu naida, genocīda, ksenofobijas propaganda) izplatīšanā, arī nevar tikt grupēti pēc vienota apdraudējuma grupas objekta, jo informācija, kas saistīta ar bērnu pornogrāfijas apriti, aizskar tikumības un dzimumneaizskaramības intereses, tāpēc pilnīgi pamatoti bērnu pornogrāfijas aprites aizliegums ir iekļauts Krimināllikuma XVI nodaļā „Noziedzīgi nodarījumi pret tikumību un dzimumneaizskaramību" 166. pantā. Kibernoziegumu konvencijas papildus protokolā paredzētie noziedzīgie nodarījumi par informācijas izplatīšanu, kas saistīta ar rasisma, ksenofobijas vai genocīda propagandu, ir atzīstami par starptautiskiem noziegumiem, kas vērti pret cilvēci, mieru, tāpēc tie acīmredzot tiks iekļauti Krimināllikuma IX nodaļā „Noziegumi pret cilvēci, mieru, kara noziegumi, genocīds", bet noziedzīgi nodarījumi pret autortiesībām un blakustiesībām ir iekļauti Krimināllikuma XVI nodaļas „Noziedzīgi nodarījumi pret personas pamattiesībām un pamatbrīvībām" 148. un 149. pantā. Likumdevējs, iekļaujot šos noziedzīgos nodarījumus šajā nodaļā, atzinis, ka ar nodarījumiem pret autortiesībām un blakus tiesībām ir aizskarta personas konstitucionālā tiesība uz autortiesību aizsardzību.

Teorētiski iepriekšminētajām kibernoziegumu grupām var saskatīt divas kopīgas pazīmes, pēc kurām tos visus varētu apvienot vienā nodaļā, piemēram, ar kopīgu nosaukumu „Kibernoziegumi" vai arī „Noziedzīgi nodarījumi pret informāciju". Autors neatbalsta šādu viedokli, jo tādējādi šādā grupā būtu ļoti grūti izdalīt kopējo apdraudēto interesi un faktiski krimināltiesību zinātne savā attīstībā saistībā ar

kibernoziegumu izpēti zināmā mērā apstātos, jo visu šo nodarījumu kopīgā apdraudētā interese tiktu definēta kā aizskārums personas tiesībām uz informācijas apriti. Tādējādi kibernoziegumi vienkārši saplūstu ar citiem noziedzīgiem nodarījumiem, jo arī tradicionālajos nodarījumos ir iespējams konstatēt personas apdraudēto interesi uz tiesībām uz informācijas apriti.

Līdz ar to var secināt, ka vienīgā kibernoziegumu grupa, kurai ir kopīgas radniecīgās intereses, ir noziedzīgi nodarījumi pret informācijas sistēmu drošību, kas šobrīd ietverti Krimināllikuma XX nodaļā „Noziedzīgi nodarījumi pret vispārīgo drošību un kārtību" (241.-245. pants) kopā ar tādiem noziedzīgiem nodarījumiem kā huligānisms, bandītisms, ar nelikumīgu narkotiku apriti saistītie nodarījumi u.c. Likumdevējs šos nodarījumus atzinis par tādiem, kuriem ir kopīgs grupas apdraudējuma objekts - apdraudētā tiesiskā interese ir vispārējā drošība. No tiesību teorijas un praktiskās lietderības viedokļa tāda pieeja, ka šādai noziedzīgu nodarījumu grupai pievienoti arī noziedzīgi nodarījumi pret informācijas sistēmu drošību, nav ne racionāla, ne arī pamatota.

### 3.2. Grupas objekts- Informāciju sistēmu drošība (ISD)

XXI gadsimtu, ko nereti dēvē arī par digitālo tehnoloģiju un informācijas sabiedrības gadsimtu, cieši saista ar elektroniskā veidā sagatavotas informācijas pārraidīšanas vai apstrādes iespēju pasaulē. Informācija var būt sagatavota dažādos veidos- gan rakstiski, gan skaņas, gan arī attēla veidā. Digitālās tehnoloģijas dod iespēju ar programmatisku resursu palīdzību pārveidot šo informāciju datordatu[245] veidā un pārraidīt šādus datus uz jebkuru vietu pasaulē. Tāpēc svarīga nozīme ir jebkuras organizācijas, uzņēmuma un iestādes elektroniskās informācijas sistēmas tehnisko un informācijas resursu aizsardzībai. Pasaulē nav vienota viedokļa, kā definēt informācijas sistēmu drošību (turpmāk tekstā - ISD)- vai kā procesu, vai kā gala rezultātu.[246]

Ja reālā vidē, piem., būvniecības drošību, var pārbaudīt, vai celtnieki nav atkāpušies no projekta, vai izmanto atbilstošas kvalitātes materiālus, un pieprasīt novērst kļūdas, tad daudz grūtāk to ir izdarīt elektroniskā vidē. Elektroniskā vidē

---

[245] Kibernoziegumu konvencijas 1.p.b.p.

[246] Autora personīgā e- pasta sarakste ar Dr. Sc.Comp. J. Borzovu "teorētisks jautājums"

tehnoloģijas attīstās tik strauji, ka šobrīd neviens nespēj atrast tādus IS drošības risinājumus, kas pilnīgi aizsargātu IS no jebkāda apdraudējuma. Starptautiskos dokumentos izstrādātie ISD jēdzieni ir elastīgi, tāpēc tos iespējams interpretēt gan par labu vienas pozīcijas piekritējiem, kuri uzskata ISD par procesu, gan arī tiem, kuri uzskata, ka jēdzienu informācijas sistēmu drošība vai lietot tikai kā gala rezultāta (stāvokļa) apzīmējumu.

Raksturīgs piemērs abpusējai pieejai ir ANO ekspertu izstrādāta un pieņemtā ISD definīcija, ka *informācijas sistēmu drošība* ir informācijas pieejamības, konfidencialitātes un integritātes nodrošināšana informācijas sistēmā.[247] Šī definīcija ir pietiekami elastīga, lai apmierinātu abu viedokļu piekritējus, jo viena puse, uzsverot vārdu **nodrošināšana**, var šo definīciju attiecināt uz gala rezultātu-stāvokli, bet savukārt citi var interpretēt kā procesu, kurā jānodrošina informācijas konfidencialitāte, integritāte un pieejamība. Tāpēc, izstrādājot ISD stratēģijas, nereti tā tiek paplašināta, ievērojot 1992.gada vadlīnijās noteiktos principus.

Tā, piem., ASV Federālā telekomunikāciju terminu glosārijā[248] informācijas sistēmu drošība ir definēta kā „.. informācijas sistēmu aizsardzība no neautorizētas pieejas, informācijas resursu apstrādes un pārraides neatļautas modifikācijas, autorizētu lietotāju aizsardzība no pakalpojuma atteices uzbrukumiem[249], aizsardzību pret patvaļīgiem lietotājiem, tai skaitā, veicot šādu draudu atklāšanu, dokumentēšanu un uzskaiti".

RITI direktors, habilitēts datorzinātņu doktors J. Borzovs privātā sarakstē ar autoru uz jautājumu, vai informācijas sistēmu drošība ir stāvoklis vai process, atbild, ka lielākajā daļā pasaules informācijas tehnoloģiju vārdnīcu ISD ir definēts kā stāvoklis.[250]

2002. gada aprīlī par Latvijas standartu LVS ISO/IEC 17799 : 2002 „Informācijas tehnoloģija. Prakses kodekss informācijas drošības pārvaldībai" atzīts

---

[247] OECD Guidelines for the security of Information systems 26 November 1992 Explanatory Memorandum to Accompany the Guidelines for the Security of Information Systems http://www.oecd.org/dsti/sti/it/secur/prod/e_secur (aplūkots 2003.gada 21. janvārī)

[248] Telecoms glosary of telecommunication terms ( http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm) (aplūkots 2003.gada 23. novembrī)

[249] Lielā terminu vārdnīca. http://www.termini.lv/index.php (aplūkots 2004.gada 12. janvārī)

[250] autora personīgā e- pasta sarakste ar Dr. Sc. Comp. J. Borzovu "teorētisks jautājums".

starptautiskais standarts ISO/IEC 17799:2000 "*Information technology –Code of practice for information security management*".[251] Minētā standarta 2.1. p. noteic, ka".. informācijas drošība ir informācijas konfidencialitātes, integritātes un pieejamības saglabātība". No minētās definīcijas redzams, ka tā atšķiras no ASV standarta, jo Latvijas standartā ISD definēta kā stāvoklis, bet ASV kā process.

Savukārt ES dokumentā "Tīklu un informācijas drošība: priekšlikumi Eiropas politikas nostādnēm"[252] skaidrots, „..ka ar tīklu un informācijas drošību saprot tīkla un informācijas sistēmas **zināmu** drošības līmeni, kas spēj pretoties gadījuma vai ļaunprātīgām darbībām". Minētajā dokumentā ISD raksturots kā līmenis-stāvoklis, kurā var nodrošināt informācijas resursu integritāti, konfidencialitāti un pieejamību, un 2.1. punkts izskaidro, ka tīkli ir informācijas sistēmu neatņemama sastāvdaļa, jo to komponenti ir kabeļi, bezvadu savienojumi, satelīti, rūteri u.c., bez kuriem nav iedomājama modernu datorsistēmu darbība. Līdzīgu viedokli izsaka arī O. Gavrilovs, norādot, ka informācijas drošība ir informācijas vides stāvoklis, kas aizsargāts tā, lai nodrošinātu tās formēšanu, izmantošanu un attīstību.[253]

Literatūrā nereti ir atrodami kļūdaini secinājumi, kas datorsistēmu identificē ar informācijas sistēmu. Informācijas sistēma ir plašāks jēdziens par datorsistēmu, un šie jēdzieni nav un nevar būt identiski. Tā, piemēram, ES priekšlikumam Padomes ietvarlēmumam par uzbrukumiem informācijas sistēmām paskaidrojošā memorandā 1.1. p. izskaidrots, ka „.. frāze "informācijas sistēma" speciāli tiek definēta kā konverģence starp elektroniskiem komunikāciju tīkliem un dažādām sistēmām, ko tie savieno. Tādā veidā informācijas sistēma ietver sevī atsevišķus personālos datorus, personālos digitālos organizētājus, mobilos telefonus, dažāda veida tīklus,

---

[251] LVS Informācijas tehnoloģija. Prakses kodekss informācijas drošības pārvaldībai LVS ISO/IEC 17799 A.

[252] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach /* COM/2001/0298 final //

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=52001DC0298&model=guichett (aplūkots 2003.gada 21. janvārī)

[253] Ibid. Гаврилов О.А.с.55

to skaitā publiskos un speciāli veidotos datu pārraides tīklus, serverus un citu interneta infrastruktūru u.c".[254]

Ziemeļvalstu informācijas sistēmu drošības politikā informācijas sistēmas definīcijā ir iekļauti ne tikai IS resursi, bet arī sistēmas administrēšana un personāls.[255] Šāda pieeja ir pareiza. To atbalstījusi arī Latvijas ZA Terminoloģijas komisija, kas informācijas sistēmu definē, kā „.. iekārtu, procedūru un personāla kopumu, kas ir izveidots, strādā un tiek uzturēts, lai vāktu, uzkrātu, apstrādātu, uzglabātu un izmantotu informāciju"[256], savukārt terminu „datorsistēma" kā „..datora un tā perifērijas ierīču (t. sk. diskdziņu, monitora, dažādu ievadizvades ierīču u. c.) pilnu konfigurāciju, kas operētājsistēmas vadībā kopīgi veic datu apstrādi". Autoraprāt, IS iespējams definēt kā datu ievadīšanas, uzglabāšanas un apstrādes sistēmu, kas paredz lietotājpieeju tajā glabātiem datiem vai informācijai. Īsi sakot, IS sniedz informācijas pakalpojumu likumīgiem lietotājiem, bet datorsistēma šādus pakalpojumus nesniedz.

Valsts Informāciju sistēmu likuma[257] 1.p. 1) p. noteic : *Valsts informācijas sistēma — strukturizēts informācijas tehnoloģiju un telekomunikāciju aprīkojuma un datu bāzu kopums, kuru lietojot tiek nodrošināta valsts funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana (turpmāk — informācijas aprite).*

Tas izriet no ISD pamatmērķa, proti, organizēt tādu pasākumu un kontroles sistēmu, lai sasniegtu mērķi, ko raksturo trīs pazīmes: 1) konfidencialitāte: 2) integritāte: 3)pieejamība. Informācijas sistēmu drošībai ir jābūt absolūti identificētai ar visām šīm pazīmēm vienlaicīgi. Ja nav kādas no tām, tad vispār nevaram runāt par informācijas sistēmu drošību kā stāvokli.

Tātad runa ir ne tikai par viena veida pasākumiem, bet gan par integrētiem, savstarpēji saskaņotiem pasākumiem, kas ietver sevī drošības administrēšanu, riska menedžmentu, datorprogrammatūras un aparatūras drošību, pieejamības kontroli,

---

254 Proposal of Council framework decision on attacks against information systems. Explanatory memorandum. Brussels COM (2002) 173 Final 19.04.2002 2002/0086 (CNS)

255 Information security in Nordic Countries. Nordiske Seminar–og Arbeijds rapporter 1993:613 p.12

256 Lielā terminu vārdnīca. http://www.termini.lv/index.php (aplūkots 2004.gada 11. janvārī)

257 Valsts informācijas sistēmu likums. Publicēts. Latvijas Vēstnesis 22.05.2002.gada 22. maijā

komunikāciju drošību, datoroperāciju drošību, fizisko drošību un saistošo plānošanu.[258] Tomēr visu šo pasākumu galvenais mērķis tiek ietverts jau iepriekšminētajos trijos vārdos– pieejamība, integritāte un konfidencialitāte.

*Pieejamība*– raksturo stāvokli, kad informācijas un informācijas sistēmu resursi ir pieejami un izmantojami noteiktā laikā pēc pieprasījuma.[259] Latvijas Bankas informācijas tehnoloģijas drošības noteikumu rokasgrāmatā jēdziens „pieejamība" definēts ne tikai kā resursu pieejamība un izmantojamība, bet arī kā „..informācijas pastāvēšana un saglabāšana, lai sankcionētiem lietotājiem to būtu iespējams lietot īstajā laikā un vietā".[260] Bieži vien pieeja definēta kā spēja pieprasīt pakalpojumu informācijas sistēmai.

Definējot pieejamību informācijas sistēmai, šai definīcijai ir jāatbilst trim kritērijiem: 1) tā attiecas tikai uz autorizētiem lietotājiem, kuriem ir tiesības pieslēgties sistēmas resursiem un iegūt nepieciešamo informāciju vai pieprasīt to; 2) tiesības piekļūt informācijas sistēmai tad, kad tas ir nepieciešams lietotājam vajadzīgā laikā. Pieejamība nosaka lietotājiem gaidīšanas kārtību, kas nepieciešama, lai piekļūtu informācijas resursiem. Atkarībā no lietotāja statusa var noteikt speciālas darba stundas, kā arī laika limitu. Pieejamība ietver sevī arī sistēmas kontaktinformāciju un informāciju par neveiksmīgiem pieslēgumiem tīkla neveiksmīgas darbības dēļ; 3) IS pieejamības raksturojums ir atkarīgs no tā, kam šī informācijas sistēma pieder.

*Informācijas integritāte* ir informācijas pareizība, kārtība, pilnīgums, precizitāte un saskaņotība ar uzņēmējdarbības vajadzībām.[261] Integritāte raksturo datu un informācijas precizitāti, to pilnīgu saglabāšanu un pareizību.[262] Integritātei ir ļoti cieša saikne ar Krimināllikuma 327. panta „Dienesta viltojums" paredzēto nodarījuma sastāvu, jo viltojums ir informācijas integritātes pārkāpšana. Integritāte attiecas ne tikai uz informāciju, bet arī uz citiem sistēmas komponentiem.

---

258 Information security in Nordic Countries. Nordiske Seminar–og Arbeijds rapporter 1993:613.p.16

259 OECD Guidelines for the security of Information systems 26 November 1992 http://www.oecd.org/dsti/sti/it/secur/prod/reg97 (aplūkots 2001.gada 21. janvārī)

260 Banku Informācijas tehnoloģijas drošības noteikumu rokasgrāmata. Latvijas Banka, 1998.,8.lpp.

261 Banku Informācijas tehnoloģijas drošības noteikumu rokasgrāmata: Latvijas Banka, 1998., 8.lpp.

262 OECD Guidelines for the security of Information systems 26 November 1992 http://www.oecd.org/dsti/sti/it/secur/prod/reg97 (aplūkots 2001.gada 21. janvārī)

Integritāte nozīmē IS aizsardzību no nelikumīgas datorprogrammu, failu, serveru un citu IS komponentu nelikumīgas modifikācijas. Modifikācija var būt gan tīša, gan nejauša.

*Konfidencialitāte* nozīmē, ka dati un informācija ir izpaužami tikai speciāli pilnvarotām personām, institūcijām autorizētā laikā un sankcionētā kārtībā.[263]

Informācijas konfidencialitāte ir iepriekšnoteiktai grupai piederoša slepena vai privāta informācija. Citiem vārdiem sakot, tā ir sensitīva informācija, kas jāaizsargā no nelikumīgas vai pārsteidzīgas izpaušanas.[264] Konfidenciāla informācija var būt pieejama tikai tam personālam, kuru informācijas īpašnieks ir īpaši pilnvarojis lietot tikai viņa darba uzdevumu vajadzībām. Datiem, kuri satur konfidenciālu informāciju, ir jābūt viegli atpazīstamiem, speciāli iezīmētiem, piemēram, ar atzīmi sensitīvi, konfidenciāls, noslēpums u.c. IS, kuras apstrādā konfidenciālu informāciju, ir jānodrošina adekvāta aizsardzība pret indivīda tiesību uz konfidencialitāti vai slepenības pārkāpšanu, kas var radīt draudus sabiedrības drošībai, labklājībai, veselībai.

Informācijas drošības neatņemams elements ir tās aizsardzība no negatīvas informācijas. Taču terminu „negatīva informācija" nedrīkst tulkot šauri, tas ir, uzskatot, ka negatīvā informācija ir tikai tie dati, kas apdraud sabiedrību pēc to satura un kuras apriti ierobežo vai aizliedz likumdevējs. Šeit ar negatīvo informācijas ietekmi ir jāsaprot jebkuri informācijas resursi, arī programmas, rīki, kas radīti speciāli ar mērķi ietekmēt informācijas resursus. Jāpiekrīt, ka informācijas aizsardzība ietver sevī aktīvu vai pasīvu darbību, kas vērsta uz to, lai sasniegtu pēc iespējas drošu informācijas resursu stāvokli.[265] Šāda pieeja ir nostiprināta daudzu valstu skaidrojošās vārdnīcās.

Teorija par noziedzīgiem nodarījumiem pret informācijas sistēmu drošību un kibernoziegumiem kopumā ir ļoti vāji attīstīta. Bieži vien pasaulē tiek pausti diametrāli pretēji viedokļi par šīs grupas nodarījumu teorētiskajām problēmām. Tāpēc pētījumi un secinājumi šajā jomā ir jāuztver ļoti piesardzīgi, jo jebkurai tādai

---

263 Ibid., OECD, http://www.oecd.org/dsti/sti/it/secur/prod/reg97 (aplūkots 2001.gada 21. janvārī)

264 Information security in Nordic Countries. Nordiske Seminar-og Arbeijds rapporter 1993:613 p12

265 Ibid.,Гаврилов О.А. с.56

teorijai trūkst lietojuma prakses. Galvenais jautājums, kas rodas, pētot juridisko literatūru un salīdzinot dažādu valstu krimināllikumus, kādu vietu likumdevējs atvēl noziedzīgiem nodarījumiem pret informācijas sistēmu drošību, proti, vai tie ir kodificēti atsevišķā krimināllikuma nodaļā ar vienotu grupas objektu vai arī tie ir kodificēti apakšnodaļās ar vienotu sugas objektu vai arī tie vispār netiek atsevišķi izdalīti un iekļauti nodaļās, kas apvieno dažādus noziedzīgus nodarījumus, kuriem grūti atrast kopēju apdraudēto interesi.

Piemēram, V. Krilovs raksta, ka „..noziegumi datorinformācijas jomā ir sabiedriski bīstami nodarījumi, kas vēršas pret attiecībām, kas nodrošina informācijas, vākšanas, apstrādes, uzkrāšanas, glabāšanas, meklēšanas un izplatīšanas procesa drošību".[266] Tālāk viņš norāda, ka šo nodarījumu sugas *(выдовой)* objekts ir sabiedriskās attiecības, kas nodrošina informācijas aprites procesu drošību un noteiktās kārtības ievērošanu, bet tiešais objekts informācijas sistēmu drošība, un šīs kategorijas noziedzīgo nodarījumu priekšmets ir priekšmetiski nostiprināta datorinformācija, taču tie nevar būt sistēmas programmatiskie un tehniskie līdzekļi.[267] Ar priekšmetiski nostiprinātu datorinformāciju viņš apzīmē tādu informāciju, kas atrodas mašīnnesējā vai atrodas datortīklā. Līdzīgu viedokli, ka KF Krimināl kodeksa 28. sadaļā ietverto noziedzīgo nodarījumu sugas *(выдовой)* objekts ir informācijas sistēmu drošība automātiskajās datorsistēmās, pauž arī B. Jaceļenko[268]. Savukārt I. Klepickis uzskata, ka Krievijā šo nodarījumu grupas objekts ir informācijas sistēmu drošība kā sabiedriskās drošības elements- sabiedriskās attiecības, kas nodrošina datorsistēmu un tīklu drošu ekspluatāciju, kas izslēdz kaitējuma nodarīšanas iespēju personām, sabiedrībai un valstij. Šo nodarījumu tiešais objekts ir atsevišķa veida attiecības, kas ietilpst ISD saturā: sistēmas īpašnieka tiesības uz sistēmā uzturētās informācijas neaizskaramību; interese par pareizu sistēmas ekspluatāciju, bet priekšmets- automātiskā datu apstrādes sistēma, kas ietver sevī materiālo elementu datorsistēmu

---

[266] Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва- Юриспрудения. 1999.с. 653

[267] Ibid.c. 653

[268] Росийское уголовное право. Особенная ч. Учебник. Под. ред. М.П. Журавлева и С.М. Никулина. Москва- Спарк, 1998 с. 336

un tīklu un nemateriālo elementu programmas un citu informāciju. A. Volevodzs uzskata, ka KF KK noteic atbildību par noziedzīgiem nodarījumiem, kuru grupas objekts ir ar likumu aizsargātas sabiedriskās attiecības datorinformācijas jomā.[269] V. Krilovs un V. Golubevs uzskata[270], ka visiem ar datoriem saistītiem nodarījumiem jābūt vienotiem ar grupas objektu - nodarījumi pret informācijas vidi, savukārt I. Klepickis, A. Adamskis[271]- ka visu šo nodarījumu tiešais objekts ir informācija un tāpēc tiem jābūt klasificētiem kā nodarījumiem pret informāciju, bet A. Voļevodzs, S. Pašins[272] sašaurina šo apdraudēto interesi un klasificē šos nodarījumus kā vērstus pret datorinformāciju u.c. Autors uzskata, ka atbalstāms ir I. Klepicka un A. Voļevodza viedoklis, ka informācijas sistēmu drošība ir jāapskata kā grupas objekts. Konsekventus soļus šīs tēzes realizēšanā ir veikusi, piemēram, Ukraina. V. Golubevs norāda, ka Ukrainas Rada 2003.gada 19. jūnijā pieņēma Likumu „Par Ukrainas nacionālo drošību", un viena no likuma prioritātēm ir cīņas pastiprināšana pret datornoziedzību un datorterorismu.[273]Līdz ar to noziedzīgi nodarījumi pret informācijas sistēmu drošību jebkurā to izpausmes veidā ir oficiāli atzīti par valsts drošības apdraudējumu.

Krimināllikuma XX nodaļa, kurā iekļauti noziedzīgi nodarījumi pret informācijas sistēmu drošību (KL 241.-245. pants), grupēti ar diviem objektiem, tas ir, ar vispārīgo drošību un sabiedrisko kārtību. Kā jau iepriekš minēts, tad „vispārīgā drošība" nevar tikt atzīta par grupas objektu, jo tai nav raksturīgs specifisks pazīmju kopums, kas dotu pamatu nošķirt šos nodarījumus no citu grupu nodarījumiem, tāpēc par Krimināllikuma XX nodaļā iekļauto noziedzīgo

---

269 Ibid., Волеводз А.Г.с. 61

270 Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва- Юриспрудения. 1999.с. 653; Criminal and legal aspects of fighting crime by V. Golubev// htttp://www.crime-research.org/library/Golubev_nov.html (aplūkots 2004.gada 23. martā)

271 Уголовное право Российской федерации. Особенная часть. Подю ред. Б.В. Здравомыслова. Москва-Юристь, 1999., с. 349
Information management: Legal and security issues by Andrzej Adamski// http://www.uncjin.org/Other/korebo/chapter5.pdf (aplūkots 2004.gada 23. martā)

272 Волеводз А.Г. Противодействие компютерным преступлениям. Правовые основы международного сотрудничества. Москва: Юрлитинформ, 2002.,с.61; Коментарий к уголовному кодексу Росийской федерации. Издание 3-е измененное и дополненное. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва- издательская группа Инфра · М-Норма,2000., с.696-697

273 Голубев А. Компютерная преступность – угроза национальной безопасности/. Cybercrime research centra mājas lapa http://www.crime-research.ru/library/interv2.html (aplūkots 2003.gada 21. novembrī)

nodarījumu grupas objektu atzīstams personu interešu aizskārums uz sabiedrībā vispārpieņemtu sabiedrisko kārtību. Vai informācijas sistēmu drošība arī ir saistīta arī ar personu tiesību interešu pārkāpšanu uz sabiedrisko kārtību? Domāju, ka ne. Lai pamatotu šo viedokli, nepieciešams apskatīt pazīmes, kas raksturo grupas objektu - sabiedriskā kārtība. Pie šādām savrupām pazīmēm var pieskaitīt sabiedrībā vispārpieņemtu personas uzvedības morālo standartu un šīs uzvedības publisko – sabiedrisko raksturu vai šīs uzvedības normatīvo regulējumu.

Informācijas sistēmu drošība pēc sava rakstura nav saistīta ne ar vienu no iepriekšminētajām pazīmēm, to neraksturo ne vispārpieņemti sabiedrības uzvedības standarti, tai nav publiska rakstura, jo tās darbība ir saistīta ar elektronisko vidi, tādējādi gan to īstenojot, gan arī apdraudēt var tikai ar darbībām, kas izdarītas ar speciālu ierīču palīdzību un izņemot atsevišķus informācijas sektorus, tai nav vispārobligāta regulējuma.

Noziedzīgiem nodarījumiem, kas vērti pret informācijas sistēmu drošību, ir raksturīgs specifisku pazīmju kopums, kas tos individualizē un gan teorētiski, gan praktiski nošķir no citām noziedzīgo nodarījumu grupām. Var izdalīt šādu pamatpazīmju grupu, bez kurām šādu noziedzīgu nodarījumu kvalifikācija nav iespējama: 1) visi iepriekšminētie noziedzīgie nodarījumi ir saistīti ar automatizēto datu apstrādes procesu. Gan teorijā, gan arī praksē ar automatizēto datu apstrādes procesu var būt saistīti arī citi noziedzīgi nodarījumi, taču, vērtējot informācijas tehnoloģiju izmantošanu kā noziedzīga nodarījuma rīku tradicionālo noziegumu veikšanai, šai pazīmei vienmēr būs tikai speciālās pazīmes raksturs; 2) visi iepriekšminētie noziedzīgie nodarījumi var tikt izdarīti tikai no attāluma, t.i., izmantojot automatizētas datu apstrādes sistēmas vai tās elementus, kas savienoti ar elektroniskiem tīkliem; 3) darbībai ir jābūt vērstai pret vienu vai vairākiem informācijas sistēmas drošības elementiem, t.i., integritāti, pieejamību vai konfidencialitāti, vai arī pret informācijas sistēmu drošību kā sistēmu kopumā. Neesot kādai no šīm pamatpazīmēm, nav arī pašu noziedzīgo nodarījumu; 4) nodarījumus var izdarīt tikai ar tīšu darbību, kas ietver sevī *dolus directus* un *dolus eventualis*; 5) personai, kas izdara noziedzīgos nodarījumus, jābūt atzītai par krimināltiesību subjektu.

Pie speciālām pazīmēm, kas parasti raksturo noziedzīgos nodarījumus pret informācijas sistēmu drošību, var pieskaitīt: 1) konkrēto automatizētās datu apstrādes sistēmas izmantošanas veidu apdraudējuma priekšmetu, nodarījuma izdarīšanas rīku vai kā mediju nelikumīgas informācijas apritei); 2) darbības veidu (*modus operandi*)- vai darbībā iesaistīta viena vai vairākas datu apstrādes sistēmas vai elementi; 3) vai nodarījums vērsts pret īpaši ar likumu aizsargātu automatizēto datu apstrādes sistēmu grupu u.c.

Vadoties no noziedzīgo objektu klasifikācijas teorijas un no elementārās loģikas viedokļa, informācijas sistēmu drošība ir atzīstama par grupas, bet nevis tiešo apdraudējuma objektu, tāpēc autors ierosina izveidot Krimināllikumā jaunu nodaļu „Noziedzīgi nodarījumi pret automatizēto datu apstrādes sistēmu drošību" un ietvert tajā Krimināllikuma 241.- 245. pantā paredzētos noziedzīgos nodarījumus.

### 3.3. Noziedzīgu nodarījumi pret informācijas sistēmu drošību objektu klasifikācijas salīdzinošie aspekti

*Rietumvalstu krimināltiesībās*

Analizējot citu valstu krimināllikumus, jāsecina, ka nosacīti šī veida nodarījumus klasificē īpašā sadaļā tikai dažas Rietumeiropas un Viduseiropas valstis. Piem., Francijas KL III sadaļa paredz grupas objekta apdraudēto interesi "Automātisko datu apstrādes sistēmu darbības apdraudējumi". Sadaļā ir iekļauti tādi noziedzīgu nodarījumu sastāvi kā, piemēram, patvaļīga piekļūšana, sistēmā esošu datu un resursu integritātes pārkāpšana, darba traucēšana, datorkrāpšana u.c. Zināma sistematizācija ir ievērota arī Polijas KL XXXIII sadaļā „Noziedzīgi nodarījumi pret informācijas aizsardzību", kas ietver tādus nodarījumus kā, piemēram, nelikumīga datorinformācijas iznīcināšana, bloķēšana, bojāšana, izmainīšana, kas rada apdraudējumu valsts vai sabiedrības interesēm u.c.

Savukārt Vācijas, Beļģijas, Nīderlandes, Grieķijas, Austrijas, Šveices, Itālijas, Spānijas, Zviedrijas, Somijas, Dānijas, Norvēģijas, Islandes, Ungārijas, Rumānijas, Serbijas u.c valstu krimināllikumos noziedzīgi nodarījumi pret informāciju sistēmu drošību nav īpaši sistematizēti un tos nesaista ar kādu specifisku noziedzīgu nodarījumu grupu. Līdz ar to šeit nevar runāt par grupas objektu, kaut gan kodeksos

dažādās sadaļās ir iekļauti KL 241- 244. pantā paredzētie noziedzīgo nodarījumu sastāvi.

Kā redzams no iepriekšminētā, tad nodarījumu pret informācijas sistēmu drošību sasaiste ar grupas objektu ne vienmēr ir konsekventa, jo iepriekšminētie piemēri uzskatāmi pierāda, ka Rietumvalstu un Viduseiropas krimināltiesību doktrīnās netiek atbalstīta tēze, ka grupas nozieguma objekta sastāvdaļa ir konkrētais nozieguma objekts- apdraudētā tiesiskā interese. Arī šo valstu juridiskajā literatūrā[274] padomju krimināltiesību prakse, klasificējot noziegumu objektus pēc vertikāles, netiek atbalstīta.

*Objektu klasifikācijas problēmas NVS valstīs*

Saskaņā ar vienošanos par Neatkarīgo Valstu Sadraudzības (NVS) sadarbību cīņā ar noziegumiem datorinformācijas jomā, par noziegumu datorinformācijas jomā atzīst krimināli sodāmu nodarījumu, kura priekšmets ir datorinformācija. Datorinformācija - informācija, kas sagatavota veidā, kas dod iespēju to apstrādāt datorsistēmās un pārraidīt elektroniski sakaru kanālos.[275] Tomēr, kā tas būs redzams turpmāk, tad ne visās NVS valstīs normatīvās bāzes harmonizācijā datornoziegumu jomā ir vienota pieeja.

Ukrainas KK XVI sadaļa "Noziedzīgi nodarījumi datorsistēmu un datortīklu jomā" par grupas objektu atzīst intereses, kas rodas, nodrošinot informācijas drošību datorsistēmās un datortīklos. Savukārt Kazahijas un Kirgīzijas KK šī veida nodarījumi ir iekļauti sadaļā „Noziedzīgi nodarījumi ekonomiskā jomā". Baltkrievijas KK XII sadaļā ir izdalīti noziegumi pret informācijas sistēmu drošību. Minētajā sadaļā iekļauti tādi nodarījumi, piemēram, nesankcionēta piekļuve datorinformācijai, datorinformācijas modifikācija, datorsabotāža, nelikumīga datorinformācijas piesavināšanās, speciālo rīku, kas dod iespēju piekļūt nelikumīgi datorsistēmai, izgatavošana u.c. Gruzijas un Azerbaidžānas KK šie nodarījumi, līdzīgi kā Krievijas Federācijas KK, ir iekļauti sadaļā „Noziedzīgi nodarījumi

---

[274] Ibid., Simester A.P., Sullivan G.R. pp.74-97; Wayne R. La Fave Criminal Law. Hornbook Series. Student edition. Thomson- West, 2003., pp;.12-15; Fundamentals of criminal law. Second edition. Paul. H. Robinson. Little, Brown and company. Boston- new- York- Toronto- London,[b.g] p.27.; Essays in Crimial law Nils Jareborg Iustus Förlag. Juridiska Förennigen i Uppsala,[b.g.] pp.11-13.

[275] Ibid., Волеводз А.Г. с. 475.

datorinformācijas jomā". Moldovas likumdevējs šobrīd strādā pie grozījumiem KK, kas paredz ieviest sadaļu „Noziedzīgi nodarījumi pret informācijas drošību", kurā tiks iekļauti tādi noziedzīgi nodarījumi kā, piemēram, nesankcionēta piekļuve datorinformācijai un tās nelikumīga ieguve, speciālu līdzekļu, kuru mērķis ir ietekmēt datorsistēmas resursus, nelikumīga izgatavošanu un izplatīšana u.c.

Kaut arī šīs grupas apdraudētā interese ir nosaukta dažādi- gan par informācijas sistēmu drošības apdraudējumu, gan valsts ekonomikas apdraudējumu, gan sabiedrības drošības apdraudējumu, tomēr visiem šiem nodarījumiem ir vairākas kopīgas iezīmes, kas dod pamatu secināt, ka aizskartā tiesiskā interese ir informācijas sistēmu drošība, kas ir valsts, sabiedrības, indivīda drošības veseluma elements.

## III nodaļa Noziedzīgie nodarījumi pret informācijas sistēmu drošību (turpmāk tekstā –ISD)

### 1. Noziedzīgu nodarījumu pret ISD vispārīgs raksturojums

Starptautiskajā klasifikācijā par noziedzīgiem nodarījumiem, kas saistīti ar informācijas sistēmu drošību, atzīst šādus noziedzīgus nodarījumus: 1) patvaļīga piekļūšana automatizētās datu apstrādes sistēmas resursiem; 2) datu un sistēmu darbības traucēšana; 3) nelikumīga informācijas pārtveršana; 4) ierīču ļaunprātīga izmantošana. Krimināllikuma XX nodaļā „Noziedzīgi nodarījumi pret vispārīgo drošību un kārtību" 241. pants paredz krimināltatbildību par patvaļīgu piekļūšanu datorsistēmai" (redakcijā līdz 2005.gada 1. jūnijam[276]- turpmāk tekstā līdz 01.06.2005.) un patvaļīgu piekļuvi automatizētai datu apstrādes sistēmai (2005.gada 28. aprīļa redakcijā - turpmāk tekstā 28.04.2005.), 242. pants- par „datortehnikas neatļautu iegūšanu"(līdz 01.06.2005.), 243. pants par datortehnikas programmatūras bojāšanu (līdz 01.06.2005.) un automatizētās datu apstrādes sistēmas darbības traucēšanu un nelikumīgu rīcību ar šajā sistēmā iekļauto informāciju (28.04.2005.), 244. pants par datora vīrusa izplatīšanu (līdz 01.06.2005.) un nelikumīgām darbībām ar automatizētās datu apstrādes sistēmu resursu ietekmēšanas ierīcēm"

---

[276] 2005.gada 28. aprīlī Saeima pieņēma grozījumus Krimināllikuma 241. pantā, 243. un 244. pantā un izslēdza 242. pantu, atstājot tos spēkā līdz 2005.gada 1. jūnijam, bet pēc 1. jūnija stājas spēkā Krimināllikuma 241. panta"patvaļīga piekļūšana automatizētās datu apstrādes sistēmai", 243. pants „"Automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju", 244. pants" Nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm" Minētie grozījumi spēkā ar 2005.gada 1. jūniju.

(28.04.2005.); 245. pants -par informācijas sistēmas drošības noteikumu pārkāpšanu.

Likumdevējs nav šo noziedzīgo nodarījumu skaitā iekļāvis noziedzīgu nodarījumu „nelikumīga informācijas pārtveršana", jo šis noziedzīgais nodarījums ietverts Krimināllikuma XIV nodaļā „Noziedzīgi nodarījumi pret personas pamattiesībām un pamatbrīvībām" 144. pantā „Korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšana". Šāda pieeja, ka noziedzīgs nodarījums tiek klasificēts kā nelikumīga korespondences noslēpuma pārkāpšana un kodificēts citās krimināllikumu nodaļās, ir sastopama arī citu valstu krimināllikumos.

### 1.1. Noziedzīgu nodarījumu pret informācijas sistēmu drošību tiešais apdraudējuma objekts

Noziedzīgs nodarījums vienmēr būs konkrēta darbība, tā būs vērsta pret konkrētu objektu, tāpēc nekādi nodarījuma objekts nevar pastāvēt vispārēja vai grupas objekta veidā, līdz ar to faktiski ir tikai viens objekts, tas, ko juridiskajā literatūrā pieņemts saukt par tiešo objektu.[277] Līdzīgu viedokli paudis arī P. Mincs, norādot, ka katrā ziņā šim labumam (konkrēti vai abstrakti) ir jābūt aizskartam.[278] Tiešais šo noziedzīgo nodarījumu apvienojošais objekts ir tiesiskā interese realizēt informācijas drošību, tas ir, nodrošināt informācijas sistēmu resursu pieejamību, integritāti un konfidencialitāti, jo, kā pamatoti norāda U. Krastiņš[279], tad par tādu nevar atzīt mantu vai citus materiālus labumus, piem., sistēmas resursus, datu nesējus, tīklus u.c. Ja pieņemam, ka objekts ir informācijas sistēmu drošība, ko raksturo trīs pazīmes- integritāte, konfidencialitāte un pieejamība, tad nodarījumu veidi pret informācijas sistēmu drošību arī dalāmi nodarījumos pret informācijas pieejamību, pret informācijas integritāti un pret konfidencialitāti.

Piemēram, patvaļīga piekļūšana datorsistēmai vienmēr būs nodarījums, kas vērsts pret informācijas pieejamības interesēm, proti, ka pieejamības kārtību IS ir tiesīgs noteikt tikai informācijas sistēmas īpašnieks vai tiesiskais valdītājs un tās pārkāpšana vienmēr skars šo personu intereses. Nodarījumi, kas saistīti ar IS datu un resursu traucēšanu, programmu bojāšanu, pamatā ir vērsti pret sistēmas īpašnieka vai tiesiskā valdītāja vai informācijas resursu īpašnieka interesi saglabāt sistēmā esošo informāciju nemainīgā stāvokli, uzturēt tās veselumu. Savukārt nodarījumi, kas saistīti ar

---

277 Ibid., Новоселов Г.П. с. 22

278 Turpat, Mincs P., 75. lpp.

279 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 40 .lpp.

nelikumīgu datu pārtveršanu, noklausīšanos, vienmēr būs saistīti ar konfidencialitātes intereses aizskārumu.

Analizējot noziedzīgo nodarījumu pret informācijas sistēmu drošību, secinu, ka minētais nodarījums nevar notikt, ja netiek pārkāpta pieejamības, integritātes vai arī konfidencialitātes interese, kas pati par sevi neveido noziedzīga nodarījuma sastāvu. Taču sistēmas resursu integritātes pārkāpšana vienmēr būs saistīta ar specifisku noziedzīga nodarījuma objekta priekšmetu, tas ir, informācijas sistēmu resursiem. Integritātes vai pieejamības pazīmes tieši neveido noziedzīga nodarījuma grupas objektu, jo integritāte un pieejamība nav obligātas pazīmes, kas raksturo sabiedrības drošību. Sabiedrības drošību var apdraudēt arī tad, ja netiks aizskarta neviena no šīm trim pazīmēm. Taču nodarījumos pret informācijas sistēmu drošību integritātei, pieejamībai un konfidencialitātei ir izšķiroša nozīme. Tās ir pazīmes, bez kuru konstatēšanas nevar būt ne runas par noziedzīgu nodarījumu pret informācijas sistēmu drošību.

### 1.2. Noziedzīgo nodarījumu pret informācijas drošību priekšmets

Juridiskajā literatūrā plaši ir pārstāvēts viedoklis, ka noziedzīga nodarījuma priekšmets ir ārējās pasaules materiālie priekšmeti, uz kuriem tieši, apdraudot konkrēto interesi, iedarbojas noziedznieks.[280] Taču uzreiz rodas jautājums: „Kas noziedzīgos nodarījumos pret informācijas sistēmu drošību ir nozieguma priekšmets?" Ja pieņemam, ka galvenais apdraudējuma priekšmets šīs kategorijas nodarījumos ir informācijas resursi, tad kā varam atzīt par materiālās pasaules priekšmetu informāciju, kas sagatavota datordatu veidā un apdraudējuma brīdī tiek pārraidīta datortīklos kā elektronu plūsma? Jautājums nebūt nav vienkāršs, jo juridiskajā literatūrā pastāv diezgan būtiska viedokļu atšķirība par to, kas ir šo nodarījumu apdraudējuma priekšmets. Piemēram, J. Krasikovs uzskata, ka enerģija, gāze un informācija nevar būt zādzības priekšmets, jo tām nav nepieciešamo

---

[280] Наумов А.В. Росийское уголовное право. Общая ч. Курс лекций. Москва: БЕК, 1996. с. 154; Учебник Уголовного права. Общая ч. Под. Ред. В.Н. Кудрявцева и А.В. Наумова. Москва: Спарк, 1996. с. 88; Курс уголовного права. Общая ч. Том 1. Учение о преступлении. Под. Ред Н. Ф. Кузнецовой т И.М. Тяжковой. Москва: Зеркало, 1999. с.210; Росссийское уголовное право. Общая ч. Учебник Под. Ред. М.П. Журавлева. 1999. Москва: издательство "Щит-М" 1999.с. 59; Уголовное право Росийской федерации Общая часть. Под. Ред. Б.В. Здравомыслова Москва: Юристь.1999.с.117 ; Уголовное право Росии. Учебник для вузов. В 2- х томах. Т.1. Общая часть. Под. ред. А.И. Игнатова и Ю. А. Красикова. Москва- Норма- Инфра- М, 1999.с.112; Turpat, Krastiņš U., 44 .lpp.

priekšmetisko pazīmju.[281] Citu viedokli pauž A. Voļevodzs. Viņš norāda, ka noziedzīga nodarījuma priekšmets var būt gan individuāli noteikta lieta, gan mantiska, nemantiska rakstura labumi, to skaitā arī informācija.[282] Tomēr rodas pamatots jautājums cik lielā mērā informācijas resursiem var attiecināt īpašumtiesības, to skaitā arī valdījumu.

Tiesu praksē ir sastopamas kuriozas situācijas, kad personas tiek atbrīvotas no atbildības par informācijas kā materiālas substances zādzību, piemēram, krimināllietā (*Oxford v Moss*[283]) u.c. Taču pret informācijas zādzību daudzās valstīs joprojām izturas piesardzīgi, jo uzskata, ka informāciju nevar atzīt par kustamu, taustāmu lietu, ko varētu izņemt no citas personas likumīga valdījuma. Vairāki autori, piem., T. Smedinghofs, uzskata, ka informācija nevar būt īpašums vai valdījums tāpēc, ka tiesības uz informāciju pastāv atrauti no jebkuras informācijas kopijas. Neatkarīgi no tā, vai šī informācija ir saglabāta fiziskā datu nesējā, piem., disketē, kompaktdiskā, minidiskā, tās īpašuma tiesības nav atkarīgas no konkrētā informācijas nesēja.[284]

Šim viedoklim nevar piekrist, jo iepriekšminētais autors informāciju ir aplūkojis kā no datu nesēja atrautu vienību, bet, ja informācija atrodas datorsistēmā, tad pati datorsistēma vai datu nesējs ir materiālās pasaules priekšmeti, fiziski eksistējošas lietas, līdz ar to arī informācija, kas saglabāta šajos datu nesējos, kļūst par materiālās pasaules vienību jeb, citiem vārdiem, kļūst par dokumentētu informāciju.[285] Kā norāda V. Kopilovs, tad dokumentētu informāciju var tiesiski reglamentēt: 1) no intelektuālo tiesību viedokļa; 2)no civiltiesību lietu tiesību daļas viedokļa.[286]

Civillikums par bezķermenisku lietu runā kā par ķermeniskas lietas sastāvdaļu vai piederumu (CL 850.p.), tad tā pieņem šīs pēdējās īpašības, un saskaņā ar to tā

---

[281] Уголовное право Росиии. Учебник для вузов. В 2- х томах. Т.1. Общая часть. Под. ред. А.И. Игнатова и Ю. А. Красикова. Москва- Норма- Инфра· М, 1999. с.112

[282] Ibid., Волеводз А.Г., с.54

[283] Eisenshitz T.S.Information transfer Policy isues of control and access. London, Library Association publishing,1984., p.38

[284] Online law The spa's legal guide to doing business on the Internet. Th. J. Smedinghoff, ed. The software publishers Association, 1996.p.126

[285] Информационное право. Москва: Юристь, 1997.,с.9

[286] Ibid. с Копилов В.А.с. 24.

uzskatāma vai nu par kustamu vai nekustamu lietu, raugoties pēc ķermeniskās šķiras, pie kuras lieta pieder (CL 846. panta 3.d). Pirmkārt, kā jau noskaidrojām iepriekš, informāciju nevar atraut no ķermeniskām lietām, konkrētajā gadījumā informācijas nesējiem – datora, telefona centrāles, papīra u.c. Visas tās lietas ir ķermeniskas lietas, kuras var pārdot, uzdāvināt, iznomāt. Tātad, ja autoram pieder dators, tad automātiski arī visas tiesības un labumi, kas saistīti ar šī datora izmantošanu.

Ja informācija ir glabājas attiecīgās informācijas sistēmas datu nesējā, tad tā kļūst par šīs sistēmas informācijas resursu neatņemamu sastāvdaļu un uzskatāma par materiālās kustamās mantas (informācijas sistēmas tehnisko resursu) kā galvenās lietas piederumu, un gadījumos, ja persona nelikumīgi iekļūst telpā, kur atrodas datorsistēma, fiziski piekļūst šīs sistēmas resursiem, tad šāda darbība ir kvalificējama pēc KL 175. panta 3.d. kā zādzība, kas saistīta ar iekļūšanu telpā. Taču, ja šī piekļūšana notikusi attālināti, fiziski neiedarbojoties uz sistēmu tehniskajiem resursiem, tad personas darbības ir saistītas ar netaustāma priekšmeta, vērtības vienības, tas ir, digitālā formā sagatavotas informācijas resursu ietekmēšanu un tāpēc šāds nodarījums ir jākvalificē kā kibernoziegums, nesaistot to ar Civillikuma īpašumtiesībām.

Dokumentālas informācijas pazīmes ir: 1) tās fiksācija materiālā nesējā; 2)indentifikācijas iespēja.[287] V. Krilovs pieļauj iespēju, ka par noziedzīgu nodarījumu datorinformācijas jomā varētu atzīt priekšmetiski nostiprinātu datorinformāciju, bet ne programmas, kas nodrošina informācijas apstrādes procesu. Ar priekšmetiski nostiprinātu datorinformāciju viņš saprot tādu datorinformāciju, kas atrodas datorsistēmā vai datu pārraides tīklā. [288] Citu viedokli pauž A. Voļevodzs, norādot, ka minēto nodarījumu priekšmeti ir ne tikai informācijas resursi, bet arī infrastruktūra un tās elementi, jo tiem ir sava vērtība, cena un citas individuāli raksturojošas pazīmes.[289] Viņu papildina I. Klepickis, norādot, ka KF KK 28. nodaļā ietverto nodarījumu kopīgais apdraudējuma

---

[287] Ibid., Волеводз А.Г., с.50

[288] Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва: Юриспрудения, 1999.,с.653

[289] Ibid. Волеводз А.Г. с.55

priekšmets ir automātiskā datu apstrādes sistēma, kas ietver sevī materiālo elementu datorsistēmu un tīklu un nemateriālo elementu programmas, un citu informāciju.[290] Šāds viedoklis novērš, autoraprāt, nesaprotamo apdraudējuma priekšmeta satura norobežošanu no sistēmas programmatiskajiem resursiem un tehniskajiem resursiem.

Pamatojot minēto tēzi, nepieciešams atgriezties pie šīs nodarījumu grupas kopīgās apdraudētās intereses, tas ir, informācijas sistēmu drošības, kuru raksturo tādas obligātas pazīmes kā konfidencialitāte, integritāte un pieejamība. Šo stāvokli nevar sasniegt, ja netiek ņemts vērā visu sistēmas komponentu, tas ir, informācijas un tehnisko resursu kopums.

Šobrīd pabeigts darbs pie MK Noteikumu projekta „Valsts informācijas sistēmu drošības noteikumi". Projekta 1.4.p. noteic, ka informācijas resursi ir valsts informācijas sistēmas sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, sistēmdatne un datu datne (arī tās, kas satur valsts informācijas sistēmā glabājamo, apstrādājamo un valsts informācijas sistēmas lietotājiem pieejamo informāciju). Bet 1.5.p. noteic, ka tehniskie resursi ir informācijas sistēmas sastāvdaļa, kurā ietilpst datori, datortīklu iekārtas, telekomunikāciju aprīkojums un citas tehniskās iekārtas.

Līdz ar to, domājams, nav nepieciešama plašāka diskusija, ka šīs grupas nodarījumu apdraudējuma priekšmets ir automātiskās informācijas sistēmas informācijas un tehniskie resursi vai to daļa. Izpratne par noziedzīga nodarījuma priekšmetu tikai kā cilvēka ārējā pasaulē objektīvi eksistējošu lietu[291] vairs neatbilst mūsdienu realitātei.

Domāju, ka šis jautājums ir risināms tā, ka par noziedzīga nodarījuma apdraudējuma priekšmetu ir atzīstami ne tikai materiālas pasaules priekšmeti, bet arī jebkurš mākslīgi radīts fakts (artifakts)- cilvēka radīta un identificējama vērtība neatkarīgi no tā, vai tā ir materiāla, nemateriāla, virtuālā realitāte u.c. Lai **artifaktu** atzītu par apdraudējuma priekšmetu, tam ir nepieciešami tikai divi elementi: 1) tam ir jābūt cilvēka radītai vērtībai; 2) tam ir jābūt identificējamam. Šī vērtība var būt izteikta jebkurā subjektīvā izpausmes veidā, naudā, intelektuālā ieguldījumā u.c. Līdzīgu viedokli savā autoreferātā aizstāv ari A. Kacmans, norādot, ka „tiešais datornoziegumu apdraudējuma priekšmets ir datorinformācija, tas ir, sabiedrības

---

290 Уголовное право Российской федерации. Особенная часть. Под. ред. Б.В. Здравомыслова. Москва: Юристь, 1999., с.352

291 Turpat, Krastiņš U., 44.lpp.

labā radīta identificējama vērtība, kas ir identificējama".[292] Ja pastāv abi šie elementi, tad par noziedzīga nodarījuma priekšmetu var atzīt jebkuru- gan materiālu, gan nemateriālu, taustāmu, netaustāmu- cilvēka radītu vērtību, tai skaitā arī ADAS glabāto vai citādi apstrādāto elektronisko informāciju un tehniskos resursus.

2. Noziedzīgu nodarījumu pret ISD objektīvās puses vispārīgais raksturojums

2.1. Objektīvās puses jēdziens un elementi

Juridiskajā literatūrā plaši ir pārstāvēts viedoklis, ka noziedzīgā nodarījuma objektīvā puse ir personas uzvedības ārējā izpausme, kas var radīt kaitīgas izmaiņas apkārtējā pasaulē.[293] Noziedzīga nodarījuma objektīvo pusi raksturo obligātās un papildpazīmes. Pie obligātajām pazīmēm, kas raksturo nozieguma objektīvo pusi pieder darbība vai bezdarbība, šīs darbības rezultātā nodarītais kaitējums un cēloņsakarība starp personas aktīvo prettiesisko uzvedību un sekām, bet papildpazīmes var būt vieta, laiks,izdarīšanas veids, nozieguma izdarīšanas rīki u.c.

Turpmāk apskatīsim tikai objektīvo pusi veidojošās obligātās pazīmes, bez kuru konstatēšanas nav iespējams personu saukt pie atbildības par konkrētu noziedzīgu nodarījumu. Šādas pazīmes ir: 1) vainojamās personas darbība vai bezdarbība; 2)cēloņsakarība starp prettiesisko nodarījumu un kaitīgām sekām; 3) kaitīgās sekas.

Jāatzīst, ka objektīvo pusi jeb *actus reus* līdzīgi skaidro arī Vispārējo tiesību un Rietumeiropas krimināltiesību teorijā. Tā, piem., P. Robinsons, Š. Dando u.c. norāda, ka tradicionāli *actus reus* satur trīs elementus: 1) nelikumīgo darbību vai bezdarbību; cēloņsakaru un šo nodarījumu kaitīgās sekas.[294] A. Simesters un Sulivans šos trīs *actus reus* elementus nosauc tā : uzvedība, sekas un apstākļi.[295] K. Klarka precizē, ka *actus reus* raksturo šādi elementi:1) uzvedībai ir jābūt aizliegtai

---

[292] Ibid., Kacman. A. ,p.53.

[293] Turpat, Krastiņš U., 49.lpp.; Turpat, Lejiņš P., 47.lpp.; Наумов А.В. Росийское уголовное право. Общая ч. Курс лекций. Москва: БЕК, 1996. с. 136; Росссийское уголовное право. Общая ч. Учебник Под. Ред. М.П. Журавлева. 1999. Москва: издательство "Щит-М" 1999.,с.62; Уголовное право Росийской федерации Общая часть. Под. Ред. Б.В. Здравомыслова Москва : Юристъ.1999. , с.124; Уголовное право Росии. Учебник для вузов. В 2- х томах. Т.1. Общая часть. Под. ред. А.И. Игнатова и Ю. А. Красикова. Москва: Норма- Инфра· М, 1999., с.115

[294] Fundamentals of criminal law. Second edition. Paul. H. Robinson. Little, Brown and company. Boston- new- York- Toronto- London., p. 54.; The Criminal law of Japan. The General part. p. 58-77; Criminal law in Denmark by Lars Bo Langsted, Van Greve and Peter Garde. Kluwer law International. The Hague· London · Boston, 1998. pp.83-89; Ibid., Clarcson C.M.V., pp.14-18

[295] Ibid.,Simester A.P. and Sullivan G.R. p. 59

un krimināli sodāmai; 2)pārkāpēja nodarījumam jābūt paveiktam; 3) notikumam jārada kaitējums, un uzvedībai jābūt tiešā cēloniskā sakarā ar radušos kaitējumu.[296]

No iepriekšminētā var secināt, ka noziedzīga nodarījuma objektīvās puses satura noteikšanā lielākajā daļā pasaules valstu krimināltiesību teorijās pausts līdzīgs viedoklis. Tas faktiski atbilst arī Latvijas krimināltiesību teorijā piemērotajam. Tātad noziedzīga nodarījuma objektīvo pusi veido nelikumīga darbība vai bezdarbība, šī nodarījuma rezultāts ir noteiktu negatīvu seku rašanās vai iespējamība, ka šādas sekas var rasties, un nodarījumam ir jābūt cēloniskā sakarā ar radušamies kaitīgām sekām.

*Prettiesiska darbība*

P. Lejiņš raksta, ka „.. "prettiesīgs" ir negatīvs jēdziens, un tādēļ viņa saturu nosaka atbilstība pozitīvajam jēdzienam: tiesīgs. Prettiesīgs ir viss tas, kas ir pret tiesībām".[297] Noziedzīgs nodarījums vienmēr ir saistīts ar konkrētas personas nelikumīgu vainojamu darbību vai bezdarbību, taču, ievērojot minētā darba specifiku, ka noziedzīgus nodarījumus pret informāciju sistēmu drošību var izdarīt tikai tīši, ar tiešu vai netiešu nodomu, autors neanalizēs nelikumīgas bezdarbības tiesiskos aspektus.

Juridiskajā literatūrā pausts viedoklis, ka darbība ir cilvēka uzvedības ārējā izpausme. A. Piontkovskis norāda, ka cilvēka darbība ietver sevī ne tikai cilvēka ķermeņa kustības, bet arī šo kustību spēka radīto likumsakarību izmantošanu.[298] Šim viedoklim nepiekrīt V. Kudrjavcevs un norāda, ka nav pareizi iekļaut darbības saturā cilvēka spēka darbības radītās likumsakarības.[299] Autors uzskata, ka, analizējot, nelikumīgas darbības saturu, ir jāņem vērā arī tas, ko A. Piontkovskis sauc par cilvēka radīto darbību spēka likumsakarībām, kas var izpausties ne tikai kā pati darbība, bet arī kā procesi, ko cilvēks vada pat bez īpaša spēka iedarbības, piemēram, zinātnes sasniegumus izmanto kā nozieguma rīkus u.c.

---

[296] Catherine Therese Clarke. From Crimnet to cyber perp: towards an inclusive approach to policing. The involving criminal mens rea on the Internet, Oregon Law rewiew, Spring, 1996.

[297] Turpat.,Lejiņš P., 62. lpp.

[298] Курс советского уголовного права в шести томах. Том. 2. Часть общая " Преступление" под. Ред. А.А. Пионтковского. Москва: Наука, 1970., с. 323

[299] Кудрявцев В.Н. Объективная сторона преступления. Москва: Госюриздат, 1960., с. 11-21

Darbību vienmēr raksturo šādas pazīmes: 1) tai ir jābūt ar krimināllikumu aizliegtai nodarījuma brīdī; 2) tai ir jābūt reālai un aktīvai, tīši vērstai uz konkrētu negatīvu rezultātu; 3) personai jāapzinās, ka tā veic aktīvu darbību un vēlas konkrēta negatīva rezultāta iestāšanos.

Līdz ar to jāpiekrīt U. Krastiņam, kas norāda, ka par darbību krimināltiesiskā nozīmē uzskatāma personas apzināta, aktīva, kaitīga, prettiesiska uzvedība, ar ko tiek realizēta šīs personas griba un tās rezultātā tiek izdarīts Krimināllikumā paredzēts ar likumu aizsargāto interešu apdraudējums.[300]

*Kaitīgās sekas*

Krimināltiesību teorijā un praksē ir pieņemts uzskatīt, ka katrs noziedzīgs nodarījums apkārtējā vidē atstāj noteiktu ietekmi. Šāda teorētiska un praktiska pieeja ir plaši izplatīta gan kontinentālajā, gan angļu- amerikāņu tiesību sistēmā. Angļu zinātnieki uzskata, ka„.. seku nepieciešamība ir arī pamats, lai izprastu *actus reus* nozīmi krimināltiesībās". [301] Faktiski vairāki Rietumvalstu tiesību zinātnieki starp kaitīgām sekām un nodarījuma kaitīgumu liek vienādības zīmi.[302]

Tomēr Latvijas krimināltiesību zinātnē noziedzīgā nodarījuma kaitīgās sekas netiek identificētas ar nodarījuma kaitīgumu. U. Krastiņš norāda, ka nodarījuma kaitīgums ir svarīgākā krimināalatbildības pazīme. Tā izpaužas kā būtisks apdraudējums valsts, sabiedrības un atsevišķu personu interesēm.[303] No tā izriet, ka sekas ir tikai viena no noziedzīgā nodarījuma kaitīguma raksturojošām pazīmēm. Tās rada būtiskas izmaiņas ar krimināllikumu aizsargātās interesēs.[304]

Tāpēc kaitīgās sekas ir jebkura noziedzīga nodarījuma obligāts priekšnosacījums, jo to nosacījumus parasti ietver panta dispozīcijā. Tās var būt materiāla rakstura, piemēram, izteiktas naudas izteiksmē, ja tās saistītas ar mantas iznīcināšanu vai bojāšanu, gan arī nemantiska rakstura, piemēram, goda un cieņas aizskaršana, vai komercdarbības traucēšana, datu pārraides bloķēšana, datu

---

300 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 57.lpp.

301 Ibid., A.P. Simester , G.R. Sullivan, p. 75

302 Ibid., A.P. Simester , G.R. Sullivan, p. 75; Wayne R. LaFave Criminal law Fourth edition Hornbook Series Student edition. Thomson West., 2003..,pp.13-15; Ibid., Shigemitsu Dando, p. 16-20

303 Turpat, Krastiņš U., 7.lpp.

304 Turpat, Krastiņš U., 61.lpp.

modifikācija, u.c. Tāpēc pamatots ir U. Krastiņa un citu autoru viedoklis, ka kaitīgās sekas var būt gan materiāla, morāla, organizatoriska, politiska rakstura.[305]

Ja sekas ir obligāts krimināltiesību elements, tad šādus nodarījumus sauc arī par materiāliem noziedzīgu nodarījumu sastāviem. Turpretim, ja likumdevējs panta dispozīcijā nav paredzējis seku iestāšanās obligātumu, tad šādus nodarījumus sauc par formāliem nodarījumiem, un atbildība tādā gadījumā iestājas tikai par nelikumīgas darbības faktu, negaidot, kādas sekas var iestāties.[306] Taču tas nenozīmē, ka šo nodarījumu rezultātā neiestājas nekādas sekas, tikai šo seku apjoms neietekmē krimināltiesību pamatu.

*Cēloņsakarība*

Krimināltiesību teorijā un praksē pastāv stingrs nosacījums, ka krimināltiesību iestājas tikai tad, ja pastāv cēloņsakarība starp prettiesisko darbību un kaitīgām sekām. Cēloņsakarība ir to (materiālo) noziedzīgo nodarījumu sastāvs, kur likumdevējs atbildības nosacījumu saistījis ar konkrētu seku iestāšanos, objektīvās puses obligāta pazīme.

Juridiskajā literatūrā plaši tiek pārstāvēts viedoklis, ka cēloņsakarībai ir vairāki obligāti priekšnosacījumi: 1) cēlonis vienmēr rodas pirms sekām (laika atstarpe starp cēloni un sekām); 2) seku iestāšanas ir likumsakarība, bet ne gadījuma rakstura. Respektīvi, darbību par seku cēloni var atzīt tikai tad, ja seku iestāšanās bija neizbēgama; 3) iestājušās kaitīgās sekas ir tieši šīs darbības rezultāts.[307] To, ka cēloņsakarības izvērtēšanā starp Latvijas krimināltiesību teoriju un Rietumvalstīs praktizēto nav lielas atšķirības, pierāda Džs. Fletčers. Viņš raksta, ka Rietumvalstu krimināltiesību teorijā cēloņsakarību ilustrē šāds piemērs: X ir Y rezultāts tikai tad, ja X ir bijis pirms un bez X - Y nevarētu iestāties. Šo testu sauc par *sine qua non – ja nebūtu.* Ja nebūtu X darbība, nevarētu iestāties Y rezultāts.[308] Mūsuprāt, iepriekšminētos nosacījumus ietver U. Krastiņa cēloņsakarības definīcija : „Cēloņsakarība (*nexus causalis*) krimināltiesībās ir tāda objektīva saikne starp

---

[305] Turpat, Krastiņš U., 63.lpp.

[306] Флетчер Дж. и Наумов А.В. Основные концепции современного уголовного права. Москва: Юристь, 1998., с.174; Ibid., Егоров В.С. . с.34; Ibid., Новоселов Г. с.49; Turpat, Krastiņš U., 63.lpp.

[307] Ibid., Флетчер Дж и Наумов А.В с.174-176; Ibid., Егоров В.С. с.36; Ibid., Г. Новоселов с.,68-69

[308] Ibid., Флетчер Дж.и Наумов А.В. с.191;

prettiesisko darbību vai bezdarbību un to radītājām laika ziņā sekojošajām kaitīgajām sekām, kurā darbība vai bezdarbība sagatavo un nosaka seku iestāšanās reālu iespēju un kurā darbība vai bezdarbība ir galvenais noteicošais faktors, kas neizbēgami radījis kaitīgas sekas."[309]

### 2.2. Objektīvo pusi raksturojošo darbību automatizētās datu apstrādes sistēmas kriminālatiesiskais novērtējums

Jebkura noziedzīgā nodarījuma pret informācijas sistēmas drošību objektīvo pusi veido: 1) personas aktīva, kaitīga un prettiesiska darbība, kas vērsta pret vienu vai vairākiem informācijas sistēmu drošības elementiem (konfidencialitāti, integritāti vai pieejamību); 2) kaitīgās sekas, kas var izpausties gan materiāla, morāla, politiska vai organizatoriska kaitējuma radīšanā; 3) cēloņsakarība, ka jebkura kaitīgā darbība, kas vērsta pret informācijas sistēmu drošību, likumsakarīgi un nepieciešami rada citu parādību.

Prettiesiskās darbības satura noteikšana noziedzīgos nodarījumos, kas saistīta ar ISD apdraudējumu, ir pietiekami komplicēta. Šo problēmu sarežģī šādi apstākļi: 1) nereti šie noziedzīgie nodarījumi tiek veikti no citas valsts teritorijas, kas, iespējams, pārstāv citu tiesību loku, citas juridiskās tradīcijas un citu kriminālatiesisko regulējumu vai, citiem vārdiem sakot, vietas, kur šādu darbību neatzīst par noziedzīgu nodarījumu; 2) darbība var tikt atzīta par patvaļīgu vai nelikumīgu tikai tajā gadījumā, ja sistēmas īpašnieks, tiesiskais valdītājs ir izstrādājis un ieviesis savā sistēmā ISD pasākumus. Ja šādu pasākumu nav, nav arī patvaļīgas darbības; 3) atzīt to vai citu darbību par patvaļīgu var tikai sistēmas īpašnieks vai tiesiskais valdītājs. Izņēmums attiecas tikai uz tādām valsts nozīmes informācijas sistēmām, kas tiek aizsargātas ar speciāliem valsts likumiem, jo tās apstrādā valstij un sabiedrībai izdzīvošanai nepieciešamu informāciju. Tāpēc, saistot šo problēmu ar noziedzīgiem nodarījumiem pret ISD, reizēm ir ļoti grūti nošķirt autorizētu darbību no neautorizētas, tas ir atkarīgs no katra noziedzīga nodarījuma veida, jo ļoti reti praksē būs gadījumi, kad tā vai cita darbība saistībā ar automatizēto datu apstrādes sistēmu ir aizliegta vai regulēta ar likumu. Taču bez iepriekšminētajiem faktoriem, kas apskatīti kā problēmu punkti darbības atzīšanai

---

[309] Turpat, Krastiņš U., 70-71.lpp.

par nelikumīgu automatizētās datu apstrādes sistēmās, vēl ir arī citi kritēriji, kas jāievēro šo darbību satura izvērtēšanā, pirms procesa virzītājs ierosina krimināllietu par konkrēta noziedzīga nodarījuma pret ISD izdarīšanu. Tas ir jautājums par apstākļiem, kad krimināLatbildība tiek izslēgta. ES ietvarlēmums par uzbrukumiem informācijas sistēmām noteic pienākumu dalībvalstīm paredzēt šādus krimināLatbildību izslēdzošus apstākļus: 1) vienkāršo lietotāju darbības, to skaitā viņu tiesības lietot šifrēšanu, lai aizsargātu savas komunikācijas un datus; 2) reversās inženierijas izmantošanu; 3) pārvaldnieku, kontrolieru un operatoru darbības sistēmā un tīklos; 4) gan pilnvarotu sistēmas darbinieku, gan ārpussistēmas pilnvarotu personu speciāli veiktas sistēmu drošību pārbaudes; 5) leģitīma zinātniskā pētniecība. Noziedzīgiem nodarījumiem pret ISD ir piemērojami šādi Krimināllikuma III nodaļas „Apstākļi, kas izslēdz krimināLatbildību" panti: 32. pantā paredzētā „galējā nepieciešamība" un 33.pantā paredzētais „attaisnojamais profesionālais risks". Neskatoties uz šādām prasībām, nav lietderīgi iepriekšminētos nosacījumus ietvert kā atsevišķu krimināllikuma panta daļu, bet katrs šī nosacījuma piemērošanas gadījums ir jārisina praksē atbilstoši konkrētiem apstākļiem. Iepriekšminētie apstākļi nav vienīgie, kas rada problēmu noteikt, kas ir atļauta darbība un kas ir patvaļība sistēmā. Šeit ļoti svarīgi ir izprast, ar ko tehniskā piekļuve sistēmas resursiem atšķiras no juridiskās kategorijas, tāpēc šie jautājumi plašāk aplūkoti turpinājumā.

Krimināllikuma 241.-244. pantā paredzētais nodarījums ir saistīts ar darbībām, ko pieņemts saukt par informācijas apriti, t.i.,piekļūšanu, ievadīšanu, kopēšanu, grozīšanu, pārraidīšanu, modificēšanu, iznīcināšanu un padarīšanu par nepieejamiem, saspiešanu u.c. Tās visas ir tehniskas darbības, taču ne vienmēr tehniska darbība rada krimināllikumā paredzētās sekas, pat tad ja tā ir notikusi. Teorijā un praksē jebkura objektīvās puses darbība ir jāizvērtē gan no tehniskā, gan juridiskā viedokļa, pretējā gadījumā var tikt pieļautas nopietnas kļūdas krimināllikuma piemērošanā un pat nevainīgu personu saukšanā pie atbildības. Tāpēc veikšu KL 241.- 245. panta dispozīcijā ietverto objektīvo darbību analīzi. Īpašu vērību pievērsīšu patvaļīgas piekļuves jēdzienam, jo faktiski patvaļīga piekļuve ir visu noziedzīgu nodarījumu pret informācijas sistēmu drošību pamats.

3. Darbības -patvaļīga piekļuve krimināltiesiskais raksturojums

Lai persona gūtu jebkādu iespēju izdarīt darbības informācijas sistēmā, vispirms tai jāpiekļūst sistēmas informācijas un tehniskajiem resursiem. Tādējādi patvaļīga, neautorizēta piekļuve informācijas sistēmu resursiem vienmēr ir saistīta ar zināmiem nosacījumiem, bez kuru iestāšanās tā nevar tikt realizēta, tas ir, vēršanās pret sistēmā noteikto piekļuves kārtību. Speciālisti izdala vairākas metodes, kā persona var realizēt patvaļīgu piekļuvi automatizētās datu apstrādes sistēmas (ADAS) resursiem, bet visbiežāk izmantotās ir šādas: 1) piekļuvi iegūst, izmantojot viltotus identifikatorus un pieejas kodus; 2) patvaļīga nepieskatītas datorsistēmas lietošana, kad tā lietotājs likumīgi ir pieslēdzies sistēmas resursiem, izmantojot savas piekļuves tiesības.[310]

2002. gadā tika pieņemtas ESAO vadlīnijas „Par informācijas sistēmu un tīklu drošību. Ceļā uz drošības kultūras veidošanu".[311] Dokumentā par vienu no galvenajiem informācijas sistēmu un tīklu drošības uzdevumiem izvirzīta nepieciešamība veicināt lietotāju uzticību informācijas sistēmām un tīkliem. Uzticamību var radīt tad, ja lietotājs būs pārliecināts, ka informācijas sistēmas lietošana ir droša, ka tā neapdraud viņa privāto dzīvi, ka neaizskar citas ar likumu aizsargātas intereses. Tāpēc katrai sistēmai ir nepieciešama sava piekļuves kārtība.

3.1.Piekļuves tehniskais raksturojums

1. Piekļuve [312]- lietotāja atļauja piekļuvei datoru tīklam, atsevišķam datoru tīkla serverim vai direktorijiem un datnēm, kas izvietotas datoru tīkla serveros. Piekļuvi tīkla resursiem konkrētam lietotājam atbilstoši vispārējai tīkla pārvaldības struktūrai piešķir tīkla administrators, pārraugs vai kādas daļas pārvaldnieks. Piekļuves kārtību parasti raksturo divi kritēriji: 1) identifikācija, ko raksturo konkrētai personai piešķirto individuāli lietojamo pazīšanās zīmju kopums (lietotāja vārds un parole). Identifikācija[313] ir lietotāja pazīšana pēc vārda un paroles. Šo darbību veic,

---

310 Investigation tool: Knowledge. Computer crime The U.N. Manual adapted by Editor Micheal J. O'Brien// http://www.mobrien.com/computer_crime.shtml#extent (aplūkots 2004.gada 20.februārī)

311 OECD Guidlines for the security of information systems and networks. Towards a culture of security

312 http://www.termini.lv/index.php?term=access%20rights&lang=EN&terms=accessability (aplūkots 2004.gada 23. martā)

313 http://www.termini.lv/index.php?term=lietotāja%20identifikācija&lang=LV&terms=identifikācija (aplūkots 2004.gada 23. martā)

lai pārbaudītu lietotāja tiesības piekļūt datiem un izvēlēties to izmantošanas režīmu; 2) autentifikācija[314] ir lietotāja atpazīšanas process, kura gaitā noskaidro, vai lietotājs ir pilnvarots lietot datus, programmas, ierīces, kā arī noteiktus sistēmas darbības režīmus. Autentifikācijai[315] ir jāatbild uz jautājumiem: 1) kas jūs pazīst? 2) kas jūs esat? 3) kas jums ir? Šai piekļuves kārtībai ir jābūt viegli lietojamai un veidotai proporcionāli iespējamai apdraudējuma pakāpei. Autori M. Baids (*M. Bide*) un T. Hings (*T.Hing*) analizējot, šo problēmu, izvirza šādus piekļuves kārtības nosacījumus: 1) identifikācijas sistēmai ir jāaptver visi informācijas aprites ķēdes locekļi; 2) tai jābūt vienkāršai un lietotājam saprotamai, un tā nedrīkst saturēt nereālas prasības; 3) tai jābūt pienācīgi drošai ( vienmēr jāpatur prātā, ka augstāka drošība prasa lielākus izdevumus); 4) tā ir jāiegaumē, ņemot vērā starpnieku lomu informācijas aprites ķēdē; 5) izstrādājot piekļuves sistēmu, jāpatur prātā, lietotāju dažādās nozīmes un to iespējamās maiņas; 6) jāņem vērā arī tas, ka lietotājs vienlaicīgi var izmantot vairākus informācijas resursus, piem., biroju, vārdnīcu, interneta pārlūkprogrammu, bibliotēku, arhīvu u.c.; 7) tai jābūt neitrālai piemērošanā.[316]

### 3.2. Piekļuves jēdziens un to saistītās juridiskās problēmas

Piekļuves kārtību noteic informācijas sistēmas īpašnieks vai resursu turētājs, piešķirot katram sistēmas lietotājam noteiktu tiesību apjomu izmantot sistēmā esošos resursus. Līdz ar to jebkura persona, kurai sistēmas īpašnieks vai resursu turētājs tehniski ir piešķīris paroli un identifikācijas kodus, kļūst par sistēmas lietotāju ar noteiktu tiesību apjomu. No tā brīža personai rodas tiesības piekļūt sistēmas resursiem, izmantot sistēmas sniegtos pakalpojumus, respektīvi, veikt darbības, kas rada noteiktas juridiskās sekas. Taču kā jebkuras tiesības tās satur arī sistēmas īpašnieka vai pilnvarotās personas subjektīvo viedokli, sevišķi tad, ja piekļuves tiesību piešķiršana notiek uz līguma vai citu savstarpēju attiecību pamata.

Šajā tiesību apjomā parasti ietilpst:

---

314 http://www.termini.lv/index.php?term=lietotāja%20autentifikācija&lang=LV&terms=autentifikācija (aplūkots 2004.gada 23.martā)

315 Greenberg Eric Mission critical Security Planner. Creating Customised strategies.Indianapolis- Willey Publishing Inc., 2003., p.40

316 User identification and authentification a brief introduction February 1998 by Mark Bide and Trevor Hing. Book industry Communication & EditEUR .p. 5

1. Lietotājam piešķirtie viņa personību tehniski raksturojošie identifikatori (lietotāja vārds, personīgais atpazīšanas kods (PIN), parole, viedkartes u.c.) To sarežģītības pakāpe ir atkarīga no sistēmā esošās informācijas klasifikācijas pakāpes. Ja sistēmā tiek apstrādāta konfidenciāla informācija, tad personai piešķirtie identifikatori ir stingrāki, ja sistēma neapstrādā tādu informāciju, kuras atklāšana vai sabojāšana var radīt draudus citiem lietotājiem, tad piešķirtie identifikatori ir primitīvāki. Lietotājam piešķirtie identifikatori ir nepieciešami, lai viņu atpazītu sistēmas loģiskās aizsardzības sistēmas un sniegtu piekļuvi.

2. Šajā tiesību apjomā ietilpst arī lietotājam deleģētās tiesības izmantot sistēmā esošos resursus, ievadīt jaunu informāciju apstrādāt to, īstenot piekļuvi konkrētiem informācijas apgabaliem u.c. A. Adamskis (*Andrzej Adamski*) šo tiesību saturā ietver šādas lietotāja tiesības: 1) zināt, ka viņam nepieciešama informācija sistēmā glabājas; 2) zināt, kas tā ir par informāciju; 3) tiesības brīvi rīkoties ar šo informāciju, labot to, grozīt, izdzēst; 4) šo tiesību pārkāpumu gadījumā ar juridiskiem līdzekļiem prasīt savu tiesību aizsardzību.[317] Autors pilnīgi piekrīt šādam viedoklim. Taču lietotājam nav tiesību ievadīt sistēmā jaunu datorprogrammu vai citu ierīci bez sistēmas administratora vai īpašnieka piekrišanas. Piemēram, izmantojot tiesu informācijas sistēmu, lietotājam nav tiesību ielādēt datorā jaunu programmatūru bez sistēmas administratora piekrišanas. Sistēmas administrators vispirms izvērtē jaunā resursa riska pakāpi un veic nepieciešamās darbības tā instalēšanai vai arī noraida šo lūgumu. Faktiski šādai kārtībai vajadzētu būt izveidotai katrā valsts un pašvaldību informācijas sistēmā, jo nereti tieši iespēja, ka vienkāršs lietotājs savā darba datorā var ielādēt jebkuru datorprogrammu, ir cēlonis, ka sistēmā tādā veidā var tikt ievadītas kaitīgas ierīces, kas var pārkonfigurēt sistēmas resursus, un tie var pilnīgi vai daļēji kļūt atkarīgi no trešās personas ietekmes.

3. Kā minēts iepriekš, tad piekļuves tiesību piešķiršana ir ne tikai tehnisks, bet arī subjektīvs akts, kas izteic attiecīgās sistēmas īpašnieka gribu. Viņš tās var

---

317 Information management: Legal and security issues by Andrzej Adamski// http://www.uncjin.org/Other/korebo/chapter5.pdf (aplūkots 2004.gada 23. martā)

piešķirt un var arī nepiešķirt. Viņš var darbību atzīt par patvaļīgu un var arī to attaisnot.

4. Piekļuves tiesību saturā ietilpst arī citi parametri, piemēram, tiesības informācijas piekļuvei tad, kad tā ir nepieciešama lietotājam, taču šī pazīme nevar ietekmēt to pazīmju kopumu, kas nepieciešams, lai konstruētu noziedzīgā nodarījuma – patvaļīga piekļuve informācijas sistēmām- dispozīciju.

Definējot patvaļīgās piekļuves nosacījumus, likumdevējam nepieciešams vadīties no lietotājam piešķirto tiesību apjoma. Šis tiesību saturs sevī ietver: 1) tiesības reģistrēties kā ADAS lietotājam, izmantojot sev piešķirtos identifikatorus. Šīs tiesības vēl nekādā gadījumā nedod pilnīgas pieejas tiesības visiem sistēmas resursiem; 2) tiesības pēc reģistrēšanās sistēmā iegūt pieeju un izmantot tikai tos ADAS resursus, kurus tiem atļāvis lietot sistēmas īpašnieks vai viņa pilnvarotā persona; 3) lietot šos resursus likumīgs lietotājs var tikai tādā veidā un kārtībā, kā to pilnvarojis sistēmas īpašnieks vai viņa pilnvarotā persona.

Piemēram, atbildīgai personai par informācijas sistēmu drošību piešķirot piekļuves tiesības, jāņem vērā, kādam nolūkam lietotājam šāda piekļuve nepieciešama. Vai lietotājs ir sistēmas darbinieks un informācija viņam nepieciešama sakarā ar darba pienākumu pildīšanu vai arī citiem nolūkiem? ASV Datordrošības institūts 2003. gadā aptaujāja 350 ASV kompānijas.[318] 45% aptaujāto atzina, ka viņu sistēmu resursiem nelikumīgu piekļuvi bija realizējuši paši sistēmas darbinieki. Šādu iebrukumu skaits pārsniedz pat no 11- 30%. Galvenokārt šie apdraudējumi ir saistīti ar to, ka sistēmas lietotāji patvaļīgi piekļūst tiem informācijas resursiem, kuru lietošanu neparedz piešķirtās tiesības. Minētais pierāda, cik svarīgi ir, konstruējot šo noziedzīgā nodarījuma sastāvu, ņemt vērā, lai panta dispozīcija aptvertu arī tādus gadījumus, kad personai ir garantēta likumīga piekļuve, bet tā pārkāpj pieejamās informācijas robežas.

Izstrādājot krimināllikuma normas par patvaļīgu piekļūšanu informācijas sistēmu resursiem, pasaulē ir sastopama dažāda pieeja. Šī pieeja ir atkarīga no tā, ko mēs uzskatām par patvaļīgu piekļuvi informācijas sistēmai. Dž. Vašingtona universitātes

---

[318] 2003 CSI/FBI Computer Crime and Security Survey p.2

profesors O. Kers (*Orin S. Kerr*) norāda, ka patvaļīga piekļuve datorsistēmām ir jauns jēdziens un satur daudz noslēpumaina.[319] Jāpiekrīt O. Keram, kaut arī šobrīd pasaulē krimināltiesību zinātnē daudz zinātnieku pievēršas kibernoziegumu problēmām, līdz šim nav izdevies atrast darbu, kurā nopietni analizēti piekļuves un patvaļīgas piekļuves juridiskie aspekti. Piemēram, komentējot Krimināllikuma 241. pantu, profesore V. Liholaja norāda, ka nodarījuma objektīvo pusi veido darbība- patvaļīga piekļūšana automatizētai datorsistēmai.[320] Komentārs nedod patvaļīgas piekļuves skaidrojumu, aprobežojoties ar to, ka nodarījuma sastāvs ir formāls, jo tas ir pabeigts ar panta dispozīcijā norādīto darbību pabeigšanu. Līdzīgu viedokli komentāros izsaka arī Krievijas Federācijas krimināLkodeksa komentāru un mācību grāmatu autori[321], aprobežojoties tikai ar norādi, ka piekļuve ir nelikumīga tad, ja personai nav noteiktas piekļuves tiesības. Līdzīgs viedoklis ir pausts arī citu autoru[322] darbos, kas veltīti kibernoziegumu pētniecības problēmām. Tomēr autors uzskata, ka, neatklājot jēdziena „patvaļīga piekļuve" juridisko saturu, nav iespējams arī konstruēt šo noziedzīgā nodarījuma sastāvu. Jo ne vienmēr patvaļīga piekļuve, ko Liholaja V. raksturo kā formālu noziedzīgu nodarījumu, būs noziedzīgs nodarījums. Autors uzskata, ka nav pareizi noziedzīgus nodarījumus pret informāciju sistēmu drošību atzīt par formāliem nodarījumiem. Šo problēmu autors iztirzāja, analizējot Krimināllikuma 241. panta 1. daļā paredzēto noziedzīgā nodarījuma sastāvu. Patvaļīgā piekļuve ne vienmēr ir krimināli sodāms nodarījums. Šādas darbības var tikt atzītas arī par civiltiesisku pārkāpumu vai arī var tikt attaisnotas pilnībā.

Piemērs. A noslēdz līgumu ar N par informācijas drošības programmatūras uzstādīšanu. Līgumā paredzēts, ka A nodrošina antivīrusu programmas regulāru modernizēšanu N vajadzībām. Līguma

---

319 Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes by Orin S. Kerr. // New york University law review . Vol. 78 (2003) Nr. 5 November, p. 1596

320 Krastiņš U., Liholaja V., Niedre A. Krimināllikuma zinātniski- praktiskais komentārs 3. sevišķā daļa U. Krastiņa redakcijā. , Rīga : AFS, 2003. 226.- 227. lpp.

321 Коментарый к уголовному кодексу Росийской федерации. Издание 3-е измененное и дополненное. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва- издательская группа Инфра · М- Норма,2000., с. 696-697.; Уголовное право Российской федерации. Особенная часть. Под. ред. Б.В. Здравомыслова. Москва-Юристь, 1999. с.353-354; Росийское уголовное право. Особенная ч. Учебник. Под. Ред. М.П. Журавлева и С.М. Никулина. Москва- Спарк, 1998, с.418.

322 Brenner Susan W. Is There Such a Thing as "Virtual Crime?", 4 Cal. Criminal Law. Rev. 1 (2001)"; Cyber Attacks during the war on terrorism: Predictive analysis. Institute for security technology studies at Dartmouth college, September 2001., p.11; Ibid., Волеводз А.Г. с.62-64 , u. c.

nosacījumi paredz arī samaksas kārtību par sniegtajiem pakalpojumiem. N sākotnēji pilda līguma noteikumus, maksā par izpildītiem darbiem, bet vēlāk izvairās no saistību izpildes. Firma, zinot piekļuves kodus, īsteno piekļuvi klienta sistēmas resursiem un bloķē sev piederošās programmatūras lietošanu. Izvērtējot piemērā minētās darbības, jāatzīst, ka šeit ir saskatāmas KL 241. panta paredzētā nodarījuma pazīmes, jo piekļuve notikusi bez sistēmas īpašnieka ziņas un trešā persona ir iepazinusies ar informācijas resursiem un tos daļēji iznīcinājusi. Taču šajā gadījumā policija nevarēja ierosināt krimināllietu tāpēc, ka programmatūras iegādāšanās nav pabeigta. Līdz ar to patvaļīga piekļuve ir saistīta ar citu tiesiski noslēgta līguma patvaļīgu nepildīšanu. Tāpēc šeit pastāv jautājums -kam tiesiski pieder sistēmas resursi?

Tādējādi ne katra patvaļīga piekļuve var tikt atzīta par noziedzīga nodarījuma elementu, jo, neizvērtējot patvaļīgās piekļuves saturu, to nevar norobežot no civiltiesiskās atbildības.

Piemērs. Kāds Latvijas Republikas valdības ministrs uzdeva savam darbiniekam veikt patvaļīgu ielaušanos ministrijas pakļautībā esošās struktūrvienības informācijas sistēmā, lai pārliecinātos, cik droši tā ir aizsargāta. Darbinieki atklāja patvaļīgo piekļuves faktu un par to ziņoja attiecīgām amatpersonām. No spēkā esošās KL 241. panta dispozīcijas viedokļa šo personu, kas realizēja patvaļīgu piekļuvi bez attiecīgi piešķirtām pilnvarām, bija pamats saukt pie krimināatbildības. Taču, protams, ka tas netika darīts, jo persona izpildīja augstākstāvošas amatpersonas rīkojumu.

Analizējot šo piemēru, nepieciešams vērst uzmanību uz personas, kas realizē patvaļīgu piekļuvi, nodomu. Ne velti kibernoziegumu eksperti diskutējot par Kibernoziegumu konvencijā ietvertā 2. panta „nelikumīga piekļuve" saturu, izvirzīja prasību šo atbildību saistīt ar nosacījumiem, ka patvaļīgā piekļuve veikta negodīgos nolūkos vai mantkārīgu tieksmju dēļ u.c.. Turpinājumā autors analizēs arī atbildību izslēdzošus apstākļus, un šajā piemērā aprakstītās darbības pilnīgi atbildīs šiem apstākļiem.

### 3.3. Patvaļīgās piekļuves jēdziens salīdzinošo tiesību aspektā

ASV tiesu praksē arī nav vienota viedokļa, ko atzīt par patvaļīgu piekļuvi,[323] īpaši asi tajā izvirzās diskusija par civiltiesisko un krimināltiesisko patvaļību. O. Kers izvirza tēzi, ka aprakstot patvaļīgas piekļuves jēdzienu, nepieciešams nodalīt tās piekļuves tiesības, kas noteiktas līgumā starp sistēmas īpašnieku un lietotāju no tām, kas noteiktas likumā.

Pretējs viedoklis pausts ES paskaidrojošā memorandā priekšlikumi „Par ietvarlēmuma par uzbrukumiem informācijas sistēmām piemērošanas kārtību". Memoranda 2.f. punktā dots autorizētas (pilnvarotas) personas jēdziens: „ Tā ir jebkura persona, kurai ir likumā vai līgumā vai citā tiesiski nostiprinātā formā

---

[323] Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes by Orin S. Kerr. // New York University law review. Vol. 78 (2003) Nr. 5 November, p. 1596

piešķirtas tiesības lietot, pārzināt, kontrolēt, pārbaudīt, nodarboties ar likumīgu zinātnisku pētniecību vai citā veidā tiesiski rīkoties ar informācijas sistēmas resursiem."[324] Autors pilnīgi atbalsta šādu viedokli, jo sistēmas īpašnieks, valdītājs vai tā pilnvarotā persona piešķir piekļuves tiesības konkrētam lietotājam. Tās var būt balstītas gan uz komercdarbības līgumu, gan arī uz likumu, gan arī uz citiem nosacījumiem. Galvenais ir tas, ka piekļuves tiesības dod lietotājam iespēju likumīgi izmantot sistēmas resursus.

Tomēr diskusijas vērts ir jautājums, vai piekļuves (*access*) jēdziens ir saistīts ar reālo vai virtuālo vidi. O. Kers savā rakstā norāda, ka tieši šis apstāklis rada neskaidrības ASV tiesu praksē. ASV štatu normatīvajos aktos arī nav vienotas izpratnes par to, kas ir patvaļīga (neautorizēta) pieeja.

Piemērs. Kanzasas štata likumu kopojumā patvaļīgā piekļuve ir iekļauta 21. sadaļas II. daļā, kur apkopoti noziedzīgi nodarījumi pret īpašumu. Minētā likuma 37. pantā dota piekļuves (*access)* definīcija. Piekļuve- datoram, datorsistēmai vai datortīkliem definēta kā tuvošanās vai instrukcija par to kā komunicēties, ievadīt, atgūt datus vai citādā veidā lietot datorsistēmas resursus. Līdzīga pieeja ir arī Mičigānas štata datornoziegumu likuma 752., 797. pantā, Floridas štata 815. sadaļas 10.p., Arizonas štata 13. 2301. p. u.c.)

Pētot šo problēmu, O. Kers konstatēja, ka minēto štatu likumi satur tādu piekļuves jēdzienu, kas attiecināms uz reālo vidi. Neskaidrību šajā jomā rada normatīvajos aktos lietotais vārds *approach*, ko latviski var tulkot gan kā tuvošanos, gan arī pieeju. Spriežot pēc Krimināllikuma 241. panta 1. daļas dispozīcijas, arī likumdevējs īsti nav izpratis patvaļīgas piekļuves jēdzienu.

Piemērs. Kanzasas štata Augstākā tiesa krimināllietā *Štats pret Alenu* atzina, ka šāda piekļuves definīcija ir pārāk plaša un tās piemērošana var radīt konstitucionālas problēmas, jo pēc šīs definīcijas par patvaļīgu piekļuvi var atzīt arī jebkuru gadījumu, kad persona fiziski, patvaļīgi atrodas datorsistēmas tuvumā.[325] Tiesa, izskatot šo lietu, atteicās spriedumā izmantot štata likumā ietverto piekļuves jēdzienu, kurš kā redzams ir sarežģīts un pat pretrunīgs, bet vadījās no ASV sabiedrībā plaši pazīstamās Vebstera vārdnīcā ietvertās piekļuves definīcijas[326], ka„.. *pieeja ir uzskatāma kā brīvība kaut ko iegūt vai lietot*".
Attaisnojot personu par patvaļīgas piekļuves mēģinājumu, tiesa norādīja, ka termins „piekļuve" ir jāattiecina uz virtuālo vidi un tāpēc persona var tikt atzīta tikai par vainīgu tad, ja cietušās sistēmas īpašnieks vai nomnieks ir izstrādājis tādu pasākumu kompleksu, kas atļauj sistēmas resursiem piekļuvi ar personas lietotājvārdu un paroli un nepareizu identifikatoru lietošana noliedz piekļuvi sistēmas resursiem.

---

[324] Proposal for a Council framework decision on attacks against information systems. Explanatory memorandum Brussels COM (2002) 173 Final 19.04.2002 2002/0086 (CNS)

[325] Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes by Orin S. Kerr. // New york University law review . Vol. 78 (2003) Nr. 5 November, p. 1596

[326] Webster dictionary http://www.m-w.com/cgi-bin/dictionary (aplūkots 2004.gada 23. martā)

Autors uzskata, ka par patvaļīgu piekļuvi sistēmas resursiem var runāt tikai tad: 1) ja sistēmā ir noteikta likumīga piekļuves kārtība; 2) ja piekļuve nav saistīta ar fizisku piekļūšanu sistēmas resursiem, respektīvi, tā ir veikta no attāluma. Līdz ar to Kanzasas Augstākās tiesas precedentam ir ļoti liela nozīme, gan piemērojot likumu līdzīgos gadījumos, gan arī veicot teorētisko izpēti par patvaļīgas piekļuves juridiskajiem aspektiem ne tikai ASV, bet arī citu valstu krimināltiesībās.

Iepazīstoties ar citu ASV štatu likumiem datornoziegumu jomā, jāsecina, ka daļa štatu, piemēram, Konektikuta (53a-250)[327], Delavara (11-931)[328], savas "piekļuves" definīcijas ir izstrādājušas analogi Mičigānai un Floridai, norādot, ka piekļuve ir instrukcija, par to kā komunicēties un izmantot sistēmu resursus. Šī definīcija parāda, ka piekļuve kā process patiesībā ir balstīta uz tehnoloģiski noteiktiem risinājumiem, instrukcijām, kuru pārkāpšanas gadījumā jebkura darbība ar sistēmas resursiem atzīstama par neatļautu jeb patvaļīgu.

Šādu viedokli praksē ieviesuši daži ASV štati, piemēram, Kolorado (18-5. 5-101), Havaja ((708-890), kas likumos ir definējuši terminu patvaļīgs (neautorizēts). Tas nozīmē piekļūšanu datoram, datorsistēmai vai datortīklam bez īpašnieka atļaujas vai pārsniedzot īpašnieka vai nomnieka atļaujā noteiktās robežas. Indiānas štata krimināllikuma 716 A 3. pants par patvaļīgu piekļuvi atzīst tīšu personas darbību, kas bez attiecīga pilnvarojuma piekļūst informācijas sistēmai. Ar šo darbību persona ir izdarījusi vienkāršu likumpārkāpumu.[329]

O. Kers patvaļīgas piekļuves lietas iedala trīs kategorijās: 1) patvaļīgā piekļuve tiek realizēta, izmantojot speciālas datorprogrammas; 2) to veic darbinieki, kas lieto sistēmas resursus pretēji sistēmas īpašnieka interesēm; 3) tā saistīta ar līgumattiecībām starp sistēmas īpašnieku un lietotāju.

1. Patvaļīgā piekļuve izmantojot speciālas datorprogrammas

Viens no raksturīgākajiem piemēriem ir kriminālllieta Savienotās Valstis pret Robertu Tappanu Morisu (*United States v Morriss*),[330] kur persona tika saukta pie atbildības par pirmā datortārpa

---

327 Connecticut General Assembly http://search.cga.state.ct.us/ (aplūkots 2004.gada 14. martā)

328 Computer crime statutes state by state// http://www.onlinesecurity.com/links/links683.php (aplūkots 2004.gada 14. martā)

329 State computer crime statutes citations// http://www.crime-research.org/library/State.pdf (aplūkots 2004.gada 23. martā)

330 United States v Moriss http://www.law.uoregon.edu/faculty/kaoki/site/secure/cases/unauthorized/us_v_morris.php (aplūkots 2004.gada 23. martā)

izgudrošanu, kas tika palaists internetā un nodarīja kaitējumu vairākām federālās nozīmes datorsistēmām.
Moriss tika apsūdzēts un notiesāts par tīšu, patvaļīgu piekļuvi federālās nozīmes informācijas sistēmām. Apelācijas sūdzībā viņš rakstīja, ka nav piekļuvis neautorizēti federālās nozīmes datorsistēmām, jo viņam kā datordrošības ekspertam bija tiesības piekļūt vairākām no tām un bija tiesības piekļūt arī internetam un sūtīt e- pastu.
R. Moriss norāda, ka ir pārkāpis tikai autorizācijas kārtību. Apelācijas tiesa noraidīja viņa argumentus. Tiesa savu viedokli motivēja ar to, ka Moriss patvaļīgo piekļuvi datorsistēmām realizēja, izmantojot, ierīces drošībai vārīgās vietas, iekļuva sistēmā, kā to nevēlējās sistēmas īpašnieks. Šobrīd šādu piekļuves metodi saista ar datorsistēmu loģiskās drošības sistēmas pārvarēšanu vai apiešanu.

2. Patvaļīgas piekļuves gadījumi, kad to veic sistēmas darbinieki, kas lieto sistēmas resursus pretēji sistēmas īpašnieka interesēm.

Šādi gadījumi, kad sistēmas darbinieks nokopē sava īpašnieka klientu datu bāzi un nodot to konkurentiem par samaksu, ir bijusi arī Latvijā. Taču diezin vai tiesa par patvaļīgu piekļuvi atzīs jebkuru faktu, kad darbinieks lieto datorsistēmas resursus pretēji darba devēja interesēm, piemēram, spēlējot datorspēles, pļāpājot internetā u.c. Piemēram, P. Grabovskis (*P. Grabovsky*) šādas darbības, kad sistēmas darbinieki patvaļīgi izmanto sistēmas resursus mērķiem, kas nav saistīti ar darba pienākumu pildīšanu pēc nozīmes, nosauc par datorkrāpšanas paveidu -laika zādzību (*time theft*).[331] Zināmā mērā šīs darbības arī ir saistītas ar patvaļīgu piekļuvi ADAS resursiem un šo resursu izmantošanu ne pēc nozīmes. Taču tāda patvaļīgas piekļuves definīcija, ietverot tajā arī patvaļīgu pakalpojumu saņemšanu, būtu pārāk plaša un varētu radīt problēmas tās piemērošanā.

Jāpiekrīt O. Keram, ka patvaļīgas piekļuves jēdzienā nav jāiekļauj darbinieku pārraidāmās informācijas satura kontrole un citi kritēriji, kas varētu radīt konkrētas juridiskās sekas. Tomēr ļoti svarīgi jebkuram sistēmas īpašniekam saprast, ka šos apdraudējumus var novērst tikai precīzi izstrādāti darbinieku darba apraksti, to skaitā arī pilnvaras ko darbinieks drīkst darīt sistēmā un ko nedrīkst.

3. Līgumtiesību pārkāpumi, kuru rezultātā pieļauta patvaļīga informācijas sistēmu resursu lietošana.

Piemēram, noslēdzot līgumu, puses apņemas neizpaust citām personām izmantojamās datu apstrādes sistēmas tehnisko un finansiālo informāciju, un šīs informācijas izpaušana uzskatāma par patvaļīgu piekļuvi sistēmas resursiem. Taču viena no pusēm izmantojot speciālu programmu, piekļūst partnera sistēmas resursiem un iegūst no tā tādu informāciju, kas dod viņiem priekšrocības komercdarbības attīstībā. Šādi gadījumi ir fiksēti arī Latvijā.

---

331 Gragovsky P., Smith R., Dempsey R. Electronic theft Unlawful Acquisition in cyberspace.- Cambridge University press, 2001., p. 63

Kā minēts iepriekš, tad ASV nav vienotas izpratnes par to, kas atzīstams par patvaļīgu piekļuvi, jo katra ASV štata likumdevēji ir suverēni savā izvēlē, izņemot gadījumus, ja tas skar ASV Konstitūcijā noteikto tiesību piemērošanu. Tāpēc nedaudz pieskarsimies atspēkojošās prezumpcijas (*rebuttable presumption*) un apstiprinošās aizstāvības (*affirmative defense*) piemērošanas aspektiem, nosakot atbildību par patvaļīgu ASV krimināltiesībās. V. Lafave (*Wayne R. LaFave*) atspēkojošo prezumpciju raksturo kā aizstāvības tiesību iesniegt atspēkojošus pierādījumus, un tiesai tie ir jāņem vērā.[332] Protams, no šāda viedokļa atspēkojošā prezumpcija mūsu izpratnē ir Latvijas KPK $19^1$. pantā noteiktā nevainības prezumpcija, kas noteic tiesas pienākumu vērtēt visus pierādījumus un jebkuras šaubas tulkot par labu tiesājamam. Taču zīmīgi ir tas, ka dažos štatos likumdevējs pašā likumā, kas paredz atbildību par patvaļīgu piekļuvi, ir definējis gadījumus, kad šādi procesuālie instrumenti ir izmantojami.

Piemērs. Ilinoisas štata likumu kopojuma 720. sadaļas 5/16D-7 pants noteic, ka gadījumā kad persona piekļūst vai var īstenot piekļuvi sistēmas resursiem, kur pieejamību nodrošina speciāls slepens kods vai īpašnieka kods, bet kura piešķiršanu nav veikusi šim nolūkam pilnvarota persona, var izmantot atspēkojošo prezumpciju, ja piekļuve sistēmas resursiem veikta patvaļīgi bez īpašnieka piekrišanas vai pārsniedzot pilnvarojuma robežas.
Precīzāk šī atspēkojošās prezumpcijas būtība izteikta Konektikutas štata krimināllikumā. Minētā likuma 53a- 251. pantā par patvaļīga piekļuvi datorsistēmai ir atzīstama darbība: 1) ja persona skaidri zina, ka tai nav atļauja piekļūt sistēmai; 2) apsūdzot par patvaļīgu piekļuvi, var tikt piemērota apstiprinošā aizstāvība[333] (*affirmative defence*) , ja
a) persona pamatoti tic, ka sistēmas īpašnieks vai cita pilnvarotā persona, kam tiesības piešķirt piekļuves tiesības, ir atļāvusi viņam šo pieeju;
b) personai ir pamats ticēt, ka sistēmas īpašnieks vai tā pilnvarotā persona var viņam piešķirt atļauju bez samaksas;
c) persona pamatoti var nezināt, ka piekļuve ir patvaļīga.[334]

Faktiski tas nozīmē to, ka pastāvot piemērā minētajiem apstākļiem, persona var tikt atbrīvota no kriminālatbildības. No tehniskā viedokļa šādu atspēkojošo argumentu piemērošana patvaļīgas piekļuves attaisnošanai nav iespējama. Piekļuves tiesības sistēmu resursiem var piešķirt tikai sistēmas īpašnieks vai viņa pilnvarotā persona. Šīs tiesības piešķir jau iepriekš, vai nu personai nosūtot

---

332 Criminal law Fourth edition. Wayne R.LaFave. Hornbook Series.Thompson West, 2003., p. 67

333 Vispārējās tiesības pieņemts princips, ka apsūdzētais atsaucoties uz viņam izvirzītām apsūdzībām izvirza apgalvojumus, kas ir pretrunā apsūdzībai un kas balstās uz vispārīgiem tiesību principiem Sk. Law com.http://dictionary.law.com/definition2.asp?selected=2363&bold=||| (aplūkots 2004.gada 24. martā)

334 Cybercrime & Security Comp. &ed.by Alan E. Brill. Oceana Publications, Inc. Dobbs Ferry, Ny issued September 1998.booklet VI.I-I6

reģistrācijas pieteikumu sistēmas īpašniekam, vai arī sistēmas īpašnieks sakarā ar darba tiesiskām attiecībām. Tādējādi persona var identificēties sistēmā tikai tad, ja viņam šim nolūkam iepriekš ir piešķirta parole, lietotāja vārds un, iespējams, vēl citi identifikatori. Ja personai šo identifikatoru nav, tad sistēmas resursi viņu neautorizēs kā likumīgu lietotāju. Tas ir pilnīgi saprotami, jo lielākā daļa ADAS savu lietotāju uzskaiti un to autorizāciju veic automātiski. Ja iepriekš personai nav piešķirts lietotāja vārds un parole, sistēmas resursi to vienkārši neatpazīs kā lietotāju, kam ir piešķirtas zināmas tiesības lietot sistēmas resursus.

Taču no juridiskā viedokļa šāda apgalvojumu esamība, protams, var radīt zināmas sekas, jo piekļuves tiesību piešķiršana ir ekskluzīva ADAS īpašnieka vai tā pilnvarotās personas tiesība. Līdz ar to nekādā gadījumā nevar izslēgt šo subjektīvo faktoru, ka incidenta gadījuma šādu tiesību esamību, kaut arī tās nav piešķirtas tehniski, juridiski atzīst sistēmas īpašnieks.

Viena no mūsdienu krimināltiesību attīstības tendencēm ir tāda, ka jāpalielina to nodarījumu skaits, par kuriem valsts iestājas personu aizskarto interešu aizsardzībā tikai pēc cietušā iesniegtās sūdzības. Tā kā patvaļīgā piekļuves saturs sastāv gan no tehniskiem, gan tīri subjektīviem faktoriem, tad vairāki tiesību zinātnieki, piem., profesors U. Zībers (*U. Sieber*)[335], H. Lipsons (*H. F. Lipson*)[336], P. Lavrensa (*Patti Lawrence*)[337] u. c. uzskata, ka patvaļīgas piekļuves lietas jāierosina tikai pēc cietušā sūdzības. Autors pilnīgi atbalsta šādu viedokli, jo šāda nostāja atbilst arī EP Ministru komitejas Rekomendācijas Nr. R (87)18 *„Par dalībvalstu krimināl ās justīcijas vienkāršošanu"* 1.5. punkta saturam un Rekomendācijas Nr. R (85)11 „Par *cietušā stāvokli krimināltiesību un kriminālprocesa ietvaros"* 1.B 5. punktam, ka".. lēmumu par kriminālvajāšanas uzsākšanu pret noziedznieku vajadzētu pieņemt, iepriekš pienācīgi apsverot jautājumu par kompensāciju cietušajam, ieskaitot visus nopietnos noziedznieka pūliņus šajā sakarībā"[338], kā arī izmantot

---

335 Sieber U. Computer crime and Criminal information law. New trends in the international risk and information society. Updated and extended version of an article in the German language published in Computer und Recht (CR) 1995, pp. 100

336 Tracking and tracking cyber- attacks: Technical challenges and global policy issues. CERT coordination center, November 2002..p.3.,

337 Acceptable use. Whose responsibility is it? By Patti Lawrence// SANS Institute 2002., p.7

338 Eiropas Padomes informācijas biroja mājas lapa http://www.coecidriga.lv/tulkojumi/R(87)18.htm (aplūkots 2004.gada 24.martā)

tiesvedības atteikšanas principu uz plaši izplatītiem nodarījumiem, ievērojot katra nodarījuma raksturu un kaitīgumu. Tādā veidā valsts tiktu atbrīvota no nepieciešamības tērēt dārgus resursus, organizējot kriminālvajāšanu, ja cietušais var panākt ar vainojamo personu izlīgumu. Tā ir katras nacionālas valsts tiesība noteikt gan konkrētā nodarījuma sastāvu, gan arī procesuālo kārtību. Latvijas Kriminālprocesa kodeksa 111. panta 2. daļa paredz, ka bez cietušā sūdzības nevar ierosināt krimināllietas par Krimināllikuma 130., 156., 157., un 158. pantā paredzētajiem nodarījumiem. Autors uzskata, ka šim sarakstam būtu lietderīgi arī pievienot Krimināllikuma 241. pantu.

Viens no svarīgākajiem nosacījumiem kibertelpas regulējuma sakārtošanā ir likumības jeb *mutantis mutandis* principa piemērošana. Citiem vārdiem sakot, likumdevējam, nosakot ierobežojumus un aizliegumus, tiesību akti ir jāizstrādā tā, lai tie ar vienādu spēku darbotos jebkurā vidē, tai skaitā arī kibertelpā. Praksē tas nozīmētu to, ka, kriminalizējot patvaļīgu piekļuvi atbildībai jābūt līdzvērtīgai Krimināllikuma 175. panta 3. daļā paredzētam nodarījumam. Taču zinot to, ka Krimināllikums paredz ļoti bargu sodu par šo nodarījumu, autors uzskata, ka šis vienādais spēks ir jāattiecina uz to, lai identiska darbība reālā vidē un kibertelpā tiktu atzīta par noziedzīgu nodarījumu.

*Eiropas valstu pieeja patvaļīgas piekļuves krimināltiesiskā regulējumā noteikšanā*

Pasaulē kriminalizējot patvaļīgu piekļuvi, ir vērojamas šādas tendences:

1. Daļa valstu, piemēram, Izraēla[339], Islande (KL 288. p.1.d.), Beļģija (KL 550 (b) 1.p.) Bulgārija (KL 319.p.1.p.), Honkonga (Dekrēts par telekomunikācijām 27.A.1.p.), Portugāle[340], Venecuēla[341], paredz krimināl atbildību par tā saucamo "tīro" patvaļīgo piekļuvi. Šajās valstīs par noziedzīgu nodarījumu tiek atzīts jebkurš gadījums, kad persona realizē patvaļīgu piekļuvi informācijas sistēmai, neatkarīgi no piekļuves mērķa un līdzekļiem.

---

339 Israel Computers Law of 1995 [b.i.]

340 Portugal Criminal information law of August 17 1991 Ch.1. Ar.7 [b.i.]

341 Venecuela Special statute against computer related crimes Title II. Art. 6[b.g.] [b.i.]

Piemēram, A., zinot, ka sistēma nav aizsargāta ar loģiskās aizsardzības līdzekļiem, patvaļīgi pieslēdzas sistēmas resursiem. Šajā procesā viņš nepārvar ne sistēmas aizsardzības līdzekļus ne arī iepazīstas ar informāciju, nerada zaudējumus, bet tikai realizē pašu pieslēgšanās faktu. Parasti šādas darbības tiek kvalificētas kā administratīvie vai krimināpārkāpumi.

2. Lielākā daļa valstu, piemēram, ASV, Lielbritānija, Dānija, Zviedrija, Somija, Igaunija, Francija, Vācija, Grieķija, Ungārija, Itālija u.c., iekļaujot krimināllikumā atbildību par patvaļīgu piekļuvi automatizētajām datu apstrādes sistēmām, šīs darbības atzīst par krimināli sodāmām tikai tad, ja tās ir saistītas ar konkrētiem papildus nosacījumiem. Visbiežāk krimināatbildību par patvaļīgu piekļuvi saista ar šādiem nosacījumiem: 1) ja darbības saistītas ar sistēmas aizsardzības līdzekļu pārvarēšanu, tai skaitā sabojājot vai apejot tos; 2) ja persona piekļuvusi sistēmai ar nolūku sabojāt vai pasliktināt sistēmā esošos informācijas resursus, 3) ja tās izdarītas mantkārīgos nolūkos u.c. Jāatzīmē, ka Kontinentālo tiesību sistēmā esošo valstu krimināllikumi nesatur izsmeļošu patvaļīgas piekļuves objektīvās puses raksturojumu, turpretī vispārējo tiesību sistēmā, kur krimināatbildību par nodarījumiem informācijas tehnoloģiju jomā regulē speciāli likumi, dots izsmeļošs noziedzīgā nodarījuma „patvaļīga piekļūšana", objektīvās puses (*actus reus*) raksturojums.

Piemēram, Maltas Krimināllikuma 337. pantā 1.d. satur 11 apakšpunktus, kas apraksta nosacījumus, kad šis pants ir piemērojams. Piemēram, ja persona izdarot patvaļīgu piekļuvi, iegūst informāciju, kopē to modificē, pasliktina tās kvalitāti, traucē citu personu tiesības izmantot sistēmas resursus, pārkāpj sistēmas resursu integritāti, atklāj piekļuves kodus paroles nepiederošām personām, izmanto šim nolūkam citām personām piešķirtus identifikatorus, izpauž sistēmā saglabāto konfidenciālo vai ierobežotas pieejamības informāciju nepiederošām personām u.c. Līdzīga pieeja ir Apvienotās Karalistes likumdošanā[342] u.c.

Šobrīd Latvijas tiesību sistēmas modernizēšanā vērojama zināma ES tiesību ietekme. Nenoliedzot šī procesa nozīmīgumu, tomēr svarīgi ir noteikt mērķi, kuru mēs vēlamies sasniegt izstrādājot to vai citu krimināllikuma normu. Iekļaujot krimināllikuma pantā izsmeļošu noziedzīgā nodarījuma darbību uzskaitījumu, mēs ar tā pieņemšanas brīdi ierobežotu šī panta piemērošanas efektivitāti. Piemēram, konstruējot Krimināllikuma 241. panta pašreizējo redakciju "Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai" jāizprot, kādus mērķus vēlas sasniegt persona, kas patvaļīgi piekļūst informācijas sistēmai.

---

[342] UK Computer misuse Act 1990 Ch.18., para 1. [b.i.]

D. Tomsons (*David Thomson*) un D. Berviks (*Desmond Berwick*), analizējot patvaļīgas piekļuves aspektus, izceļ šādus mērķus:

- tieši vai netieši iegūst iespēju lietot datorsistēmas pakalpojumus;
- pārtver vai rada komunikācijas vai jebkuras datorsistēmas funkcijas pārtveršanai labvēlīgus apstākļus;
- rīkojas ar mērķi nodarīt sistēmas lietotājiem vai sistēmas resursiem kaitējumu;
- izmanto datorsistēmu vai tās resursus ar mērķi izdarīt citu noziedzīgu nodarījumu.[343]

Nevar piekrist, ka patvaļīgo piekļuvi identificē ar komunikāciju līdzekļu noklausīšanos vai pārraides pārtveršanu. Šos argumentus autors, izklāstīs analizējot atšķirības starp patvaļīgu piekļuvi un citiem noziedzīgiem nodarījumiem.

Precīzāk un vispusīgāk patvaļīgās piekļuves mērķus ir izteikuši krievu autori, norādot, ka persona, kas realizē patvaļīgu piekļūšanu vēlas sasniegt šādus mērķus:

- iegūt pieeju sistēmā glabātai informācijai;
- iegūt pieeju attiecīgās sistēmas resursiem un izmantot tos;
- padarīt informācijas sistēmu par darbnespējīgu bez draudiem tikt atklātam;
- izmantot sistēmas resursus, lai izveidotu vietu citu mērķu sasniegšanai, piem., organizējot uzbrukumu citai informācijas sistēmai. Tādā gadījumā cietušajā informācijas sistēmā kā uzbrukuma resurss tiks atzīmēta citai personai piederoša IS.[344]

Izdarot kopsavilkumu par patvaļīgās piekļuves mērķiem, tos var iedalīt trīs galvenās kategorijās: 1) iegūt iespēju piekļūt sistēmas resursiem, lai iedarboties uz to integritāti (veselumu); 2) izmantot informācijas sistēmas resursus, lai piekļūtu citas sistēmas resursiem nolūkā ietekmēt to integritāti; 3) izmantot informācijas

---

[343] Minimum Provisions for the investigation of computer based offences by David E. Thompson and Desmond R. Berwick © 1998 National Police Research Unit.

[344] Леонов Д.Г. , Лукацкий А.В., Медведовский И.Д., Семянов Б.В. Атака из Интернет. Аспекты защиты. Москва: Соломон-Р, 2002., с. 9

sistēmu kā mediju ar mērķi izdarīt citu noziedzīgu nodarījumu. No iepriekš veiktās patvaļīgās piekļuves analīzes ir skaidri redzams, ka lielā daļa pasaules valstu atbildību par patvaļīgu piekļūšanu paredz tikai tad, ja personas darbība ir saistīta ar papildus nosacījumiem. Izstrādājot grozījumus Krimināllikuma 241. pantā, autors ieteica izslēgt iespēju piemērot krimināltatbildību par „tīro" patvaļīgo piekļuvi un izslēgt no minētā panta 1. daļas sastāva priekšmetu -atsevišķi novietotu un ar tīklu nesavienotu datorsistēmu. Šo priekšlikumu likumdevējs arī atbalstīja.

### 3.4. Patvaļīgas piekļūšanas automātiskām datu apstrādes sistēmām (ADAS) nošķiršana no citiem noziedzīgiem nodarījumiem

*Patvaļīgas piekļūšanas atšķirības no noziedzīgiem nodarījumiem pret īpašumu*

„Patvaļīga piekļūšana automātiskai datu apstrādes sistēmai" pēc pazīmēm ir līdzīga Krimināllikuma 175. panta 3. d. aprakstītajam noziedzīgā nodarījuma sastāvam. Krimināllikuma 175. panta 3. daļa ir saistīta ar iekļūšanu dzīvoklī vai citā telpā vai glabātuvē[345]. Informācijas sistēma ar visu tās resursu kopumu arī tiek uzskatīta par konteineru, kurā glabājas informācija.

Piemērs. Krimināllietā *ASV pret Ali Saleh Kahlan Al-Marri*[346] tiesa konstatēja, ka slēgtu datoru failu un cieto disku aizsardzības statuss ir līdzvērtīgs slēgtam konteineram un aizsargājami adekvāti, un kā citas privātuma vērtības ir pakļautas konstitucionālai aizsardzībai. Tādejādi abi objekti ir konstitucionāli aizsargājami.

Abi nodarījumi var būt izdarīti mantkārīgu motīvu vadīti. Abi nodarījumi var būt tikai izdarīti tīši ar tiešu nodomu. Tādējādi kļūdaini var nonākt pie secinājuma, ka abu noziegumu apdraudētā interese ir viena un tā pati, proti, personas tiesība uz sava īpašuma aizsardzību.

Starp šiem nodarījumiem pastāv arī būtiskas atšķirības, piemēram, Krimināllikuma 241. pantā apdraudējuma priekšmets ir elektroniskā veidā apstrādājami informācijas resursi, netverama, netaustāma vērtības vienība, bet Krimināllikuma 175. pants paredz, ka nozagt var tikai kustamu un taustāmu mantu. Respektīvi, Krimināllikuma 175. panta 3. daļas apdraudējuma priekšmets vienmēr būs saistīts ar kustamas, taustāmas mantas valdījuma vai īpašuma tiesībām, bet informācijas resursu apdraudējums Krimināllikuma 241. panta izpratnē, nevar tikt

---

345 Is there such thing as "Virtual crime" Susan W. Brenner// California criminal law review. Vol. 4., 2001.p.1.

346 United states of America v Ali Saleh Kahlan Al-Marri// http://news.findlaw.com/hdocs/docs/almarri/usalmarri61803dmol.pdf (aplūkots 2004.gada 14.martā)

atzīts par priekšmeta valdījuma vai īpašuma tiesību pārtraukšanu, jo tiek pārkāptas piekļuves tiesības uz sistēmas resursu izmantošanu.

Otra būtiska atšķirība ir tā, ka patvaļīgu piekļuvi informācijas sistēmā var izdarīt tikai no attāluma, tas ir, izmantojot speciālos datu pārraides vai telekomunikāciju tīklus, lai piekļūtu par apdraudējuma mērķi izvēlētai informācijas sistēmai. Protams, ka informācijas sistēmas drošības aspekti ietver arī visu informācijas sistēmu resursu fizisko aizsardzību, to nodrošināšanu pret ielaušanos telpās un citiem neparedzētiem apstākļiem, taču jāpiekrīt J. Čirilo (*J. Chirillo*), ka daudz svarīgāk ir aizsargāt šo informāciju no attāluma gadījumos, ja tiek pārkāptas piekļuves tiesības.[347]

*Patvaļīgas piekļuves norobežošana no Krimināllikuma 144. panta "Korespondences pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšana"*

Teorijā vairāki autori[348] izvirza viedokli, ka patvaļīga piekļuve sistēmas resursiem un pieslēgšanās/pārtveršana ir viena un tā pati darbība. Tomēr autors piekrīt Kibernoziegumu konvencijā izteiktajam viedoklim, ka šie nodarījumi ir jākvalificē atsevišķi.

Pirmkārt, atšķirība ir speciālajā apdraudējuma objektā. Kaut gan abos nodarījumos viena no apdraudētām interesēm ir informācijas sistēmu drošība, tomēr atšķiras drošību raksturojošā pazīme. Patvaļīgas piekļuves gadījumā persona tīši pārkāpj sistēmā noteiktās piekļuves tiesības. Patvaļīga piekļuve nozīmē, ka pārkāpējs vai nu informāciju par pieejas paroli iegūst nelikumīgi, vai, izmantojot dažādas viltības, to atklāj, vai arī, izmantojot trūkumus datorsistēmas drošībā, tajā iekļūst caur sistēmas drošības programmatūrā atrasto spraugu vai arī izmanto citai personai piešķirtas tiesības.[349]

Noklausīšanās/pārtveršanai (*interception*) raksturīgs tas, ka persona vēršas pret citu ISD pazīmi, proti, konfidencialitāti. Persona pārkāpj sistēmas īpašnieka tiesību

---

347 Hack attacks revealed. A complete reference for Unix, Windows and Linux with custom security toolkit. Second edition John Chirillo. Indianopolis-Willey publishing, 2002, p.93.

348 Grabovsky P.N. Smith R. Crime in the digital age. Controling telecommunications and cyberspace illegalities. – Transaction publishers/ The federation press, 1998., p.37; Соколов А.В. Шпионские стучки. Новое и лутшее.- Полигон, Санкт-Петербург , 2000.,с.184; Computer crime in Poland: three years' expierence in enforcing the law. Contribution by Andrzej Adamski Conf CY (2001) Nat 14

349 Comentary on articles of the Convention PC-CY (2000)14- Draft EM REV.3, p. 2..

iepazīstināt ar informācijas resursiem tikai šim nolūkam pilnvarotās personām. Savas darbības persona realizē, nelikumīgi pieslēdzoties vai nu telekomunikācijām, vai datorsistēmai, pārtverot pārraidīto datu saturu. Lai izdarītu šo nodarījumu, personai nav nepieciešams patvaļīgi piekļūt sistēmas resursiem, bet tā pārtver informāciju tās pārraides procesā un izmanto to saviem mērķiem. Jāpiezīmē, ka šeit runa var būt tikai par nelikumīgu darbību, jo 1995. gada 17. janvārī ES Padomes rezolūcija (96/C 329/01)[350] par likumīgu telekomunikāciju pārtveršanu noteica kārtību, kad šāda darbība ir atzīstama par pilnīgi likumīgu.

Otrkārt, šī darbība ir saistīta ar personas korespondences noslēpuma- speciāli adresātam paredzētu ziņu, datu, vēstuļu, to skaitā elektronisko pasta sūtījumu, datņu- nelikumīgu atvēršanu. Līdz ar to šim nodarījumam ir raksturīgas divas apdraudētās intereses: 1) šis nodarījums ir vērsts pret informācijas sistēmu drošības speciālo pazīmi konfidencialitāti; 2) šis nodarījums vērsts pret personas privātās dzīves noslēpumu, kas ietver arī korespondences noslēpumu.

*Patvaļīgas piekļuves nošķiršana no noziedzīgiem nodarījumiem, kur atbildība paredzēta par nelikumīgas informācijas apriti*

ASV Deitonas universitātes 2004. gada rīkotajā kibernoziegumu seminārā[351] dalībnieki izvirzīja ideju ar terminu „patvaļīga piekļuve" aptvert tos gadījumus, kad persona pieslēdzas informācijas avotiem, kuru izmantošana aizliegta ar likumu, piemēram, bērnu pornogrāfiju saturošiem avotiem. Tādā veidā dodot iespēju ar vienotu mehānismu vērsties pret šādiem nodarījumiem, neveidojot jaunus noziedzīgu nodarījumu sastāvus. Šīs idejas autori uzskata, ka tādā veidā iespējams arī izpildīt Kibernoziegumu konvencijas protokola prasības un ierobežot informācijas, kas kurina rasu naidu, ksenofobiju u.c. apriti.

Autors neatbalsta šādu viedokli, jo ar patvaļību saprot tādus gadījumus, kad personai nav attiecīgu piekļuves tiesību informācijas sistēmai, ko tai piešķīris attiecīgās sistēmas administrators vai cita pilnvarota persona, bet nevis valsts noteiktu aizliegumu izmantot to vai citu informācijas resursu. Līdz ar to rīcību, ka

---

350 Council Resolution of 17 January 1995 on the lawful interception of telecommunications Official Journal C 329 , 04/11/1996 P. 0001 – 0006// http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31996G1104&model=guichett (aplūkots 2004.gada 23. martā)

351 Dayton Cybercrime Seminar 2004.spring http://lawschool.westlaw.com (aplūkots 2004.gada 25. martā)

persona pārkāpj valsts noteikto atsevišķu informācijas veidu aprites kārtību, nevar kvalificēt kā patvaļīgu piekļūšanu.

*Piekļūšana publiski pieejamām mājas lapām*

Pasaulē aizvien plašāk izplatās gadījumi, kad personas likumīgi piekļūst publiski pieejamām mājas lapām, piem., partiju, laikrakstu vai personālajām mājas lapām. Tās izmaina to saturu un tādā veidā sabojā mājas lapas. D. Deninga (*D. E. Denning*) šīs personas nosauc par politiski motivētiem „hakeriem" (*hacktivists*)[352]. Šo personu mērķis ir radīt nekārtības kibertelpā, un viena no darbības metodēm ir ar speciāli pielāgotām datorprogrammām vai rīkiem, ietekmēt publiski pieejamo mājas lapu resursus. Pasaulē šī procesa novērtēšanā nav vienota viedokļa. Eksperti to atzina, izstrādājot kibernoziegumu konvenciju. Problēma rodas, ka pati piekļuve mājas lapai caur hipersaiti[353], sīkdatni[354], sāknēšanu[355] vai citu publiski pieejamu piekļuves mehānismu nav nelikumīga, jo mājas lapas autors to ir izveidojis pieejamu jebkuram interneta lietotājam. Pieslēdzoties šādai mājas lapai, lietotāji nevar tikt nodalīti autorizētos un neautorizētos, jo to neparedz šāda informācijas avota izveidošanas parametri. Ja nav noteikta piekļuves kārtība, tad nav pamata runāt par piekļuves prettiesiskumu.

Piemērs. ASV lietā *EF Cultural travel BV, ET AL. v Zefer Corporation and Explorica, INC., ET AL.*. EF un Explorica bija divas konkurējošās firmas tūrisma biznesā. Explorica nolīga Zefer, lai tas izstrādātu speciālu datorprogrammu "*scraper*", ar kuras palīdzību tā nokopēja informāciju no konkurentu publiski pieejamās mājas lapas par sniegto pakalpojumu cenām, salīdzināja tās ar citiem pakalpojumiem un izvietoja vienā Excell programmas izklājlapā un tādā veidā ieguva iespēju izanalizēt cenu politiku un piedāvāt lētāku pakalpojumu. EF iesūdzēja Explorica tiesā par patvaļīgu piekļuvi publiski pieejamai mājas lapai, motivējot ar to, ka šādas programmas lietošana pārsniedz piešķirtās lietotāja tiesības. Tāpēc tā ir uzskatāma par patvaļīgu piekļuvi. Tiesa sūdzību noraidīja, motivējot ar to, ka EF savā mājas lapā nebija precīzi norādījusi, kas mājas lapas lietotājam atļauts un kas aizliegts. Neesot šādai skaidrai norādei, piemēram, ka publiski pieejamā mājas lapā esošos resursus nedrīkst kopēt vairāk kā vienā eksemplārā vai to analīzei izmantot speciālas programmas utt., nav pamata arī runāt par patvaļīgu piekļuvi.[356]

---

352 Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy by Dorothy E. Denning Georgetown University// http://www.nautilus.org/info-policy/workshop/papers/denning.html (aplūkots 2004.gada 7. februārī)

353 http://www.termini.lv/index.php?term=hipersaite&lang=LV&terms=hipersaite (aplūkots 2004.gada 23. martā)

354 http://www.termini.lv/index.php?term=cookie&lang=EN&terms=cookies (aplūkots 2004.gada 23. martā)

355 http://www.termini.lv/index.php?term=boot&lang=EN&terms=boot (aplūkots 2004.gada 23. martā)

356 EF Cultural travel BV, ET AL. v Zefer Corporation and Explorica, INC., ET AL// http://business.cch.com/computer/1020/EFCultural.pdf (aplūkots 2004.gada 11. martā)

Līdz ar to šādas darbības neatbilst noziedzīgā nodarījuma „patvaļīga piekļūšana" jēgai, jo netiek pārkāptas piekļuves tiesības. Taču nenoliedzami, ka personai, izmantojot šādas mājas lapas, ir tiesības tikai rīkoties un izmantot tur publicēto pieejamo informāciju tādā apmērā, kādā to piedāvā pakalpojumu sniedzējs vai mājas lapas īpašnieks. Ja persona ar speciāliem programatiskiem līdzekļiem maina mājas lapas dizainu, saturu un tādā veidā traucē informācijas resursa normālu darbību, tad atkarībā no vainīgā nodoma šādas darbības ir kvalificējamas vai kā sistēmas un tajā ievietoto informācijas resursu traucēšana vai arī, ja tā ir bezmotīvu rīcība, tad tā ir rupja sabiedriskā miera traucēšana, kas izpaužas acīm redzamā necieņā pret sabiedrību, traucējot uzņēmumu vai iestāžu vai organizāciju darbu, jo nenoliedzami, ka, sabojājot citai personai piederošu mājas lapu, uz laiku tiek pārtraukta iespēja resursa īpašniekam izmantot mājas lapu tam nolūkam kam tā radīta, piemēram, sniegt informācijas pakalpojumus, realizēt e- pārvaldi vai veikt citas funkcijas. Tāpēc šādi gadījumi ir kvalificējami kā huligānisms.

Ir arī tādas mājas lapas, kurām ir iespējams piekļūt caur internetu, bet kas prasa to lietotājiem speciālu autorizāciju. Piemēram, autoram ir pieeja dažiem ASV valdības informācijas resursiem un ASV, Lielbritānijas u.c. valstu augstskolu informācijas resursiem internetā tāpēc, ka minētās iestādes viņam piešķīra lietotāja vārdu, paroli un identifikācijas kodu. Šādu informācijas resursu nevar uzskatīt par vispārpieejamu, bet gan par pieejamu tikai reģistrētiem lietotājiem. Ja kāds patvaļīgi piekļūs šādas mājas lapas resursiem, tad viņu var saukt pie atbildības par patvaļīgu piekļūšanu datorsistēmas resursiem.[357] Dotajā piemērā internetā izvietotā mājas lapa ir uzskatāma par datorsistēmas informācijas resursu un atzīstama par Krimināllikuma 241. panta priekšmetu, jo tās lietošanas kārtību un lietotāju autorizācijas pakāpi noteic tās īpašnieks. Tāpēc, lai patvaļīgi piekļūtu šādai mājas lapai, personai ir jāpārvar mājas lapas aizsardzībai ieprogrammētie loģiskās aizsardzības līdzekļi, bet šāda darbība ir atzīstama par patvaļīgu piekļuvi krimināllikuma izpratnē.

---

[357] Informācijas un komunikāciju tiesības Ķiņa U. redakcijā II. sēj., Trešā grāmata. Rīga: Turība, 2002.-281. lpp.

### 3.5. Apstākļi, kas izslēdz krimināLatbildību par patvaļīgu piekļuvi

Pasaulē nav viendabīga attieksme pret patvaļīgas piekļuves saturu. Tāpēc, izstrādājot jauno Krimināllikuma 241. panta redakciju, tās tekstam ir jābūt viegli uztveramam un saprotamam, lai to un nepieciešamības gadījumā varētu piemērot citas Konvencijas un ES dalībvalstis. Latvijai saistoši ES institūciju pieņemtie normatīvie akti noteic, ka, vērtējot patvaļīgas piekļuves saturu, ir jāņem vērā apstākļi, kas izslēdz atbildību par patvaļīgu piekļuvi. Jautājums par apstākļiem, kas izslēdz krimināLatbildību par nodarījumu par patvaļīgu piekļuvi ADAS, līdz šim ne krimināltiesību teorijā ne arī praksē nav diskutēts. Te nevar pilnībā attiecināt arī Krimināllikuma III. nodaļā 28-34. pantā minētos apstākļus. Pašreizējā redakcijā patvaļīga piekļuve atzīta par formālu nodarījumu. Tam nav nepieciešama materiālu seku iestāšanās. Tāpēc autors šaubās, vai vispār likumdevējs paredzējis Krimināllikuma III nodaļā minēto nosacījumu piemērošanu formālu nodarījumu gadījumos. Analizējot attaisnojošos apstākļus, jāatzīst, ka tie ir attiecināmi uz diviem pret informācijas sistēmu drošību vērstiem nodarījumu sastāviem, tas ir, uz Krimināllikuma 241. pantu- patvaļīga piekļūšana, un Krimināllikuma 244. pantu – ierīces ļaunprātīga izmantošana.

No Krimināllikuma III nodaļā minētajiem apstākļiem par piemērojamiem Krimināllikuma 241. panta nodarījuma attaisnošanai, autors izceļ:

1) Krimināllikuma 32. p. galējo nepieciešamību, ja patvaļīga piekļuve ADAS izdarīta, lai novērstu kaitējumu, kas apdraud valsts vai sabiedrības intereses, vai šīs personas, vai citas personas tiesības, kā arī, ja šo kaitējumu nebija iespējams novērst citiem līdzekļiem;

2) Krimināllikuma 33. p. attaisnojamu profesionālo risku, ja piekļuve sistēmas resursiem saistīta ar profesionālu darbību, kam ir noziedzīga nodarījuma sastāva pazīmes, bet ja tā veikta lai sasniegtu sociāli derīgu mērķi, piem., ar speciāli izveidotu datorprogrammu atklāt pārraugāmās sistēmas drošības vārīgās vietas, ja šo mērķi nebija iespējams sasniegt citādā veidā.

A. Judins izvirza profesionālā riska attaisnošanai šādus kritērijus: 1) persona riskē nolūkā sasniegt sociāli derīgu mērķi; 2) veiktās rīcības atbilst laikmeta zinātnes un tehnikas līmenim un pieredzei; 3) izvirzītais mērķis nav bijis

sasniedzams, nesaistot rīcību ar risku; 4) persona, kas pieļāvusi risku, ir darījusi visu kaitējuma novēršanai tiesiski aizsargātām interesēm; 5) risks ir saistīts ar personas profesionālu darbību.[358]

Autors uzskata, ka noziedzīgos nodarījumos pret informācijas sistēmu drošību sistēmas administratora vai pārvaldnieka darbība, pārbaudot sev uzticēto ADAS drošību, ir tieši saistīta ar profesionālo risku, jo administratoram ir regulāri jāveic pasākumi, lai viņš atklātu vārīgās drošības vietas sistēmā. To var veikt, pielāgojot vai izstrādājot programmu moduļus, kas pārbauda sistēmu drošību. Bet, kā redzams kriminālliet ā *US v Moris*[359], tad neskatoties uz to, ka viņš programmu radīja sociāli derīgam mērķim, proti, pārbaudīt sev uzticēto sistēmu drošību, tiesa viņu atzina par vainīgu patvaļīgā piekļūšanā federālajām informācijas sistēmām, jo viņa radītā programma tām nodarīja lielu kaitējumu. Faktiski Moris darbība bija saistīta ar profesionālo pienākumu, risku sociāla mērķa labā, piemērojot zinātnes risinājumus, taču domāju, ka, testējot ar tīklu savienotu ADAS, piem., ar speciāli izveidotas datorprogrammas palīdzīgu, nav praktiski iespējams veikt visus pasākumus, lai novērstu kaitējumu tiesiski aizsargātām interesēm. Kā jau minēts iepriekš, tad nav iespējams izgatavot tādu pārbaudes rīku, kas būtu absolūti nevainojams un bez kļūdām. Ja šis fakts ir visiem zināms, tad ir skaidrs, ka jebkura sistēmas pārbaude, izmantojot šim nolūkam veidotu datorprogrammatūru, satur arī profesionālu risku. Tāpēc pilnīgi nodrošināties pret iespēju nodarīt kaitējumu citu personu interesēm vienkārši nav iespējams. Tāpēc jāpiekrīt A. Judinam, ka ne katra ar risku saistīta darbība nodrošina vēlamo rezultātu un, neskatoties uz pūlēm, var sociāli derīgu mērķi arī nepanākt.[360] No iepriekšteiktā var secināt, ka ne katrs profesionāls risks var tikt atzīts par attaisnojamu. Morisa gadījumā tiesa norādīja, ka viņa vaina ir tā, ka viņš, programmējot šo datorprogrammu, ko šobrīd visā pasaulē pazīst kā "datortārpu", izmantoja līdz tam nepārbaudītu tehnoloģisku risinājumu un zaudēja kontroli pār šīs programmas vadību;

---

[358] Judins A.Krimināl atbildības izslēdzamības apstākļi. Rīga: TNA, 2000., 171 lpp.

[359] Judgement in US v Robert Tappan Morris// http://www.rbs2.com/morris.htm (aplūkots 2004.gada 23. martā)

[360] Turpat, Judins A., 172. lpp.

3) Krimināllikuma 34. pantu noziedzīgas pavēles vai noziedzīga rīkojuma izpildīšanu, ja persona nav apzinājusies šīs pavēles vai rīkojuma noziedzīgo raksturu un tas nav bijis acīm redzams. Minētajam gadījumam atbilst iepriekšminētais gadījums par ministra uzdevumu padotajam ielauzties ministrijas pakļautībā esošā informācijas sistēmā. Daļēji Krimināllikuma 34. pantā paredzētiem nosacījumiem atbilst arī gadījumi, ja pavēle vai rīkojums par sistēmas drošības pārbaudi dots dienesta kārtībā padotai personai, kas nav attiecīgās sistēmas lietotājs vai darbinieks. Respektīvi, personai tiek dots uzdevums piekļūt sistēmas resursiem vai ar speciālas ierīces palīdzību vai arī apejot sistēmas aizsardzības līdzekļus un atklāt tās aizsardzībā vārīgās vietas vai veikt manipulācijas ar informāciju.

U. Krastiņš, raksturojot krimināltbildību izslēdzošus apstākļus, norāda, ka tiem piemīt vairākas kopīgas pazīmes: 1) visos gadījumos ir saskatāma personas darbības līdzība ar kāda Krimināllikumā paredzētā noziedzīgā nodarījuma sastāva objektīvās puses pazīmēm; 2) šādos apstākļos darbības vērstas uz sociāli derīga mērķa sasniegšanu; 3)kaitīgums, kas ar šādām darbībām tiek nodarīts kādām citas personas interesēm, ir attaisnojams; 4) realizējot savas darbības apstākļos, kas izslēdz krimināltbildību, personas subjektīvā attieksme pret šīm darbībām, jo tās vērstas uz sociāli derīga mērķa sasniegšanu.[361]

Līdzīgu viedokli pauž arī V. Orehovs, norādot, ka, kaut arī darbība ir saistīta ar zināma kaitējuma nodarīšanu ar likumu aizsargātām interesēm, tā nevar tikt atzīta par noziedzīgu nodarījumu tāpēc, ka darbībai nav prettiesiska rakstura, un līdz ar to persona nav vainojama.[362] Autors pilnīgi piekrīt viedoklim, ka par attaisnojošu darbību var runāt tikai tad, ja darbība pati par sevi, kaut arī satur Krimināllikuma 241. un 243. pantā paredzētās objektīvās puses pazīmes, ir vērsta uz sociāli derīga mērķa sasniegšanu vai savu likumisko tiesību realizēšanu. Ja šādu nosacījumu nav, tad nevar būt ne runas par personas darbību attaisnojošiem apstākļiem.

---

361 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 228.lpp.

362 Орехов В.В. Необходимая оборона и иные обстоятельства, исключающие преступность деяния.Санкт-петербург-Юридический центр Пресс, 2003, с.22

ES priekšlikuma par Ievarlēmumu paskaidrojošā memorandā[363] izvirzīta prasība par likumīga lietotāja tiesību satura un apstākļu, kas izslēdz krimināLatbildību par patvaļīgu piekļuvi, noteikšanu nacionālajā likumdošanā. Jautājums ir svarīgs un noteikti ņemams vērā izstrādājot grozījumus Krimināllikumā. Kā minēts iepriekš, tad ne visi ietvarlēmuma memorandā ietvertie atbildību izslēdzošie apstākļi atbilst Krimināllikuma III nodaļā paredzētajiem nosacījumiem. Jāpiekrīt A. Judinam, ka krimināltiesības tāpat kā dzīve nevar būt iedomājama bez izmaiņām. Tās prasa jaunu apdraudējumu rašanās, valsts saistības, iestājoties dažādās starptautiskās organizācijās tml. Tāpēc krimināllikuma papildināšana ar jauniem pantiem, kas paplašinātu krimināLatbildības izslēdzamības apstākļu kopu, ir objektīvi nepieciešama, jo tādējādi tiks novērsti tiesību robi, kuru dēļ dažos gadījumos ir visai grūti nodrošināt tiesību ievērošanu.[364] Autors neatbalsta viedokli, ka šādi atbildību izslēdzošie apstākļi jāiestrādā Krimināllikuma 241. panta redakcijā. Šie krimināLatbildību izslēdzošie apstākļi attiecas uz plašāku nodarījumu, kas vērsti pret informācijas sistēmu drošību, loku. No vienas puses, iestrādājot precīzus nosacījumus, kad personas darbība nav atzīstama par patvaļīgu piekļuvi, likumdevējs skaidri un precīzi paustu savu pozīciju un tādā veidā nodrošinātu attiecīgo personu tiesiskās garantijas, bet no otras puses, kāpēc viena nozieguma sastāvam ir jābūt šādām garantijām, bet savukārt citām nē. Tomēr Krimināllikumā piem., 254. pants, 324. pants tieši paredz nosacījumus personu atbrīvošanai no krimināLatbildības. Tas nozīmē, ka šāda prakse Krimināllikuma sevišķā daļā jau pastāv. Ņemot vērā to, ka Latvija 2004. gada 1. maijā pievienojās ES juridiskajai telpai, ir ļoti svarīgi, lai dalībvalstis pēc iespējas tuvinātu savus viedokļus par noziedzīgo nodarījumu pret informācijas sistēmu drošību saturu, to skaitā arī par atbildību izslēdzošiem apstākļiem.

---

[363] Proposal for a Council framework decision on attacks against information systems. Explanatory memmorandum COM (202) 173 final

[364] Turpat, Judins A., 259. lpp.

ES Padomes priekšlikumā par ietvarlēmumu paskaidrojošā memorandā[365] ieteikts paredzēt šādus nosacījumus personu atbrīvošanai no atbildības par patvaļīgu piekļuvi:

1. *Vienkāršo lietotāju darbības, to skaitā viņu tiesības lietot šifrēšanu, lai aizsargātu savas komunikācijas un datus.* Ja personai sistēmas īpašnieks vai pilnvarotā persona ir piešķīrusi lietotāja pieeju sistēmas resursiem, tad tai ir tiesības piekļūt sistēmai, apstrādāt sev paredzēto informāciju un veikt nepieciešamos pasākumus, lai aizsargātu to konfidencialitāti, piemēram, izmantojot kriptogrāfiju. Kriptogrāfijas pamatuzdevumi ir nodrošināt datu drošu pārraidi un aizsardzību. Vispirms kriptogrāfija nodrošina informācijas konfidencialitāti, tas ir, informācijas pieejamību tikai autorizētām personām. Pastāv vairākas iespējas, kā nodrošināt konfidencialitāti, sākot no fiziskās aizsardzības līdz matemātiskajiem algoritmiem, kas nodrošina datu nesalasāmību. Otrkārt, kriptogrāfija nodrošina arī datu integritāti, lai netiktu neautorizēti aizskarts to veselums, tas ir, novērstu jebkādu neautorizētu lietotāju manipulāciju ar datiem. Datu manipulācija ietver datu iestarpināšanu, izdzēšanu un aizstāšanu ar citiem datiem.

Šifrēšanu, tai skaitā arī kriptogrāfiju, var izmantot arī kā patvaļīgas piekļuves instrumentu, piemēram, persona likumīgi piekļūst informācijas sistēmai un šifrē tādu informāciju, uz kuru tai nav tiesību. Atstājot šifrēšanas atslēgu sev, tā, piem., izspiež naudu no informācijas īpašnieka, jo pretējā gadījumā informācija ir zaudēta. Vai gadījums, kad, realizējot patvaļīgu piekļuvi informācijas sistēmai, persona neatļauti šifrē piekļuves identifikatorus, tādā veidā bloķē sistēmas darbību un nodara kaitējumu. Tādējādi, kā redzams, persona, kurai ir likumīga pieeja sistēmas resursiem, var izmantot šifrēšanas instrumentus arī negodīgos nolūkos. Problēma ir tā, ka Latvijā šifrēšana nav tiesiski regulēta, līdz ar to šo jautājumu var regulēt tikai katras sistēmas īpašnieks vai tā pilnvarotā persona deleģējot precīzas piekļuves tiesības lietotājam.

2. *Reversā inženierijas izmantošana.* Reversā inženierija[366] ir process, kura mērķis ir iegūt neizpaužamo informāciju *(know- how)* vai zināšanas par cilvēka

---

[365] Proposal for a Council framework decision on attacks against information systems. Explanatory memorandum COM (202) 173 final

darba rezultātā radītu vērtību. Praksē izšķir likumīgu un nelikumīgu reversās inženierijas lietošanu. Piemēram, P. Samuelsone uzskata, ka likumīgs reversās inženierijas piemērs ir tad, ja persona analizē pusvadītāju trīsdimensiju topogrāfijas shēmu un pēc tam to izmanto uz citas platformas, uzsākot ražot jaunu produktu. Reversā inženērija tiek izmantota kā prakses standarts datorprogrammu un pusvadītāju ražošanā. Šīs metodes likumīga izmantošana izpaužas datorprogrammas vai pusvadītāja koda dekompilācijā un demontēšanā ar mērķi padarīt šos produktus savietojamus ar citām datorprogrammām. Tomēr šīs darbības ir likumīgas tad, ja to atļauj datorprogrammas izmantošanas licence, un šobrīd lielākā daļa datorprogrammu ražotāju aizliedz reverso inženēriju izmantot savās datorprogrammās.

ES Direktīva par datorprogrammu aizsardzību noteic, ka personai, kurai ir tiesības lietot datorprogrammu ir tiesības vērot, pētīt, testēt datorprogrammu funkciju izpildi, noteikt programmu lietošanas elementus un principus, kas ir programmas darbības pamatā, kā arī veikt citas darbības bez tiesību turētāja atļaujas.[367] Līdz ar to var izdarīt secinājumu, ka reversās inženierijas izmantošana ir pieļaujama galvenokārt autortiesību un intelektuālā īpašuma jomā. Reversās inženērijas juridiskos aspektus Latvijas Republikā regulē Autortiesību likuma[368] 29. un 30. pants, kas noteic lietotāju tiesības un ierobežojumus gan datorprogrammu adaptēšanas un cita veida pielāgošanas tiesībās, gan datorprogrammu sadarbspējas nodrošināšanā.

Reversās inženierijas nelikumīgie pielietošanas aspekti. Reversās inženierijas izmantošana nereti tiek uzskatīta par rūpnieciskās spiegošanas sastāvdaļu un patvaļīgas piekļuves realizēšanas instrumentu. Liela daļa datordrošības ekspertu uzskata, ka reversā inženierija kā patvaļīgas piekļuves instruments tiek izmantota katru dienu, iesūtot sistēmā datortārpus vai Trojas zirgus un tādā veidā paralizējot sistēmas darbību vai izveidojot, tā saucamās aizmugurējās lūkas (*back door*),

---

366 The law and economics of reverse engineering by Pamela Samuelson and Susanne Scotchmer// Yale Law Journal May 2002.p.1577

367 Directive 91/250 of May 1991 on the legal protection on computer programs// OJ L 122 , 17/05/1991 P. 0042 - 0046

368 WWW.Likumi.lv. Mājas lapa Autortiesību likums// http://www.likumi.lv/doc.php?id=5138 (aplūkots 2004.gada 25. martā)

pārņem tās darbības kontroli. Izmantojot reverso inženieriju, ir iespējams iedarboties uz datorprogrammu kodiem, ievietojot programmā kādu kaitīgu funkciju, vai, izmantojot reversās inženierijas metodi, apiet arī sistēmas drošības līdzekļus un nelikumīgi piekļūt sistēmas resursiem.

3. *Pārvaldnieku, kontrolieru un operatoru darbības sistēmā un tīklos.* Lai realizētu informācijas sistēmu drošību, katrā sistēmā ir nepieciešams izstrādāt savus iekšējos informācijas sistēmas drošības noteikumus. Šajos noteikumos ir jāparedz sistēmas lietotāju un amatpersonu tiesības un pienākumus sistēmas resursu izmantošanā un pieejamībā. Šajā punktā minētās personas ir sistēmas īpašnieka darbinieki, kas savus pienākumus veic uz darba tiesisko attiecību pamata. Neapšaubāmi, ka viņu pienākums ir kontrolēt, lai pārraugāmās sistēmas resursi funkcionētu nepārtraukti, lai sistēmā tiktu nodrošināti visi drošības parametri. Tāpēc ES ietvarlēmums satur pilnīgi pamatotu prasību nepieļaut kriminālatbildību par darbībām, ko sistēmas atbildīgās amatpersonas veic savu tiesību ietvaros, pat tad, ja šo darbību rezultātā tiek nodarīts kaitējums sistēmas īpašniekam.

4. *Pilnvarotu sistēmas darbinieku gan ārpussistēmas pilnvarotu personu speciāli veiktas sistēmu drošības pārbaudes.* Nesen presē bija publicēta informācija, ka Igaunijas valdība gatavojas nolīgt "hakerus", lai pārbaudītu valdības sistēmas drošības stāvokli un atklātu vārīgās vietas. Šādas pārbaudes uzaicinātie eksperti nereti veic, izmantojot tos pašus instrumentus, ko izmanto personas, lai realizētu patvaļīgu piekļuvi ADAS. Tādā veidā speciāli veidotie programmatiskie līdzekļi dod iespēju atklāt trūkumus un vārīgās vietas sistēmas drošībā un veikt pasākumus to novēršanā. To nevar izdarīt bez patvaļīgas piekļūšanas imitēšanas. Tāpēc šāda darbība ir pielīdzināma profesionālam riskam, jo tā ir vērsta uz sociāli derīgu mērķi.

6. *Leģitīma zinātniskā pētniecība.* Jautājumi par atbrīvošanu no kriminālatbildības, ja darbība ir veikta zinātniskās pētniecības nolūkos, ir jau risināti vairākos normatīvos, aktos. Piemēram, MK Noteikumos Nr 348 „Noteikumi par erotiska un pornogrāfiska rakstura materiālu ievešanu, izgatavošanu, izplatīšanu, publisku demonstrēšanu vai reklamēšanu VI 16.1.6. punkti paredz šo materiālu izmantošanu zinātniskiem pētījumiem vai medicīniskos nolūkos. Drošības sistēmas drošības pētīšana vienmēr ir saistīta ar zināmu risku, tāpēc arī,

veicot šādu pētījumu, sistēmas īpašniekam var tikt nodarīts zināms kaitējums vai pat realizēta patvaļīga piekļuve sistēmas resursiem.

Tā kā patvaļīgas piekļuves satura tulkošanā nav vienota viedokļa netiek, tad nav pareizi krimināllikumā iestrādāt pilnīgas un vispusīgas tādu noziedzīgu nodarījumu kā patvaļīga piekļuve informācijas sistēmām, ierīču ļaunprātīga izmantošana u.c. definīcijas. Izstrādājot definīciju, mēs ar to pašu brīdi sašaurinām attiecīgā jēdziena piemērošanas iespējamību, bet tas, ņemot vērā tehnoloģiju straujo attīstību, var kļūt par bremzējošu faktoru šādu noziedzīgu nodarījumu apkarošanā.

Autors atbalsta Kibernoziegumu konvencijā ietverto pieeju, kas konvencijā paredzētiem noziegumiem nedod izsmeļošu definīciju, bet gan raksturīgāko pazīmju aprakstu. Tādējādi Konvencija dod iespēju katrai dalībvalstij attīstīt savu krimināLo likumdošanu, ievērojot nacionālās īpatnības, bet tai pašā laikā nosakot minimālo kritēriju kopumu, kas dalībvalstīm jāievēro, īstenojot konvencijas prasības.

3.6. Citu objektīvo pusi saturošu darbību krimināltiesiskais raksturojums

**Ievadīšana**- tehniska darbība, kuras rezultātā datu apstrādes sistēmā tiek ievadīta jauna informācija. Jebkurš datu apstrādes sistēmas lietotājs ir tiesīgs atbilstoši savām lietotāja tiesībām veikt informācijas ievadīšanu sistēma. Piemēram, ja persona, kurai ir tiesības veikt datu apstrādi sistēmā, no interneta resursa ievada sistēmā sev nepieciešamu dokumentu, tad šāda darbība būs absolūti tiesiska. Taču, ja sistēmas administrators ir uzlicis lietotājam ierobežojumu ielādēt sistēmā programfailus, bet lietotājs to apzināti pārkāpj, tad šāda rīcība zināmā mērā var tikt atzīta par patvaļību. Tomēr arī šādai informācijas ievadīšanai, nav krimināltiesiska rakstura, jo Krimināllikuma 243.pantā paredzēta atbildība tikai par apzināti nepatiesas informācijas ievadīšanu sistēmā. Tas nozīmē, ka persona, kas veic šo darbību, jau pirms informācijas ievadīšanas sistēmā zina, ka šī informācija ir kaitējumu nesoša vai arī tā ir viltota ar mērķi ietekmēt informācijas resursus, lai veiktu specifiskas darbības, ko nav autorizējis sistēmas īpašnieks vai tiesiskais valdītājs. Likumdevējs ir noteicis, ka krimināLatbildība par šādām darbībam iestājas tikai tad, ja ar to fiziskai vai juridiskai personai nodarīts būtisks kaitējums.

**Kopēšana.** Kopēšana ir kopiju radīšana jebkurā materializētā formā, to skaitā, elektroniskā, faksimila, fotokopiju u. c. veidos. Galvenais aktīvās darbības mērķis ir jebkādā materializētā veidā neatļauti iegūt kopiju. Krievijas KK 272. pants „Nelikumīga pieeja datorinformācijai" paredz atbildību, ja šo darbību rezultātā informācijas resursi tiek sabojāti, bloķēti, modificēti vai kopēti. V. Liholaja, komentējot KL 242. pantu (red. līdz 2005.gada 1. jūnijam), norāda, ka minēto nodarījuma priekšmetu kopēšana nozīmē to pavairošanu jebkurā veidā.[369] No tehniskā redzes viedokļa tam var piekrist. Līdzīgu viedokli privātā sarakstē ar autoru atbalsta arī RITI direktors tehnisko zinātņu doktors J. Borzovs, norādot, ka no tehniskā redzes viedokļa persona, atverot uz datora ekrāna informāciju, to automātiski nokopē.

Analizējot KL 241.-245. panta dispozīcijā ietverto darbības „kopēšana" jēgu, ir skaidrs, ka nodarījums neparedz atbildību par failu tehnisku kopēšanu sistēmas resursu ietvaros. Šeit patiesībā rodas nesamierināma problēma starp darbības tehnisko un juridisko saturu. Ja tehniski kopēšanu izdara ar to brīdi, kad ieslēdz datoru, tad juridiski kopēšana ir darbība, kuras rezultātā informācija tiek pārnesta uz citu datu nesēju un tiek izveidota kopija, kura vairs neatrodas sistēmas īpašnieka tiesiskā valdījumā vai īpašumā.

Piemērs. Kā redzams no Vidzemes apgabala tiesas sprieduma S.C. lietā, tad S.C. nolūkā veikt krāpšanu, nokopēja a/s "Unibanka" speciāli veidoto datorprogrammu"A", izveidojot tās kopiju citā datu nesējā, proti, savā portatīvajā datorā, un papildus izveidoja programmu "A1", un veica ar to attiecīgas manipulācijas un to rezultātā izkrāpa cietušai naudu vairāk kā 35 000 latu.
Dotajā piemērā, darbības nav kvalificētas pēc KL 242. panta 2. daļas, tomēr, spriežot pēc celtās apsūdzības, tās pilnīgi satur visas KL 242. panta 2. daļā paredzētās noziedzīgā nodarījuma pazīmes, proti, neatļautu datorprogrammas "A" kopēšanu uz cita nošķirta datu nesēja. Šī darbība izdarīta, pieslēdzoties cietušā datortīklam, respektīvi, izmantojot sakaru līnijas, un veikta apejot, sistēmas aizsardzības līdzekļus, jo ar speciāli izveidotu programmu, S.C. ieguva informāciju un nokopēja citā datu nesējā cietušai personai piešķirto digitālo parakstu. Darbību rezultātā cietušai tikai nodarīts būtisks kaitējums, jo iegūtā programma tika izmantota krāpšanā, kuras rezultātā tika nodarīti zaudējumi vairāk kā 35 000 latu apmērā.

**Informācijas modificēšana un grozīšana** pēc būtības ir jēdzieni ar vienādu nozīmi, jo, nesagrozot informāciju, to nav iespējams modificēt. Informācijas modificēšana vai grozīšana, to veicot autorizētai personai, ir normāla informācijas aprites sastāvdaļa un lietotāja tiesība rīkoties ar sev pieejamiem sistēmas resursiem,

---

[369] Krastiņš U., Liholaja V., Niedre A. Krimināllikuma zinātniski- praktiskais komentārs (3) Sevišķā daļa. Profesora U. Krastiņa redakcijā. Rīga: AFS, 2003, 228-229.lpp.

tai skaitā grozīt to saturu, ievadīt jaunu informāciju, dzēst nevajadzīgo u.c. Modificēšana nozīmē padarīt informāciju atšķirīgu no oriģināla. Bojāšana, dzēšana, miksēšana ir tikai modifikācijas metodes. Krimināalatbildība par informācijas modificēšanu vai grozīšanu var iestāties tikai tad, ja šīs darbības veic persona, kurai uz to nav tiesību vai kura pārkāpj piešķirtā pilnvarojuma robežas.

**Bojāšana**- Informācijas vai aizsardzības sistēmu, informācijas nesēju, programmatūras bojāšana ir tāda darbība, kuras rezultātā informācija, informācijas nesējs (diskete, CD, cietais disks (*hardware*) u.c.) vai programma nav spējīga izpildīt tai paredzētos uzdevumus. Tas ir stāvoklis, kad iepriekšminētie objekti ir daļēji zaudējuši savu paredzēto nozīmi, bet šo darbību ir iespējams atjaunot.

**Iznīcināšana** – ir informācijas vai aizsardzības sistēmu, informācijas nesēju, programmatūras fiziska iznīcināšana, kas ir tāds stāvoklis, kad minētais priekšmets nav vairāk izmantojams pēc savas nozīmes un tā darbību nav iespējams atjaunot. Datorprogrammu un informācijas iznīcināšanu var izdarīt arī ar tehniskām un elektroniskām metodēm. To sauc nevis par iznīcināšanu, bet par *dzēšanu* (erasure). Piemēram, matemātikas zinātņu doktors P. Treijs uzskata, lai iznīcinātu informāciju, ir fiziski jānogalina cilvēks, kas ievadījis šo informāciju informācijas nesējā. Tāpēc viņš uzskata, ka elektronikā ir jālieto vārds *dzēšana*. EP Kibernoziegumu konvencijas paskaidrojošā memorandā norādīts, ka iznīcināšana „delition" pēc savas dabas ir līdzīga taustāmas materiālas substances iznīcināšanai.[370] Pēc būtības šim faktam ir tikai teorētiska nozīme. Galvenais ir konstatēt, ka attiecīgais priekšmets ir darboties nespējīgs un tā darbību nav iespējams atjaunot.

**Aizklāšana** (*supression*). Aizklāšana nozīmē jebkuru darbību, kas beidz pieeju datorsistēmā vai medijā saglabātiem datiem. Šis termins satur divas nozīmes: 1) ka dati ir nodzēsti un tie vairs fiziski neeksistē; 2) ka tie padarīti nepieejami, tas ir, šiem datiem nevar piekļūt un tie ir ekspluatācijai nederīgi.

Iepriekšaprakstītās darbības ir tikai daļa no tām, kas raksturo pilnu informācijas aprites ciklu, tāpēc pilnīgi pamatoti daudzu valstu likumdevēji, veidojot konkrēto

---

[370] Cybercrime Convention Explanatory Memorandum , para, 61.

noziedzīgo nodarījumu dispozīcijas, necenšas to tekstā iekļaut plašu darbību aprakstu, jo pilnīgi pietiek ar to, ja likumdevējs norāda, ka darbības raksturs saistīts ar integritātes, konfidencialitātes vai pieejamības pārkāpšanu, un tas attiecīgi nozīmē, ka integritāti var pārkāpt tikai tad, ja jebkādā veidā tiek mainīts sistēmas resursu veselums, konfidencialitāti- ja persona piekļūst tādiem informācijas resursiem, uz kuriem tiem nav tiesību, bet pieejamība- ja persona zinot, ka viņai nav tiesību piekļūt sistēmas resursiem, tīši veic darbības, lai šādu piekļuvi veiktu. Tehnisko darbību daudzums, kuru rezultātā var tikt aizskartas personas tiesības uz informācijas integritāti, pieejamību un konfidencialitāti, ir ļoti plašs. To uzskatāmi raksturo šāds piemērs.

Kibernoziegumu konvencijas apspriešanas laikā ASV Stanfordas universitātes Hūvera institūta speciālisti[371] ieteica, definējot Konvencijas 4.pantu, papildus neatļautai grozīšanai, bojāšanai, iznīcināšanai, pasliktināšanai vai aizklāšanai, vai apzināti nepatiesai informācijas ievadīšanai ietvert vēl tādas darbības kā, piemēram, pārsūtīšana, novirzīšana, ļaunprātīga maršrutēšana, izveidošana u.c. Eksperti šādu viedokli noraidīja, jo atzina, ka izvēlētais modelis ir visplašāk lietotais veids pasaulē, kas apzīmē jēdziena „traucēšana" saturu.[372]

Tāpēc pareizi rīkojas tās valstis, kas pēc iespējas vispārināti formulē konkrētos krimināllikuma pantus, nesaistot tos ar tehnisku darbību aprakstu.

### 3.7. Cēloniskais sakars

Cēloņsakarība. Rietumu krimināltiesību teorijā cēloņsakarību apzīmē ar testu *sine qua non*- ja nebūtu. Tas nozīmē, ka X ir Y rezultāts tikai tad, ja X ir bijis pirms un bez X nevarētu iestāties Y. Šo formulu juridiskajā literatūrā pamato Dz. Fletčers, V. Jegorovs, U. Krastiņš u.c. No iepriekšminētā izriet arī plaši sastopamā cēloņsakarības (*nexus causalis*) definīcija – ka tā ir objektīva saikne starp prettiesisko darbību un to radītajām laika ziņā sekojošām kaitīgajām sekām. Šī teorētiskā definīcija ir piemērojama arī noziedzīgajos nodarījumos pret ISD.

### 3.8.Noziedzīgu nodarījumu pret ISD seku raksturojums

Kaitīgas sekas ir jebkura nodarījuma obligāts priekšnosacījums. To saturu parasti ietver panta dispozīcija. Juridiskajā literatūrā plaši izplatīts viedoklis, ka sekas izpaužas kā kaitējums ar krimināllikumu aizsargātai interesei. Vairāki autori

---

371 The legal framework –unauthorised access to computer systems by Stein Schjolberg // http://www.mosstingrett.no/info/legal.html (aplūkots 2004.gada 20.martā)

372 Committee of experts on crime in cyberspace (PC-CY) Summary report of the 7th Plenary meeting. Restricted PC- CY (2000)11. p.9.

(N. Kuzņecova, U. Krastiņš, A. Naumovs, A. Simesters, G. Sullivans u.c.) uzskata, ka sekām ir jābūt tādām, kas rada izmaiņas apkārtējā vidē, dabā. Neapstrīdot šo tēzi, disertācijā šis jautājums attiecībā pret sekām, kas rodas noziedzīgos nodarījumos pret ISD, ir tulkots plašāk, proti, par izmaiņām apkārtējā vidē nevar atzīt tikai fiziskas, ar aci saskatāmas pārmaiņas dabā izvietotajos priekšmetos, bet terminu „apkārtējā vide" jāattiecina arī uz ar aci neredzamām un netaustāmām parādībām, tāpēc ar izmaiņām tajā ir jāsaprot arī gaiss, kosmoss, elektroniskā vide jeb kibertelpa.

Krimināltiesību teorijā izteikti dažādi viedokļi par seku nozīmi nodarījumos, ko pieņemts saukt par formāliem noziedzīgu nodarījumu sastāviem un materiāliem noziegumu sastāviem. Noziedzīgu nodarījumu iedalījumu materiālos un formālos sastāvos atbalsta V. Liholaja, U. Krastiņš, A. Naumovs, A. V. Kudrjavcevs u.c., tomēr teorijā ir arī citi viedokļi- T. Cereteli, N. Kuzņecova, B. Ņikiforovs, A. Traiņins, u.c. uzskata, ka, šādi dalot noziedzīgus nodarījumus, kaitīgas sekas no obligāta noziedzīga sastāva elementa kļūst par fakultatīvo. Uzskatu, ka dalījums materiālos un formālos noziedzīga nodarījuma sastāvos ir pamatots. Kaitīgo seku saturs ir jāanalizē plašākā un šaurākā kontekstā, t.i., plašākā kontekstā kaitīgās sekas izpaužas visu ar krimināllikumu aizsargājamo interešu kopuma apdraudējumā, bet šaurākā nozīmē tas ir konkrētais kaitējums, kas nodarīts konkrēta noziedzīga nodarījuma rezultātā. Formālos noziedzīgo nodarījumu sastāvos pamatots ir viedoklis, ka pati darbība jau ir sekas, piemēram, 244. panta 1.daļā darbība „vīrusa izplatīšana" jau ir noziedzīgā nodarījuma kaitīgās sekas, respektīvi, darbība un sekas nav nodalāmas. Pārējie Krimināllikuma 241.- 245. pantā ietvertie noziedzīgie nodarījumi atzīstami par materiāliem noziegumu sastāviem, jo šo pantu dispozīcijā likumdevējs ir paredzējis atbildības iestāšanos tikai tad, ja radīsies konkrētas kaitīgas sekas jeb vispirms būs darbība un tad kā darbības rezultāts iestāsies kaitīgas sekas. Jāpiekrīt A. Matvejevai, kura norāda, ka

kibernoziegumu kaitīgumu noteic tieši nevis pati darbība, bet tieši tas kaitējums, kas radies vai varēja rasties šo darbību rezultātā.[373]

Noziedzīgos nodarījumos pret ISD sekas ir dalāmas divās kategorijās:

1. Mantiskās sekas, kas izpaužas konkrētu zaudējumu nodarīšanā sistēmas īpašniekam vai tiesiskajam valdītājam, vai ari datu subjektam. Krimināllikuma (241.-245. pants) pašreizējā redakcijā tās ir paredzētas 241., 243., 245. pantā – būtisks kaitējums.

2. Fiziskās sekas- datu apstrādes sistēmu darbības fiziska sagraušana vai darbības traucēšana.

*Būtiska kaitējuma noteikšanas kritēriji automatizētā datu apstrādes sistēmā*

Likuma "Par krimināllikuma spēkā stāšanās laiku un kārtību" 23. pantā ir teikts:

*(1) Atbildība par krimināllikumā paredzēto noziedzīgo nodarījumu, ar kuru radīts būtisks kaitējums, iestājas, ja noziedzīgā nodarījuma rezultātā, ne vien nodarīts ievērojams mantisks zaudējums, bet arī apdraudētas vēl citas ar likumu aizsargātas intereses un tiesības, vai ja šāds apdraudējums ir ievērojams.*
*(2) Par ievērojamu mantisku zaudējumu atzīstams mantiskais zaudējums, kas nodarījuma izdarīšanas brīdī pārsniedz piecu tai laikā Latvijas Republikā noteikto minimālo mēnešalgu kopumu.*

No iepriekšminētā panta teksta var secināt, ka būtisks kaitējums satur divus kritērijus: 1) mantisko kritēriju, kur noteikts, ka par būtisku var atzīt kaitējumu, ja zaudējumi pārsniedz piecas minimālās mēnešalgas; 2) sociālais kritērijs, ar kuru apzīmēts cita rakstura kaitējums, kas var būt gan morāls, gan var izpausties kaut kādā veidā kā kaitējums ne tikai cietušajam, bet ar to var tikt aizskartas arī citu personu likumiskās intereses. Šo uzskaitījumu varētu turpināt. Diemžēl praksē nereti procesa virzītājs (izņemot lietas par patvaļīgu koku ciršanu- KL 109. pants) nosakot būtisku kaitējumu galvenokārt vadās galvenokārt tikai no mantiskā kritērija. Autors atbalsta ideju, un tas izriet arī no starptautiskiem tiesību aktiem, kas pieņemti kibernoziegumu jomā, ka, lai iestātos krimināLatbildība par nodarījumiem pret informācijas sistēmu drošību, būtiskam kaitējumam ir jābūt kā robežšķirtnei, kas ir par pamatu, lai tiktu ierosināta krimināLvajāšana pret personu,

---

[373] А. А. Матвеева Информационная безопасность и проблемы сцвершенствования уголовного законодательства. Уголовное право в XXI веке. Материалы Международной научной конференции состоявшейся на юридическом факультете МГУ им.М.В. Ломоносова 31 мая- 1 июня 2001г. Москва ЛексЭст 2002 с. 181- 186

kurš veicis tīšas darbības, kas vērstas pret sistēmas pieejamību, konfidencialitāti un integritāti. Taču, manuprāt, jēdzienā „būtisks kaitējums" saistībā ar pētāmo noziedzīgo nodarījumu grupu, saglabājot abu kritēriju nozīmi, ir jāieliek cits materiālais saturs. Šobrīd, ievērojot 23. pantā iekļautos kritērijus, faktiski jebkura patvaļīga darbība, kas vērsta pret ADAS resursu drošību, rada sistēmas īpašniekam zaudējumus vismaz piecu minimālo algu apmērā. Taču pat paši sistēmas īpašnieki tos neuzskata par tik nozīmīgiem, lai vērstos policijā ar lūgumu saukt vainīgo personu pie krimināltatbildības. Tāpēc nereti ne tikai Latvijā, bet arī citur pasaulē daudzi patvaļīgu darbību fakti, kas vērsti pret ADAS resursiem, vispār nenonāk policijas redzeslokā. Lai padarītu efektīvāku pētāmo noziedzīgo nodarījumu apkarošanu, uzskatu, ka līdzīgi kā tas ir izdarīts ar pielikumu meža nodarījumu lietās, šāds pielikums par likuma 23. panta piemērošanu nodarījumos pret ADAS resursiem, jo nākotnē šo nodarījumu skaits ievērojami palielināsies, būtu jāiestrādā minētajā likumā. Tas ievērojami atvieglinātu speciālistu darbu šādu seku noteikšanai. Tāpēc apskatīsim, kritērijus, pēc kādiem varētu tikt veidots šāds pielikums:

1. Materiālais kritērijs. Praksē arvien biežāk nāksies saskarties ar problēmu par mantisko zaudējumu apmēra noteikšanu. Uzskatu, lai maksimāli objektīvi tiesu praksē varētu tikt novērtētas mantiskās sekas saistībā ar noziedzīgiem nodarījumiem pret informācijas sistēmu drošību, lietderīgi būtu izstrādāt un ieviest vienotu zaudējumu noteikšanas metodoloģiju. Tas izslēgtu iespēju, kad cietušais sistēmas īpašnieks par neadekvātiem ieguldījumiem savas sistēmas drošībā un kvalitātē varētu pieprasīt nepamatoti augstu mantisko atlīdzību. Šim nolūkam ierosinu praksē piemērot šādu zaudējumu aprēķināšanas metodi: 1) zaudējumi, kas saistīti ar sistēmas dīkstāvi; 2)izdevumi, kas saistīti ar bojātās informācijas atjaunošanu vai tās aizstāšanu; 3) izdevumi, kas saistīti ar jaunu programmatisku resursu instalēšanu, kas paredzēti sistēmas drošības funkciju atjaunošanai; 4) izdevumi, kas saitīti ar sistēmas lietotāju piekļuves tiesību korekciju. Zaudējumu aprēķinā jānorāda arī sistēmas bilances vērtība, atskaitot amortizācijas izdevumus. Domāju, ka pie būtiska kaitējuma noteikšanas kibernoziegumos, likuma 23. pantā minētais meriālo zaudējumu apjoms no piecām minimālajām mēnešalgām būtu

saglabājams, bet nekādā gadījumā tas nedrīkstētu būt primārais. Kā primāro kritēriju es izvirzītu sociālo kritēriju. Praksē būtu lietderīgi ieviest principu, ka persona nevar pretendēt uz zaudējumu atlīdzību, ja viņš izmantojis nelicenzētus, nelikumīgi iegūtus programmatiskos resursus.

2.Sociālais kritērijs: Strādājot kopš 1997.gada pie jautājumiem, kas saistīti ar nodarījumiem pret informācijas sistēmu drošību, esmu secinājis, ka pamatoti rīkojas tās valstis, kas klasificē savās drošības doktrīnās informācijas sistēmas pēc to apdraudējuma pakāpes bīstamības.

Piemērs. N 2003. gada patvaļīgi piekluva K pilsētas automatizētai datu apstrādes sistēmai, kas regulē pilsētā trauksmes ieslēgšanas signālus iespējamo gaisa uzbrukumu gadījumā. Viņš ievadīja sistēmā speciālu programmu, kas iedarbināja trauksmes signālus plkst. 02.00 naktī, kas izsauca paniku pilsētas iedzīvotājos un specdienestos. Vairāki cilvēki guva smagas veselības traumas un faktiski pilsētas dzīve bija paralizēta uz 12 stundām, kamēr izdevās atrast datorspeciālistu, kas spēja neitralizēt programmas darbību un trauksmes signālu izslēdza.

2004.gada 23. martā N ieslēdzot personīgo datorsistēmu, saņēma paziņojumu, ka viņa sistēmā ir ūdens, un viņš pat dzirdēja ši ūdens skalošanās troksni sistēmblokā. Šīs darbības radīja ta saucamais vīruss viltnieks, ko viņš bija ielādējis kopā ar programmu no interneta. Protams, ka šis vīruss viņam sagadāja zināmu uztraukumu, neērtības, bija jāizsauc speciālists, kas neitralizēja vīrusu, bet šim notikumam nebija sociālās bīstamības, tas neradīja un nevarēja radīt kaitējumu sabiedrības interesēm.

Šie abi piemēri uzskatāmi pierāda to, ka, kaut arī sistēma atbilst automatizētas datu apstrādes sistēmas jēdzienam un arī šāds viltus vīruss var nodarīt sistēmas darbības traucējumus, starp pirmo un otro piemēru pastāv būtiska atšķirība sociālā kaitīguma jomā. Tāpēc vairākas valstis, piemēram, ASV, Vācija, izstrādājot e-vides drošības doktrīnas vai plānus, visas valstī esošās sistēmas iedala četrās grupās:

A. Sistēmas ar ļoti augstu sociālā riska apdraudējuma pakāpi. Pie šādām sistēmām parasti pieskaita tās, kas apstrādā valsts noslēpumu saturošu informāciju, kuru darbības traucējuma vai sagraušanas gadījumā var būt ievērojami apdraudēta valsts politiskā, ekonomiskā drošība.

B. Sistēmas ar augstu apdraudējuma pakāpi. Pie tādām pieskaita tās, kuras apstrādā sabiedrības un valsts funkcionēšanai svarīgu informāciju, piemēram, tādu informāciju, kas saistīta ar energo resursu, valsts finansu sistēmas, centrālo valsts varas aparātu, tiesu sistēmu, prokuratūru, kā arī citas sistēmas, kas nodrošina valstij un sabiedrībai svarīgu funkciju izpildi, bet kuru darbības traucējuma vai

sagraušanas gadījumā var tik nodarīts kaitējums valsts un sabiedrības interesēm. Sistēmas, kas atbilst A. un B. klasifikācijai, lietderīgi būtu atzīst par valsts informācijas sistēmam un ar likumu un citiem likumpamatotiem aktiem noteikt to tiesisko statusu un drošības tehniskās un organizatoriskās prasības.

C. Sistēmas ar ierobežotu apdraudējuma pakāpi. Pie šādām sistēmām parasti pieskaita tās, kas nodrošina informācijas apriti komercdarbības veikšanai konkrētā uzņēmumā. Ja tiek apdraudēti šo resursu drošība, tad no tā parasti cieš ierobežots personu loks, kas atzīti par likumīgajiem šīs sistēmas lietotājiem.

D. Zema riska apdraudējuma sistēmas. Tās atrodas tikai privātpersonu lietošanā, un to darbība tiek pārsvarā izmatota personīgo vajadzību apmierināšanai. Uzbrukuma gadījumā, pat sagraujot šo sistēmu darbību, netiek nodarīts būtisks sociāls kaitējums, bet pamatā kaitējums aprēķināms tikai materiālo zaudējumu veidā. Taču arī šeit sistēmas var vēl sadalīties sīkākās kategorijās, proti, tās, kas sniedz pakalpojumus, un tās, kas tikai saņem pakalpojumus. Protams, ka par šo iedalījumu var diskutēt, taču nevis no tehniskā, bet īpaši no juridiskā viedokļa šo kritēriju noteikšanai tieši seku novērtēšanas gadījumā ir ļoti svarīga nozīme.

Piemērs. Izvērtēšu gadījumu, kad N piekļūst D sistēmas resursiem un ievada tajos kaitīgu ierīci. D sistēmā ir uzinstalēta pirātiska Windows kopija, pirātiska Microsoft Office kopija un dažas datorspēles. Uz pirātiskās Microsoft Ofice kopijas bāzes sistēmas īpašnieks ir izveidojis datu bāzi. Datorvīruss sagrauj šīs sistēmas resursus, tai skaitā arī datu bāzi. Informācija par šo uzbrukumu nonāk policijā, un tai jāuzsāk apstākļu noskaidrošana.

Ja minētajā likumā būs speciāls pielikums, tad policijas darbinieki, vienkārsi varēs attiekties uzsākt izmeklēšanu, jo nodarījumā nav iestājušās likumā paredzētās sekas „būtisks kaitējums", jo pietrūkst šī sociālā kritērija. Savukārt, ja tāds pats uzbrukums būtu noticis informācijas sistēmā, kas nodrošina automatizētu elektroenerģijas piegādi, piem., Rīgai, tad, nenoliedzami, būtiskais kaitējums jau izpaudīsies tikai tajā apstāklī, ka šāds uzbrukums pret sistēmu ir veikts un sekas „sistēmas darbību traucēšana vai sagraušana" ir iestājušās. Dotajā gadījumā ir jārunā par vēl vienu sociālā faktora elementu, proti, nepieciešamību konstatēt, vai darbību rezultātā ir iestājušās arī fiziskas sekas, t.i., drošības sistēmu sagraušana vai būtiska traucēšana.

Fiziskās sekas. Kibernoziegumu konvencijā un ES Padomes Ietvarlēmumā ir skaidri norādīts, ka krimināatbildību ir nepieciešams paredzēt tikai par būtisku

sistēmas darbības traucēšanu. ES Padomes ietvarlēmuma par uzbrukumiem informācijas sistēmām paskaidrojošā memoranda 4.b pants noteic, ka vārda nozīme *serious* ir uzskatāma kā nodarījuma sastāva elements, kam jāparāda šī nodarījuma kaitīgums, taču tas netiek definēts, jo traucēšana var izpausties dažādos veidos. Tā var būt saistīta ar dažāda rakstura uzbrukumiem, atšķirīgiem sistēmu lielumiem, informācijas sistēmas drošības politikas un citiem aspektiem. Tāpēc katrai dalībvalstij ir jānoteic, kāds saturs ir ietverams terminā „nopietns traucējums" *serious hindering* .[374] Autors uzskata, ka šim terminam atbilstošākā nozīme latviešu valodā ir „būtisks sistēmas darbības traucējums".

Sniegt skaidrojumu terminam „būtisks sistēmas darbības traucējums" praktiski nav iespējams, jo tas ir cieši saistīts ar to, kurai sistēmu grupai apdraudētais priekšmets pieder. Ja valsts informācijas sistēmai, tad jebkurš, pat mazākais sistēmas apdraudējums šīm speciāli aizsargātām sistēmām jāatzīst par „būtisku darbības traucējumu". Vienā gadījumā sistēmas darbības būtisku traucējumu var saistīt ar laiku, cik ilgi pastāv šāds traucējums. Taču arī šeit jābūt ļoti uzmanīgiem, jo līdzīgi kā zemestrīce, kas izplatās ar dažādu spēku, tā arī uzbrukumi sistēmu resursiem var tikt veikti ar dažādu spēku un intensitāti. Vienā gadījumā sistēmas darbības traucēšana dažu minūšu garumā var novest pat pie smagām sekām, taču citā pat vairāku stundu darbības traucējumi nekādas būtiskas sekas neradīs.

Izveidojot valstī sistēmu klasifikāciju pēc apdraudējuma pakāpes un piešķirot tai juridisku nozīmi, t.i., iekļaujot to konkrētā normatīvā aktā, likumdevējs dotu iespēju krimināltiesību speciālistiem daudz objektīvāk novērtēt sistēmu darbību traucējuma būtiskuma raksturu, piemēram, ja darbība traucēta A, B. sistēmās, tad jebkurš traucējums atzīstams par būtisku, ja darbība traucēta C sistēmā, tas ir, sistēmās, kas parasti sniedz maksas e- pakalpojumus, tad par būtisku var atzīt sistēmas darbības traucējumu ilgāku par 30 minūtēm, bet, ja apdraudēta sistēma ir D, tad par būtisku atzīstams šādas sistēmas darbības traucējums ilgāk par stundu.

Sistēmas resursu pilnīga vai daļēja darbības pārtraukšana. Nenoliedzami, ka katrs uzbrukums svešai informācijas sistēmai ir nepatīkams un savā veidā

---

[374] Proposal for a Council framework decision on attacks against information system. COM (2002)173 final Explanatory report, p. 19.

kaitējums, taču ne katrs no šādiem apdraudējumiem rada ievērojamu sociālu kaitīgumu. Ja persona tīši ievada sistēmā vīrusu vai citu kaitīgu rīku un tas sabojā, piemēram, vienu failu, tad šis apdraudējums nav bīstams citiem sistēmas lietotājiem, taču, ja tiek sagrauta sistēmas aizsardzība vai ievērojami pavājināta, tad tas patiesībā nozīmē, ka uzbrucējs var pilnīgi pārņemt sistēmu savā kontrolē un neierobežoti rīkoties ar tās resursiem. Tāpēc šāda veida darbības ir ievērojami bīstamākas un arī novērtējamas proporcionāli apdraudējuma pakāpei un sekām. Ja sistēmas īpašnieks objektīvi pierāda, ka uzbrukuma gadījumā ir pilnīgi vai daļēji sagrauta sistēmas resursu darbība, tad šis apstāklis jāsaista ar zaudējumu materiālo aprēķinu. Ja sistēma sniedz citiem lietotājiem maksas pakalpojumus, tad zaudējumu aprēķinā, bez iepriekšminētiem kritērijiem ir jāparedz arī zudušās peļņas aprēķins. Jautājums par sekām saistībā ar noziedzīgiem nodarījumiem pret ISD ir ļoti būtisks, jo sekas šo darbību rezultātā nereti vispār var parādīties otrā pasaules malā, tāpēc praksē jāapzinās, ka šī objektīvās puses elementa konstatēšana, izvērtējot konkrēto noziedzīgo nodarījumu, var būt ļoti problemātiska.

Izdarot kopsavilkumu par iepriekšteikto, uzskatu, ka likuma „Par krimināllikuma spēkā stāšanās laiku un kārtību" 23. panta piemērošanu saistībā ar kibernoziegumiem būtisko seku noteikšanā būtu jāvadās no šādiem kritērijiem:

1. Primārais -sociālais kritērijs, kas ietver sevī sistēmas klasifikāciju pēc apdraudējuma pakāpes. Šim nolūkam būtu ieteicams papildināt Nacionālās drošības koncepciju ar Latvijas teritorijā esošu ADAS sistēmu klasifikāciju pēc to sociālās nozīmības un apdraudējuma pakāpes. Atbilstoši apdraudējuma pakāpei likuma pielikumā norādīt, ka par būtisku sistēmas darbības traucējumu (izņemot valsts informācijas sistēmas) atzīstams gadījums, kad sistēmas resursu darbības traucēšana tiek veikta ilgāk par pusstundu. Valsts informācijas sistēmās jebkurš sistēmas darbības traucējums atzīstams par būtisku.

2. Sekundārais – materiālais kritērijs- zaudējumu apmērs, nosakāms, piemērojot iepriekšminēto metodiku: 1) zaudējumi, kas saistīti ar sistēmas dīkstāvi; 2) izdevumi, kas saistīti ar bojātās informācijas atjaunošanu vai tās aizstāšanu; 3) izdevumi, kas saistīti ar jaunu programmatisku resursu instalēšanu, kas paredzēti sistēmas drošības funkciju atjaunošanai; 4) izdevumi, kas saitīti ar sistēmas lietotāju

piekļuves tiesību korekciju; 5)neiegūtā peļņa, ja sistēma sniedz maksas informācijas pakalpojumus. Zaudējumu aprēķinā jānorāda arī sistēmas bilances vērtība, atskaitot amortizācijas izdevumus. Uzskatu, ka aprēķinot zaudējumus, ir svarīgi ievērot tā saucamo „puvušā koka" (*poison tree*) principu, proti, ka gadījumos, kad cietušais izmantojis nelicenzētu programmatūru, viņam nav tiesību prasīt zaudējumu atlīdzību, nelikumīgu darbību pret sistēmu gadījumā, jo persona izmantojot savu interešu apmierināšanai nelikumīgi iegūtus programmatiskos resursus, nevar pretendēt uz likumīgu savu interešu aizskāruma novēršanu. No puvuša koka nav iespējams iegūt veselus augļus. Tas attiecināms uz jebkuru zaudējumu noteikšanas kārtību, izņemot gadījumus, ja iestājušās smagas sekas.

*Zaudējumi lielā apmērā*

Krimināllikuma 243. panta 2.daļā paredzēta atbildība par automatizētās datu apstrādes sistēmas darbības apzinātu traucēšanu, ievadot, pārnesot, bojājot, izdzēšot, pasliktinot, izmainot vai aizklājot informāciju, ja ar to tiek bojāta vai iznīcināta aizsardzības sistēma vai nodarīti zaudējumi lielos apmēros,-

Piemērs. Kaitīgās programmas "Melisa" izgudrotājs un izplatītājs D. Šmits tika atzīts par vainīgu 80 miljonu dolāru zaudējumu nodarīšanā[375], Ukrainas hakeris M. Kovaļčuks 2003. gada tika apcietināts Bangkogā un viņam izvirzīta apsūdzība par zaudējumu nodarīšanu dažādām ASV datorfirmām par 100 miljoniem USD.[376]

Šis piemērs uzskatāmi parāda, ka veicot tīšus uzbrukumus automatizētam datu apstrādes sistēmām, bieži vien noziedznieki tos veic ar nolūku iegūt sistēmā esošos naudas resursus vai informāciju, kas dod pieeju tiem, vai piekļūstot sistēmas lietotāju failiem, vai tieši noņemot naudu no banku kontiem. Ne velti salidzinājumam tiek minēts iespaidīgs skaitlis, ka ASV vidēji banku laupītāja ieguvums laupīšanas procesā ir apmēram 2000 USD, bet personas, kas nodarbojas ar elektronisko laupīšanu, vidēji iegūst katrā reizē pelņu apmēram 200 000 USD. Tādējādi visā pasaulē izvirzīti jautājumi, ka ir jāpastiprina atbildība gadījumos, ja nodarījumi pret sistēmu drošību ir veikti mantkārīgu tieksmju dēļ un nodarīti zaudējumi lielos apmēros.

---

375 Slot Machine Justice for Melissa Author by Mark Rash// http://www.securityfocus.com/columnists/81 (aplūkots 2004.gada 12. martā)

376 Голубев В.Типология преступлений в сфере использования ЭВМ// http://www.crime-research.ru/library/Golubev1203.html (aplūkots 2004.gada 20.martā)

Likuma „ Par krimināllikuma spēkā stāšanās laiku un kārtību" 20.pants noteic:

*Atbildība par Krimināllikumā paredzēto noziegumu, kas izdarīts lielā apmērā, iestājas, ja nozieguma priekšmeta kopējā vērtība nodarījuma izdarīšanas brīdī nav bijusi mazāka par piecdesmit tai laikā Latvijas Republikā noteikto minimālo mēnešalgu kopsummu.*

Darba grupa, izstrādājot grozījumus Krimināllikumā nolūkā sakārtot mūsu krimināllikumu atbilstoši starptautisko normatīvo aktu prasībām, atzina, ka nepieciešams iekļaut likumā pastiprinātas atbildības nosacījumu, ja patvaļīgās piekļuves vai datu vai sistēmas darbība traucēšana vai iznīcināšana veikta mantkārīgos nolūkos vai arī nodarīti zaudējumi lielos apmēros. Kāpēc šāds risinājums? Šāda pieeja galvenokārt balstīta uz diviem principiem: 1) atbildībai par darbībām, kas veiktas elektroniskā vidē ir jābūt līdzvērtīgai tai, ja šādas darbības tiktu veiktas reālā vidē (*mutantis mutandis*); 2) šādas prasības izvirza arī Eiropas Savienības Padomes ietvarlēmums par uzbrukumiem informācijas sistēmām, lai pēc iespējas tuvinātu visu Eiropas Savienības valstu krimināllikumus. Iekļaujot projektā atbildības nosacījumu – „lieli apmēri", ir skaidrs, ka seku noteikšanā primārais ir materiālais kritērijs, tas personai, kurai nodarīti zaudējumi, jāpierāda, ka tie pārsniedz piecdesmit tai laikā noteikto minimālo mēnešalgu kopsummu.

*Smagas sekas*

Domājot par jauniem noziedzīgiem nodarījumiem, kas vērti pret informācijas sistēmām, autors uzskata, ka šo noziedzīgo nodarījumu izplatība, izdarīšanas veids izvirza nepieciešamību, lai smagas sekas atzītu par šī nodarījuma kvalificējošo pazīmi. Lai pierādītu šīs kvalificējošās pazīmes nepieciešamību autors izmantos šādu piemēru:

2003. gadā kaitīgā programma *Slammer* tikpat kā pilnīgi nogrāva kādas nacionālas bankas bankomātu sistēmām, *Sobig* programma sagrāva ASV Austrumu krasta pasažieru un kravu pārvadāšanas satiksmi un kavēja Kanādas lidmašīnu biļešu rezervācijas sistēmu.[377]

Smagas sekas ir definētas Likuma par Krimināllikuma spēkā stāšanās un piemērošanas kārtību 24. pantā:

*Atbildība par Krimināllikumā paredzēto noziedzīgo nodarījumu, kas izraisījis smagas sekas, iestājas, ja noziedzīgā nodarījuma rezultātā izraisīta cilvēka nāve,*

---

[377] Risk management solutions: Response to cyber threats and cyberterrorism// http://www.insurancejournal.com/magazines/west/2004/02/23/features/37008.htm (aplūkots 2004.gada 23.februārī)

*nodarīti smagi miesas bojājumi vai psihiskas dabas traucējumi vismaz vienai personai, mazāk smagi miesas bojājumi vairākām personām, mantiskais zaudējums lielā apmērā vai radīts citāds smags kaitējums ar lik u mu aizsargātām interesēm un tiesībām.*

1995. gadā ASV Aizsardzības ministrija organizēja eksperimentu ar nosaukumu "*Diena pēc...*". 1995. gada janvārī – jūnijā ministrija simulēja *informācijas karu*[378]. Modeļa pamatā bija imitēts tāds konflikts starp ASV un kādu ārvalsti, kam jānotiek 2000. gadā. Scenārijā bija paredzēts, ka pretinieks uzbrūk vienlaikus visām ASV un tās sabiedroto valstu informācijas sistēmām. Uzbrukumu dēļ notiek katastrofas, nelaimes gadījumi, pilnīgi tiek paralizēti sakari, radīta panika iedzīvotāju vidū. Piemēram, uzbrukumi tika vērsti pret ASV lielākajām bankām, kā dēļ tūkstošiem dolāru nelikumīgi tiek noņemti no bankas klientu kontiem, bet citiem, savukārt, tie ieskaitīti. Dzelzceļa datorsistēmā iesūtītā loģiskā bumba noteiktā laikā paralizēja sistēmas darbu, tāpēc Merilendā notika ātrgaitas pasažieru vilcienu sadursmes. Tā kā Vašingtonā tika bloķētas vairākas informācijas sistēmas, notika Lielbritānijas lidmašīnas katastrofa, Kairā tika bloķēti visi palīdzības dienesti. Uzbrukumi bija speciāli vērsti pret ASV un satelītvalstu militāro iestāžu datorsistēmām, un tās tika izsistas no ierindas. Tika izsistas no ierindas precīzās raķešu un citu tālvadības ieroču tēmēšanas sistēmas, tās nevarēja efektīvi darboties pret ienaidnieka tankiem un karaspēku.[379]

Minētā eksperimenta galvenais uzdevums bija atklāt informāciju sistēmas drošības vājās vietas. Ir pilnīgi skaidrs, ka pilnīgu informācijas sistēmu drošību nav iespējams panākt. To pierāda iepriekšminētā eksperimenta galarezultāti. To, ka šādi apdraudējumi, īpaši valstīs ar augstu tehnoloģisko potenciālu, ir iespējami, pierāda reālā dzīve. Iepriekšminētajā ziņojumā norādīts, ka ASV Pentagona datorsistēmām, pēc Aizsardzības Informācijas drošības aģentūras (DISA) ziņām, 1995. gada laikā

---

[378] Informācijas karš – darbības, kas vērstas uz to, lai sasniegtu informācijas pārākumu un nacionālās militārās stratēģijas atbalstu, iedarbojoties uz pretinieka informāciju un informācijas sistēmām un tajā pašā laikā pastiprinot savas informācijas un informāciju sistēmu aizsardzību. What is information warfare http://www.tangle.seas.gwu.edu/~reto/inforwar/what/htm ( aplūkots 2000.gada 29.decembrī.).

[379] Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Chapter Report, 05/22/96, GAO/AIMD–96–84), sk. http://www.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=wais.access.gpo.gov&filename=ai96084.txt&directory=/diskb/wais/data/gao (aplūkots 2000.gada 29. februārī).

notikuši līdz 250 000 uzbrukumu, no kuriem 65% bijuši veiksmīgi. Aģentūras ziņojumā norādīts, ka šādu iebrukumu skaits ar katru nākamo gadu dubultojas.

Iepazīstoties ar šo informāciju, atmiņā nāk kādā kibernoziegumu eksperta teiktais, ka valstīs, kur visa ekonomika, politika un sadzīve ir atkarīga no informācijas un komunikācijas tehnoloģiju darbības, noziedznieks ar tastatūras palīdzību 5 minūšu laikā var iznīcināt valsts ekonomiku un radīt īstu paniku valsts iedzīvotājos. Iepriekš minētais eksperiments, kas atgādina Holivudā uzņemto grāvēju "*Dienu pēc..*", kur šādas sekas bija parādītas pēc atomuzbrukuma Amerikai, apliecina, ka plašus kaitējumus, katastrofas var radīt ne tikai ar atombumbu, bet arī lietojot informāciju tehnoloģijas.

Par lielu nelaimi ASV daļa no šajā eksperimentā konstatētajiem faktiem guva savu apstiprinājumu teroristiskajā uzbrukumā Ņujorkas Pasaules tirdzniecības centra debesskrāpjiem un Pentagonam Vašingtonā, kas notika 2001. gada 11. septembrī. Šo noziegumu izmeklēšanas procesā noskaidrots, ka teroristu nolaupīto lidmašīnu darbības bija cieši saskaņotas ar hakeru iebrukumiem lidostu un NASA informācijas sistēmās, kā arī saistītas ar sekmīgu kriptogrāfisko tehnoloģiju izmantošanu, kas liedza ASV specdienestiem iegūt nepieciešamo informāciju par plānotajiem terora aktiem. Speciāli izveidota domēnu vārdu sistēma regulāri deva iespēju teroristiem sazināties konkrētajās interneta adresēs, kā, piemēram, www.worldtradecentrebombing.com un citās, kur informācija tika sagatavota pat astoņās valodās. Šādi izveidota mājaslapu sistēma deva iespēju teroristiem globāli apmainīties ar nepieciešamo informāciju un koordinēt savas noziedzīgās darbības.[380] To, ka iepriekšminētā eksperimenta iedomātās sekas XXI gadsimtā var kļūt par realitāti, pierāda ASV specdienestu un datorsistēmu ekspertu uzsāktie pētījumi, kas liecina, ka teroristu rīcībā nonāk visi jaunākie tehnoloģiju sasniegumi, tajā skaitā arī informācijas tehnoloģijas. Tāpēc ir reāla iespēja, ka teroristi savu uzbrukumu var veikt ar datorsistēmu palīdzību. Kā norāda bijušais ASV Nacionālās Infrastruktūras aizsardzības centra direktors Vatis, tad kiberuzbrukumam ir

---

[380] sk. FBI Investigates Web Domains Suspicious Names Registered Before Attack // http://abcnews.go.com/sections/scitech/TechTV/techtv_domains010921.html (aplūkots 2001.gada 25.septembrī).

vajadzīgs viens cilvēks un klēpja dators.[381] Sevišķi domājot par tādiem jauna veida apdraudējumiem kā pakalpojumatteices uzbrukumi, kur vienlaicīgi var tikt iesaistīti pat vairāki tūkstoši datorlietotāju, likumdevējam ir lietderīgi arī krimināllikumā kā atbildības nosacījumu paredzēt gadījumu, kad var iestāties smagas sekas, kas var būt saistītas gan ar cilvēku upuriem, gan materiālo zaudējumu nodarīšanu lielos apmēros vai var tikt nodarīts cits smags kaitējums ar likumu aizsargātām tiesībām un interesēm. Var rasties jautājums, kā traktēt nosacījumu: „cits smags kaitējums ar likumu aizsargātām interesēm un tiesībām". Domāju, ka šeit var izmantot tos pašus principus ko saturiski skaidrojot „būtisku kaitējumu", taču, protams, ka saturiskām sekām šeit ir jābūt smagākām, kā vērtējot būtisku kaitējumu. Šādam nolūkam var izmantot to pašu sistēmu klasifikācijas modeli pēc apdraudējuma pakāpes, vērtēt uzbrukuma plašumu. Piemēram, ja šāda uzbrukuma rezultātā tiek traucēta normāla lidmašīnas pacelšanās uz 30 minūtēm, tās arī jau būtu atzīstamas par smagām sekām, jo smagi cieš visu lidmašīnas pasažieru likumīgās intereses, piemēram, apdraudētas ir viņu tiesības laikā nokļūt uz nākamo lidmašīnu, kas savukārt var radīt citu interešu apdraudējumu. Acīm redzot izsmeļošu recepti šeit iedot nav iespējams, taču, ja tādi gadījumi praksē būs, tad galvenais kritērijs, protams, būs cilvēku bojā ejā, sakropļošana, psihisku traucējumu radīšana. Tieši šim mērķim arī darba grupa izvēlējas abu seku iekļaušanu projektā gan „lielos apmērus" gan „smagas sekas".

### 4. Noziedzīgā nodarījuma subjekts

Juridiskajā literatūrā faktiski pastāv salīdzinoši liela vienprātība, ka noziedzīgā nodarījuma subjekts ir pieskaitāma, Krimināllikumā paredzētu vecumu sasniegusi persona, kas vainojama noziedzīgā nodarījumā. Tādējādi, lai personu varētu saukt pie krimināltatbildības, tai obligāti jāpiemīt šādām pazīmēm: 1) tai ir jābūt fiziskai personai; 2) viņai jābūt sasniegušai14 gadu vecumu ( KL 11.pants); 3) personai jābūt pieskaitāmai, tas ir, personai ir jāspēj saprast savas darbības un jāspēj tās vadīt; 4) personai ir jābūt tādai, kuras uzvedība ir aizliegta vai ierobežota

---

[381] U.S. networks run big risk of cyber-strikes, experts assert// http://www.siliconvalley.com/docs/news/depth/cyber100101.htm# (aplūkots 2001.gada 25.septembrī).

krimināllikumā. Trūkstot kādai no šīm pazīmēm, persona nevar tikt atzīta par noziedzīgā nodarījuma subjektu.

### 4.1.Subjekts- fiziska persona

Lielākā daļā pasaules valstu krimināllikumos un krimināltiesību teorijā par noziedzīgā nodarījuma subjektu atzīst fizisku personu. A. Naumovs pamatoti norāda, ka noziedzīgā nodarījuma subjektu nedrīkst jaukt ar noziedzīgu personību, jo ne katra persona var būt par subjektu, bet noziedzīga personība ir daudz plašāks termins, un to savā pētniecībā izmanto kriminologi.

ASV krimināltiesību doktrīnā[382] par subjektu runā plašākā nozīmē, attiecinot to uz jebkuru cilvēku neatkarīgi, no tā, vai persona ir pieskaitāma vai ne un sasniegusi noteikto vecumu. Taču tos atbrīvo no krimināatbildības. Kā minēts iepriekš, tad subjektu- fizisku personu raksturo divas galvenās pazīmes: 1) vecums un 2) pieskaitāmība.

*Vecums*

A. Naumovs[383] ar vecumu apzīmē precīzas dzīves koordinātas- nodzīvotā laika daudzumu. Viņš norāda, ka izšķir šādus vecuma noteikšanas kritērijus: 1) vecums pēc pases – hronoloģiskais vecums; 2) bioloģiskais vecums- funkcionālais; 3) sociālais – civilais; 4) psiholoģiskais- psihiskais. Vecuma noteikšana krimināltiesībās raksturo personas spēju saprast un novērtēt savas darbības, tikai tad personu var saukt pie krimināatbildības. Jāpiezīmē, ka jautājumā par personas vecumu, ar kuru iestājas krimināatbildība, pasaulē nav vienotības. Autors 1996.gadā piedalījās Londonā konferencē "*Children who kill*" un bija pārsteigts, ka Lielbritānijā par smagiem noziegumiem pie krimināatbildības var saukt personas no 10 gadu vecuma, bet Skotijā no 8 gadu vecuma. Tomēr tiesu prakse vienmēr, izskatot šis lietas, ir vadījusies no tā, vai nepilngadīgā darbībās saskatāmas *actus reus* un *mens rea*, kā arī bērna apzināšanās, ka viņš izdarījis smagu noziegumu.

ASV pieņemts uzskatīt, ka personu var saukt pie krimināatbildības, ja tā sasniegusi 14 gadu vecumu, tomēr jautājums nav atrisināts valsts mērogā, jo katrai

---

382 Ibid., Флетчер Дж. Наумов А.В. с.125

383 Наумов А. В. Уголовное право. Общая часть. Учебник для вузов. Москва:М· Инфра, 1997.,с.169-171

pavalstij ir likumdevēja tiesības, un, kaut gan pastāv prezumpcija, ka par 14 gadiem jaunāka persona nav spējīga izdarīt noziegumu, tomēr to var noliegt pierādījumi, ka subjekts sapratis, ko dara un ka tas, ko dara, ir nepareizi. Kā precīzi norāda vairāki ASV bērnu tiesību aizstāvji, tad šādu krimināls nespējas prezumpciju parasti ievēro pret 7 gadu vecuma bērniem, bet gadījumos, ja noziedzīgas darbības izdarījuši vecāki bērni, tiesa var atteikties no šādas prezumpcijas un piemērot pret nepilngadīgo krimināls odu.

Francijā[384] par nozieguma subjektu var tikt atzīta gan fiziska, gan juridiska persona. Subjekts netiek atzīts par nozieguma sastāva elementu, tāpēc plaši pētījumi Francijas krimināltiesību teorijā netiek veikti, un fiziskās personas vecuma elements, pieskaitāmība, tiek apskatīta kā noziedzīgā nodarījuma morālais elements. Kaut arī Francijas Sodu likums tieši nav noteicis vecumu, ar kuru iestājas krimināl atbildība, tomēr likumdevējs ir izdalījis trīs subjektu vecuma grupas : 1) nepilngadīgie, kas nav sasnieguši 13 gadu vecumu. Šīs grupas personām nevar piespriest krimināls odu; 2) personas vecumā no 13 līdz 16 gadiem. Šai grupai arī var piemērot tā saucamo krimināls neatbildības (*презумпция уголовной неответственности*) prezumpciju un piemērot audzinoša rakstura līdzekli. Tomēr ir gadījumi, kad, ja nodarījuma apstākļi un vainīgā persona to prasa, piemēro arī kaut kādu krimināls odu; 3) personas vecumā no 16- 18 gadiem. Arī pret tām var tikt piemērota krimināls neatbildības prezumpcija, bet tāpat tās var tikt atzītas par vainīgām un notiesātas.

Vācijas Sodu likums un Itālijas Sodu likums līdzīgi kā Krimināllikums par subjektu atzīst 14 gadu vecumu sasniegušu, pieskaitāmu[385] personu.

Japānā par nozieguma subjektu atzīt tikai fizisku personu. Ja nodarījumus izdarījušās personas ir no 14 līdz 20 gadu vecumam, šādas lietas tiek skatītas ģimenes tiesās saskaņā ar likumu par nepilngadīgiem. Krimināl rakstura sodus nevar piemērot personām jaunākām par 16 gadiem.

---

[384] Уголовное право зарубежных стран. Общая часть. Под . ред. Проф. И.Д. Козочкина. Москва: Омега Л,2003.,с.299-306

[385] Ibid., Уголовное право зарубежных стран. Общая часть с.388, 525

V. Liholaja, pētot krimināLatbildības pamatus Spānijā, secinājusi, ka Spānijas KL 20. pants paredz vispārējo krimināLatbildību no 18 gadu vecuma, bet līdz tam personām tiek piemērota nepilngadīgo atbildības nosacījumi.[386]

Iepriekšminētā analīze pierāda, ka pasaulē un pat Eiropā nav vienotas pieejas noziegumu subjektu vecumam. Teorētiskā plāksnē tas, protams, nerada lielas problēmas, jo katrai valstij ir suverēnas tiesības pieņemt savus krimināllikumus. Taču problēmas ar nozieguma subjektu vecuma kritēriju kā krimināLatbildības pamatu radīsies tad, ja, piemēram, 12 gadu vecs datormīļotājs no Latvijas patvaļīgi iekļūs kādas valsts informācijas sistēmā un šajā valstī likums atļaus saukt pie krimināLatbildības bērnus no 11 gadu vecuma, un persona var kļūt par duālās jurisdikcijas subjektu.

*Pieskaitāmība*

Krimināltiesību teorijā un praksē piemēro nozieguma subjekta pieskaitāmības prezumpciju. Pieskaitāmību parasti nenosaka, bet gan prezumē, ka cilvēks, kas ir sasniedzis krimināltiesību subjekta vecumu, izdarot noziedzīgo nodarījumu, ir apzinājies savu darbību raksturu, spējis tās vadīt un novērtēt sasniegto rezultātu. Nepieskaitāmība jebkurā gadījumā ir fiziskas personas garīga anomālija.

Krimināllikuma 13. panta 1.d. noteic, ka, „.. pie krimināLatbildības nav saucama persona, kas nodarījuma izdarīšanas laikā atradusies nepieskaitāmības stāvoklī, tas ir, psihisko traucējumu vai garīgās atpalicības dēļ nav varējusi saprast savu darbību un to vadīt."

Likumdevējs skaidri un precīzi ir formulējis tās pazīmes, kas raksturo personas nepieskaitāmību, proti, nespēja saprast savu darbību un vadīt savu uzvedību. Š. Dando norāda, ka Japānā Sodu likuma 39.p. garīgās nenormālības apzīmēšanai izmanto divus terminus - saprāta zudums (*loss of mind*) un saprāta vājums (*weakness of mind*). Abi šie stāvokļi raksturo prāta spējas vai atbildību.[387] Taču daudzu valstu krimināltiesībās pieskaitāmības kritēriji nav definēti, kaut gan tie, atzīstot personu par garā slimu, ir pamats viņa atbrīvošanai no krimināLatbildības.

---

[386] Liholaja V. KrimināLatbildība Spānijā un Latvijā. Rīga: Latvijas Vēstnesis, 2003., 9. lpp.

[387] Ibid., Shigemitsu Dando p. 141

U. Krastiņš un daudzi citi autori nepieskaitāmībai izdala divus kritērijus: 1) juridisko kritēriju, kas izpaužas personas nespējā saprast savu darbību un vadīt to; 2) medicīnisko jeb bioloģisko, ar ko saprot psihiskas slimības un garīgu atpalicību.[388] Autors uzskata, ka šajā problēmā nav nepieciešams iedziļināties, jo līdzīgu viedokli ir izteikuši daudzi autori, un faktiski par to, kas raksturo subjektu - fizisku personu, nav domstarpību. Daudz problemātiskāks jautājums ir, vai nozieguma subjekts var būt juridiska persona.

### 4.2. Juridiskās personas atbildība

Tradicionāli krimināltiesībās ar nozieguma subjektu mēs saprotam tikai fizisku personu, jo tas izriet no vainas kā cilvēka subjektīvās attieksmes pret nodarījumu principa. Šādu viedokli atbalsta lielums lielais vairākums krimināltiesību speciālistu.

Tomēr jautājums nav tik skaidrs, jo Latvija ir ES dalībvalsts. Tas mums uzliek noteiktas saistības harmonizēt savu likumdošanu atbilstoši ES prasībām. 2002. un 2001. gadā ir pieņemti vairāki ES normatīvie akti, kas noteic dalībvalstīm pienākumu paredzēt juridisko personu krimināatbildību. Kaut gan krimināltiesību teorētiķi kategoriski iebilst pret šādu praksi, jo tradicionāli Latvijas krimināatbildības pamats vienmēr ir bijusi vaina kā cilvēka subjektīvās attieksmes izpausme pret viņa nodarījumu.[389], tomēr vairāki ES normatīvie dokumenti uzliek dalībvalstīm par pienākumu paredzēt juridisko personu atbildību.

Kā redzams no ES *Corpus Juris* ieviešanas salīdzinošā pētījuma[390], tad pašreizējās ES dalībvalstis jautājumā par juridisko personu krimināatbildību var iedalīt trīs grupās: 1)Francija, Īrija, Nīderlande, Apvienotā Karaliste, Beļģija, kur likums tieši paredz juridisko personu krimināatbildību; 2) Grieķija un Itālija, kas neatzīst šādu atbildības veidu un uzskata, ka šādas atbildības paredzēšana varētu radīt konstitucionāla rakstura problēmas; 3) Vācija un Austrija, kas neatzīst šāda veida atbildību. ES priekšlikums Padomes ietvarlēmuma COM (2002)173 final

---

388 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 79.lpp.

389 Turpat, Krastiņš U., 77.lpp.

390 The implementation of the Corpus Juris in the member states vol.1. Prof. M.Delmas- Marty ,Prof.J.A.E.Vervaele (eds) Antwerpen-groningen-Oxford- Intersentia, 2000., p. 134

*(attacks against information system)* par uzbrukumiem informācijas sistēmām 9. pants noteic, ka dalībvalstīm juridisko personu atbildības pamats jākonstruē tā, lai tās līdz 2003.gada decembrim ietvertu krimināLo vai civiltiesisko atbildību par patvaļīgu piekļūšanu informācijas sistēmas resursiem, darba traucēšanu, kaitīgu ierīču apriti, nelikumīgu pārtveršanu un svešas identitātes izmantošanu internetā. Savukārt ES ietvarlēmumā (2001)413 JHA *combating fraud and counterfeiting of non-cash means of payment* (par krāpšanas un viltošanas apkarošanu bezskaidras naudas norēķinos) 7. pants noteic, ka dalībvalstīm jāveic pasākumi, lai līdz 2003.gada jūnijam nodrošinātu juridisko personu atbildību par apzinātu maksāšanas līdzekļu viltojumu, datorkrāpšanu, krāpšanu, viltošanu, izmantojot šim nolūkam speciāli sagatavotas ierīces. Ietvarlēmumā 7.pantā norādīts arī juridiskās personas atbildības pamats, ja :1) nodarījumu izdarījusi persona, kam ir uzņēmuma pārstāvības tiesības; 2)amatpersona pieņem lēmumus juridiskās personas vārdā; 3) amatpersona īsteno kontroli juridiskās personas iekšienē; 4) iesaista citas personas noziedzībā nodarījumā.[391]

(2001) 413 JHA lēmumā 8.p. satur ieteicamās sankcijas pret juridiskām personām: 1) naudas sods; 2) juridisko personu izslēgšana no tiesībām saņemt sabiedrisku atbalstu un palīdzību; 3) terminēta juridiskās personas darbības pārtraukšana; 4) juridiskās uzraudzības noteikšana; 5) lēmums par uzņēmuma likvidāciju.

Arī Kibernoziegumu konvencijas, kurai Latvija gatavojas pievienoties, 12.pants "Korporatīvā atbildība" noteic, ka dalībvalstīm jāveic tādi likumdošanas un citi pasākumi, kas nepieciešami juridisko personu saukšanai pie atbildības par konvencijā paredzētiem noziegumiem, ja tie veikti juridisko personu interesēs. Minētā panta 4.punkts noteic, ka šādai atbildībai jābūt pieņemtai bez aizspriedumiem par juridisko personu krimināLatbildību.[392]

Minētās konvencijas paskaidrojošā memorandā 124.punktā izskaidrots, lai iestātos juridisko personu atbildība, ir nepieciešami četri nosacījumi: 1) jābūt

---

[391] EJ I 149/3 2.06.2001.

[392] Convention on cybercrimes.Budapest 23 XI 2001// http://conventions.coe.int/Treaty/EN/cadreprincipal.htm (aplūkots 2003.gada 11. decembrī)

izdarītam kādam no konvencijas 2.- 10. pantā- paredzētajiem noziegumiem; 2) noziegumam ir jābūt veiktam juridiskās personas interesēs; 3) noziegums (ieskaitot atbalstīšanu un uzkūdīšanu) ir jāveic augsta stāvokļa amatpersonai -fiziskai personai, kas ieņem juridiskā personā vadošu amatu, kā, piemēram, direktoram; 4) personai, kas ir augsta stāvokļa juridiskās personas amatpersona, jādarbojas sava pilnvarojuma ietvaros, jābūt apveltītai ar: a) pilnvarām pārstāvēt juridisko personu, b) tiesībām pieņemt lēmumus un kontrolēt to izpildi. 125. punkts savukārt izskaidro, ka juridisko personu atbildību var piemērot arī tad, ja noziegumu nav izdarījušas juridiskās personas vadošas amatpersonas, bet arī citas personas ar juridiskās personas pilnvarojumu. Šajā gadījumā atbildība var iestāties arī par nodarījumiem, kas radušies amatpersonu nepietiekamas kontroles rezultātā. Tomēr eksperti norāda, ka ar šādu kontroli nav jāsaprot vispārējs darbinieku saziņas līdzekļu kontroles režīms. [393] Minētā dokumenta 126. punkts pieļauj dalībvalstīm elastīgu pieeju šī jautājuma risināšanā, norādot, ka tā var būt krimināla, civila vai administratīva atbildība, ieskaitot monetāras sankcijas, bet tai jābūt efektīgai, samērīgai un ietvertai likumā.

Francija ir viena no valstīm, kurā vēsturiski bija paredzēta dažu veidu juridisko personu (asociāciju, korporāciju, universitāšu biedrību un pat pilsētu kā īpašu cilvēku apvienību) krimināatbildība. Pret juridisko personu atbildību arī Francijā sākotnēji bija izvirzīti tie paši argumenti, kas Latvijā[394]: 1) juridiskā persona darbojas ar savu pārstāvju starpniecību, ka nodarījumam nevar būt morālā elementa, tas ir, juridiska persona nevar izdarīt vainojamu noziedzīgu nodarījumu; 2) personiskās atbildības princips un atbildības un soda individualizācijas princips; 3) trešais iebildums saistīts ar juridisko personu sodīšanu. Tomēr Francijas Sodu likums paredz juridisko personu atbildību gan "tīrā veidā", gan vienlaicīgi ar juridisko personu pilnvarotām fiziskām personām (Sodu likuma 121-2.p.). Kā norāda[395]juridisko personu krimināatbildības oponenti, šeit var rasties jautājums

---

393 Convention on cybercrime (ETS. No 185) Explanatory report// http://conventions.coe.int/Treaty/EN/cadreprincipal.htm (aplūkots 2003.gada 21. decembrī)

394 Turpat, Krastiņš U.,77.lpp.

395 Уголовное право зарубежных стран. Общая часть. Под . ред. Проф. И.Д. Козочкина. Москва: Омега Л,2003.,с.306-314

par *ne bis in dem* – nevar sodīt divreiz par vienu pārkāpumu, tomēr Francijas juristi uzskata, ka tas, ka vienlaicīgi atbild gan fiziska, gan juridiska persona, nepārkāpj šo principu. Francijā juridisko personu atbildība pamatojas uz diviem kritērijiem: noziedzīgam nodarījumam ir jābūt paveiktam:1) juridiskās personas labā; 2) ar tā vadītāja vai pārstāvja starpniecību. Paveiktam juridiskās personas labā nozīmē, ka juridiskā persona no attiecīgā nodarījuma, piem., krāpšanas internetā, gūst materiālu vai cita rakstura labumu. Obligāts atbildības priekšnoteikums, ka nodarījums jāveic vai nu juridiskās personas vadītājam vai pilnvarotai personai. Ja nodarījumu juridisko personu labā veic tehniskie darbinieki, apkalpojošais personāls, kas nav uzskatāmi par juridiskās personas pilnvarotiem pārstāvjiem, šāda atbildība neiestājas. Kā pētījumā norāda autori[396], tad Francijas tiesu praksē ir sastopami tikai daži spriedumi, kur juridiskās personas notiesātas par nelegāla darbaspēka izmantošanu, par nelaimes gadījumu darbā, kur cietušais zaudēja 100% darba spēju, un par preču viltojumu. Zīmīgi ir tas, ka neviens no tiesas spriedumiem nesatur motīvu daļu, tikai kailu fakta konstatāciju, un visos gadījumos piespriests naudas sods. Jāatzīmē, ka Francijā juridiskās atbildības institūts ir veidojies ļoti ilgā laikā. Latvija izvēlējās savu juridisko personu krimināatbildības modeli To ierosināja profesors U. Krastiņš. Galvenā projekta būtība: neatzīt juridisko personu par krimināltiesību subjektu, taču likumā iestrādāt mehānismu, ka pret to var piemērot piespiedu krimināltiesiska rakstura līdzekļus. 2005.gada 5. maijā[397] Saeima pieņēma darba grupas izstrādātos priekšlikumus un izdarīja Krimināllikumā šādus grozījumus:

Krimināllikuma 12.pantu izteica šādā redakcijā „Fiziskās personas kā publisko tiesību juridiskās personas pārstāvja atbildība"

Par noziedzīgu nodarījumu publisko tiesību juridiskās personas lietā atbild tā fiziskā persona, kura šo nodarījumu izdarījusi kā attiecīgās juridiskās personas pārstāve vai tās uzdevumā, vai būdama juridiskās personas dienestā, kā arī šādas fiziskās personas līdzdalībnieks.
Juridiskām personām, kas nav publisko tiesību juridiskās personas, var piemērot piespiedu ietekmēšanas līdzekļus, kas norādīti šā likuma VIII[1] nodaļā.

Krimināllikumā ieviesta jaunu nodaļu **"VIII[1] nodaļa „Juridiskām personām piemērojamie piespiedu ietekmēšanas līdzekļi"**

---

396 The implementation of the Corpus Juris in the member states vol.1. Prof. M.Delmas- Marty ,Prof.J.A.E.Vervaele (eds) Antwerpen-groningen-Oxford- Intersentia, 2000., p. 134

397 Likums stājas spēkā vienlaikus ar Kriminālprocesa likuma spēkā stāšanos.

70[1]. pants. Pamats piespiedu ietekmēšanas līdzekļa piemērošanai juridiskai personai

(1) Par šā likuma sevišķajā daļā paredzēto noziedzīgo nodarījumu izdarīšanu juridiskai personai var piemērot piespiedu ietekmēšanas līdzekli, ja noziedzīgo nodarījumu juridiskās personas interesēs ir izdarījusi fiziskā persona, rīkodamās individuāli vai kā attiecīgās juridiskās personas koleģiālās institūcijas loceklis, balstoties uz tiesībām pārstāvēt juridisko personu vai pieņemt lēmumus juridiskās personas vārdā, vai arī īstenojot kontroli juridiskās personas ietvaros.

(2) Juridiskās personas sodīšana neizslēdz vainojamās fiziskās personas, kā arī tās līdzdalībnieku krimināltatbildību.

(3) Juridiskai personai piemērojamie piespiedu ietekmēšanas līdzekļi neattiecas uz valsti, pašvaldībām un citām publisko tiesību juridiskām personām.

70. [2] pants. Juridiskai personai piemērojamo piespiedu ietekmēšanas līdzekļu veidi

(1) Juridiskai personai, kura izdarījusi noziedzīgu nodarījumu, var noteikt vienu no šādiem piespiedu ietekmēšanas līdzekļiem:

1) likvidācija;

2) tiesību ierobežošana;

3) mantas konfiskācija;

4) naudas sods;

5) kaitējuma atlīdzināšana.

(2) Par šā likuma sevišķajā daļā paredzētiem krimināpārkāpumiem un mazāk smagiem noziegumiem juridiskām personām piemēro naudas sodu.

(3) Par šā likuma sevišķajā daļā paredzētiem smagiem un sevišķi smagiem noziegumiem juridiskām personām var piemērot likvidāciju, tiesību ierobežošanu, mantas konfiskāciju vai naudas sodu.

(4) Mantas konfiskāciju juridiskām personām var piemērot arī kā papildus piespiedu ietekmēšanas līdzekli, ja juridiskā persona nodarījuma rezultātā guvusi mantisku labumu un tai kā pamata piespiedu ietekmēšanas līdzeklis ir piemērota tiesību ierobežošana vai naudas sods.

(5) Kaitējuma atlīdzināšanu juridiskām personām var piemērot gan kā pamata, gan arī kā papildus piespiedu ietekmēšanas līdzekli, ja noziedzīgā nodarījuma rezultātā ir radīts būtisks kaitējums vai smagas sekas.

70.[3] pants. Likvidācija

(1) Likvidācija ir juridiskās personas, tās filiāles, pārstāvniecības vai struktūrvienības darbības piespiedu izbeigšana.

(2) Juridiskā persona, tās filiāle, pārstāvniecība vai struktūrvienība ir likvidējama tikai tajos gadījumos, ja juridiskā persona, tās filiāle, pārstāvniecība vai struktūrvienība ir īpaši izveidota noziedzīga nodarījuma vai vairāku noziedzīgu nodarījumu izdarīšanai, vai ja tā ir izdarījusi smagu vai sevišķi smagu noziegumu.

(3) Likvidējot juridisko personu, tās filiāli, pārstāvniecību vai struktūrvienību, valsts īpašumā bez atlīdzības ir atsavināma visa tās īpašumā esošā manta. Nav atsavināma tā manta, kas nepieciešama juridiskās personas saistību izpildei attiecībā pret darbiniekiem, valsti un kreditoriem.

70.[4] pants. Tiesību ierobežošana

Tiesību ierobežošana ir tiesību atņemšana uz noteiktu veidu uzņēmējdarbību, speciālā likumā paredzēto atļauju vai tiesību atņemšana vai aizliegums veikt noteikta veida darbību uz laiku no viena līdz pieciem gadiem.

70.[5] pants. Mantas konfiskācija

(1) Mantas konfiskācija ir juridiskās personas īpašumā esošās mantas pilnīga vai daļēja piespiedu bezatlīdzības atsavināšana valsts īpašumā, kuru var piemērot kā pamata vai kā papildus piespiedu ietekmēšanas līdzekli.

(2) Tiesa, nosakot daļēju mantas konfiskāciju, konkrēti norāda, kāda manta ir konfiscējama.

(3) Nosakot pilnīgu mantas konfiskāciju, nav konfiscējama tā juridiskās personas īpašumā esošā manta, kas ir nepieciešama saistību izpildei pret darbiniekiem, valsti un kreditoriem.

(4) Var konfiscēt arī juridiskās personas īpašumā esošu mantu, kas ir nodota citai juridiskai vai fiziskai personai.

70.[6] pants. Naudas sods

(1) Naudas sods ir naudas piedziņa, kas atbilstoši noziedzīgā nodarījuma smagumam un juridiskās personas mantiskajam stāvoklim ir nosakāma no vienas līdz desmit tūkstošiem Latvijas Republikā noteikto minimālo mēnešalgu apmērā sprieduma taisīšanas brīdī, norādot spriedumā šā naudas soda summu Latvijas Republikas naudas vienībās.

(2) Naudas sods, kas uzlikts juridiskajai personai, maksājams no juridiskās personas līdzekļiem.

(3) Ja juridiskā persona izvairās no naudas soda samaksas, tad šis piespiedu ietekmēšanas līdzekļa veids tiek izpildīts piespiedu kārtā.

Uzskatu, ka minētā pieeja ir viena no visveiksmīgākiem risinājumiem juridiskās personas atbildības jomā pasaulē, jo: 1) pilnīgi neskar sensitīvo „vainas individualizācijas" jautājumu, kas līdz šim visvairāk attur daudzas valstis, tai skaitā arī vairākas ES valstis, ieviest šo atbildības formu; 2) tas formāli atbilst pilnīgi visām starptautiskām konvencijām, kas paredz dalībvalstīm juridisko personu atbildību par konkrētu noziedzīgu nodarījumu, ieskaitot kibernoziegumus, veikšanu vai atbalstīšanu; 3) projekts neparedz juridiskās atbildības piemērošanu tikai par atsevišķiem noziedzīgiem nodarījumiem, kā to prasīja no Latvijas starptautiskās saistības, bet to var nepieciešamības gadījumā piemērot par jebkuru krimināllikuma sevišķā daļā ietvertu nodarījumu, ja izmeklēšanas laikā tiek konstatēti pierādījumi par juridiskās personas saistību ar konkrēto nodarījumu.

## 5. Subjektīvā puse

Subjektīvās puses jēdziens aptver subjekta psihisko attieksmi pret sabiedriski bīstamu nodarījumu. Juridiskajā literatūrā noziedzīgā nodarījuma subjektīvā puse definēta kā noziedzīgā nodarījuma sastāva elements, kas dod priekšstatu par iekšējiem psihiskiem procesiem, kas rodas personas, kuras izdara noziedzīgu nodarījumu, apziņā, ko raksturo konkrēta vainas forma, motīvs, mērķis un emocijas.[398] Respektīvi, noziedzīgā nodarījuma subjektīvā puse atspoguļo saistību starp personas apziņu un gribu un viņas izdarīto nodarījumu.[399] Subjektīvās puses pamatpazīme ir vaina. U. Krastiņš, mūsuprāt, ir devis ļoti vienkāršu, bet vienlaikus izsmeļošu vainas definīciju: „Vaina ir personas psihiskā attieksme nodoma vai

---

[398] Советское уголовное право. Общая часть. Москва- издательство Московского университета, 1981.,С.179;А.В. Наумов Уголовное право.Общая часть. Учебник для вузов. Москва- М·Инфра,1997.,с.181;

[399] Turpat, Krastiņš U., 89.lpp.

neuzmanības formā pret viņas izdarīto prettiesisko darbību vai bezdarbību un ar to saistītajām kaitīgajām sekām."[400]

## 5.1. Vaina

Bez vainas nav noziedzīga nodarījuma. Satversmes 92.panta 2. teikums jautājumu par personas vainu ir izvirzījis kā cilvēktiesību standartu: "Ikviens uzskatāms par nevainīgu iekams viņa vaina nav pierādīta ar likumu."

Savukārt Sarversmes 82. pants noteic: „Tiesu Latvijā spriež rajona (pilsētas) tiesas, apgabaltiesas un Augstākā tiesa, bet kara vai izņēmuma stāvokļa gadījumā - arī kara tiesas".Tātad nevienu nevar nosaukt par vainīgu, kamēr to par tādu nav atzinusi tiesa. Līdzīgs viedoklis tiek atbalstīts visās demokrātiskās valstīs, taču līdz ar to rodas jautājums, vai vaina kā elements ir obligāta noziedzīga nodarījuma sastāva pazīme.

Vaina ir viena no noziedzīga nodarījuma sastāva obligātajām pazīmēm. P. Lejiņš definē vainu kā tādas norises indivīda psihē, kuru dēļ mēs šo indivīdu uzskatām par atbildīgu par viņa uzvedību.[401] Līdzīgu viedokli pauž S. Dando[402], ka vaina nav tikai tīrs personas antisociālā rakstura atspoguļojums, bet drīzāk viena no personības realizācijas vai funkcionēšanas formām. Šim viedoklim var piekrist, jo vainai nenoliedzami ir jābūt saistītai ar kaut kādu noziedzīga nodarījuma realizāciju, bet persona nevar tikt atzīta pat vainīgu tikai tāpēc, ka tās raksturs ir antisociāls. Vaina vienmēr izpaudīsies noteiktās bīstamās darbībās vai bezdarbībā, tāpēc tai nav tiešas saistības ar personas antisociālo raksturojumu. Līdzīgu viedokli pauž krimināltiesību teorētiķi visā pasaulē, jo ar vainu var apzīmēt individuālās personas krimināli sodāmas darbības vai bezdarbības novērtējumu. Tāpēc vairākās valstīs vaina netiek uzskatīta par noziedzīga nodarījuma sastāva elementu, jo arī Rietumu tiesību teorijā plaši izmantotais termins *mens rea* lielāku uzmanību pievērš nodoma izpētei. Kā norāda G. Sulivans, *mens rea* bieži tiek tulkots kā vainojamā prāta stāvoklis, kas satur nodarījuma vainas elementu.[403] Praksē tam ir maza

---

400 Turpat, Krastiņš U., 90.lpp.

401 Turpat, Docents Lejiņš P., 68. lpp.

402 Ibid., Shigemitsu Dando p.137

403 Ibid., A.P. Simester , G.R. Sullivan, p. 114.

nozīme. Lai prokurors pierādītu apsūdzību, viņam pietiek pierādīt, ka noziedzniekam bija vainojams prāta stāvoklis pret krimināli sodāmo darbību vai bezdarbību, respektīvi, jāpierāda personas nodoms, bet vainu noteiks tiesa. ASV tiesību teorētiķi, definējot vainu, to saista ar personas, kas izdara noziedzīgu nodarījumu, psihisko stāvokli. Tomēr autoru domas dalās, kā definēt šo subjektīvo stāvokli, jo vieni uzskata, ka vaina jāsaista ar spēju izprast, citi par nodomu un izpratni, trešie par izpratni un vēlēšanos, ceturtie par nosodāmu psihisku stāvokli; piektie par - jebkuru psihisku stāvokli u.c.[404] Vācijas krimināltiesību doktrīnā ar vainu definē izpildītāja iekšējo stāvokli pret savu nodarījumu, ko raksturo pārmetums. Izšķir divas vainas formas- nodomu un neuzmanību. Taču Vācijas Soda likums nesatur vainas formu raksturojumu. Līdzīga pieeja ir arī citās Rietumeiropas valstu krimināltiesību doktrīnās. Taču, analizējot iepriekšminēto praksi, jāatzīst, ka juridiskajā literatūrā ir plaši izplatīta definīcija, ka vaina ir personas psihiskā attieksme nodoma vai neuzmanības formā pret viņas izdarīto prettiesisko darbību vai bezdarbību un ar to saistītām kaitīgām sekām.[405] Taču, kaut arī vainu lielākā daļa pasaules valstu definē kā personas psihiskās darbības rezultātu, vienmēr jāatceras, ka vainas konstatācija lielā mērā ir atkarīga no tiesneša subjektīvā viedokļa, ko viņš veido, pamatojoties uz konkrētajā krimināllietā savāktajiem pierādījumiem. Taču svarīgi ir tas, ka tiesnesim ir pienākums konstatēt objektīvi pastāvošo personas vainu konkrētā nodarījumā. Tāpēc Latvijas tiesību doktrīnā vaina ir obligāta noziedzīga nodarījuma sastāva pazīme, kas izpaužas nodoma vai neuzmanības formā.

## 5.2. Nodoms

Krimināllikuma 9. pants noteic, ka „... noziedzīgais nodarījums atzīstams par izdarītu ar nodomu (tīši), ja persona, kas to izdarījusi, ir paredzējusi nodarījuma sekas un vēlējusies tās (tiešss nodoms) vai, kaut arī šīs sekas nav vēlējusies, tomēr apzināti pieļāvusi to iestāšanos (netiešs nodoms)."

---

404 Уголовное право зарубежных стран. Общая часть. Под . ред. Проф. И.Д. Козочкина. Москва: Омега Л, 2003., с.130

405 Turpat, Krastiņš U., 90.lpp.

Kā norāda G. Sullivans, tad nozieguma lietā centrālais un parasti svarīgākais jautājums ir par to, vai izpildītāja noziegums ir tīšs. Parasti nav nepieciešams sīki izstrādāt nodoma definīciju, lai nolemtu, vai *actus reus* ir tīšs. Tomēr viņš ierosina nodoma konstatēšanā izmantot šādas vadlīnijas: 1) parasti iecerētais *actus reus* ir paraugs nodoma izpratnei; 2)atzīts, ka *actus reus* bija patiesībā noteiktas izpildītāja darbības sekas. [406] Līdzīgu viedokli pauž arī citi autori, piemēram, V. La Fave (*Wayne R. LaFave*), aprakstot tradicionālo nodoma saturu, norāda, ka noziegums ir jādefinē tā, ka noziedzniekam, kas atzīstams par vainīgu tā izdarīšanā, tīši jābūt iesaistītam konkrētā uzvedībā.[407] Ar uzvedību V. La Fave saprot: 1) tieši krimināllikumā aprakstītu un aizliegtu darbību vai bezdarbību; 2) prāta stāvokli, kas pavada darbību vai bezdarbību; 3) konkrētā nozieguma nodarījuma dispozīcija ir jāuzraksta tā, lai tā aptvertu aizliegto darbību vai bezdarbību un kāds prāta stāvoklis nepieciešams nozieguma izdarīšanai.[408]

S. Dando norāda, ka Japānas Krimināllikuma 38 (1)[409] pants noteic, ka darbība nav sodāma, ja tā izdarīta bez krimināla nodoma. Pirmkārt, šī panta nozīme ir parādīt, ka tieši nodoms ir svarīgs nozieguma sastāva elements. Otrkārt, noziegums nav izdarīts ar nodomu, ja nav konstatēti nodoma pavadošie rekvizīti, līdz ar to viņš secina, ka minētais pants noteic, ka noziegums ir izdarīts ar nodomu tad, ja pastāv vainas nepieciešamie satura elementi un priekšnoteikumi.[410]

Autoraprāt, ļoti precīzi un kodolīgi nodomu definējis Š. Dando norādot, ka".. nodoms ir izpildītāja savas personīgās attieksmes skaidra izpausme, pretēji krimināllikuma normām". P. Lejiņš nodomu definē, kā „..savas gribas apzināšanos un seku paredzēšanu"[411]. Ieslēdzot jēdzienā tikai divas pazīmes, *gribu* un *sekas*, šī definīcija aptver tikai daļu no noziedzīga nodoma konstatēšanas priekšnoteikumiem, jo ārpus šīs definīcijas paliek pazīme, ka izpildītājs vēlas izdarīt tieši ar krimināllikumu aizliegtu darbību, kaut gan teorijā pastāv arī

---

406 Ibid., Sinester A.P. , Sullivan G.R. p. 114

407 Substantive criminal law Wayne R.La Fave Part.2 General principles Chapter 5. Mental states // Westlaw 2003

408 Substantive Criminal Law Wayne R. LaFave Part 1. Introduction; Sources and Limitations Chapter 1. Introduction And General Considerations// Westlaw 2003

409 Līdzīga pieeja ir Vācijas KL 15.p. un Francijas KK 121-3. pantā

410 Ibid., Shigemitsu Dando p.150.

411 Turpat, Docents Lejiņš P., 69. lpp.

viedoklis[412], ka šis apstāklis nav noteicošais motīva konstatēšanā. Tas izriet no principa, ka likuma nezināšana neatbrīvo no atbildības. Tomēr, kā redzams tālāk tekstā, ne vienmēr šī formula var tikt piemērota.

G.Sulivans uzskata, ka nodoms ir kaut kas atšķirīgs no motīva vai vēlēšanās. Šī atšķirība starp vēlēšanos un nodomu izpaužas tajā apstāklī, ka nereti cilvēki vēlas kaut ko tādu, ko nekad nevarēs sasniegt. Šādam viedoklim var piekrist, jo nodoms materializējas tikai ar brīdi, kad konkrēta persona, zinot, ka viņa uzvedība ir pretrunā ar krimināltiesību normām, realizē savu nodomu attiecībā pret konkrētu objektu un vēlas konkrētu negatīvu seku iestāšanos. Noziedzīgu nodarījumu, kas izdarīts ar tiešu nodomu, nosaka noteikts motīvs, kas vienmēr radies pirms tā, jo nodoms rodas un nostiprinās motīva ietekmē, un motīvs virza personas gribu uz noziedzīga rezultātā sasniegšanu.[413]Tādējādi jāpiekrīt, ka motīvs ietekmē nodoma rašanos, tas aktīvi virza personas uzvedību uz konkrēta mērķa sasniegšanu. A. Naumovs norāda, ka, runājot par motīvu, to var attiecināt arī uz nodarījumiem aiz neuzmanības. Tomēr viņš pamatoti norāda, ka tad ir jārunā par divu veidu motīviem: 1) tīšos noziedzīgos nodarījumos, sniedz raksturojumu, kāpēc noziedznieks ir izdarījis to vai citu noziedzību nodarījumu, kas rada noteiktas kaitīgas sekas: 2) noziedzīgos nodarījumos aiz neuzmanības motīvs raksturo, kādu apstākļu dēļ persona tā rīkojās, ka viņa uzvedība radīja sabiedriski bīstamas sekas, kuru iestāšanos viņš nevēlējās.[414] Tiesu praksē nereti motīva noteikšana ir obligāta kvalificējoša pazīme.

Piemērs. Krimināllikums neparedz atbildību par kustamas mantas patvaļīgu lietošanu. Tiesu praksē ir daudz gadījumu, kad personai inkriminēts, ka viņa tīši, mantkārīgu motīvu vadīta, ir nolaupījusi A piederošo automašīnu. Taču patiesībā persona bija iereibusi, iesēdās vienā automašīnā un aizbrauca ar to uz savu dzīves vietu, kur atstāja. Rezultātā tai inkriminēts KL 175. pantā attiecīgajā daļā paredzētais nodarījums. Taču lai notiesātu personu par svešās mantas nolaupīšanu, nepieciešams pierādīt, ka persona rīkojusies, mantkārīgu motīvu vadīta. Rezultātā šobrīd tiesu praksē šis jautājums tiek lemts dažādi. Vienas tiesas uzskata, ka tā ir zādzība, citas pārkvalificē pēc KL 279. panta kā patvarību, bet ir gadījumi, kad tiesas šīs darbības attaisno, jo vainojamās personai nav bijis mantkārīgs motīvs.

Vārdu savienojums "pretēji krimināltiesību normām" ietver arī nodoma paplašināto jēdzienu, ko devis U. Krastiņš. Viņš norāda, ka".. noziedzīgs

---

412 Turpat, Krastiņš U., 96 lpp.

413 Krastiņš U., V. Liholaja, A. Niedre Krimināllikuma komentāri.1. grāmata. Vispārīgā daļa.Rīga- AFS,1999., 77lpp.

414 Наумов А.В. Уголовное право.Общая часть. Учебник для вузов. Москва- ИНФРА,1997.,с. 201

nodarījums izdarīts ar nodomu (tīši), ja persona, kas to izdarījusi, ir apzinājusies savas darbības vai bezdarbības bīstamo raksturu, paredzējusi bīstamās sekas un vēlējusies vai apzināti pieļāvusi šo seku iestāšanos"[415]. Līdzīga pieeja ir arī Ķīnas (KK 14.p.), Polijas (KK 9.p.), Krievijas Federācijas (KK 25p.) tiesību praksē. P. Lejiņš šīs sekas klasificē: 1) neizbēgamās- sekās, kas neizbēgami iestājas. Piem., persona patvaļīgi piekļūst datorsistēmai, sagraujot informācijas sistēmu aizsardzību, tātad noziedzīga nodarījuma izpildītājs neizbēgami būs sabojājis informācijas sistēmas resursus; 2) ticamas sekas- pēc prakses lielākajā daļā gadījumu iestājas. Ticamība tam, ka izpildītājs, patvaļīgi piekļūstot bankas informācijas sistēmai, nenolaupīs informāciju, ir maz ticama. Tāpēc jau likumdevējs ir novērtējis un iekļāvis Krimināllikuma 241. panta 1.d., kā ticamas sekas, kas radītu iespēju nepiederīgai personai iepazīties ar sistēmā ievietotu informāciju, kas nenoliedzami lielākoties, šādu nodarījumu veicot, arī iestājas. 3) iespējamās sekas – pa lielākai daļai sekas neiestājas, bet nav izslēgts, ka tās var iestāties. Piemēram, N izgatavo datortārpu un palaiž to internetā. Viņš neparedz konkrētu seku iestāšanos, bet iespējams, ka šī tārpa darbība var sabojāt arī datorsistēmas, bet var arī nesabojāt.

P. Lejiņš norāda, ka izpildītājam jāparedz un jāatbild par neizbēgamām un ticamām sekām, bet iespējamās sekas nav jāparedz un par tām nav jāatbild. Šādam viedoklim nevar piekrist. Sevišķi runājot par noziedzīgu nodarījumu, kas izdarīts ar netiešu nodomu, likumdevējs jau ir paredzējis personas atbildību par iespējamām, pieļaujamām sekām.

Kibernoziegumu jomā nereti uzbrukumi informācijas sistēmām tiek veikti arī bez konkrēta mērķa nodarīt sistēmai kaitējumu. Iespējams, ka šādas negatīvas sekas pēc 10- 15 dienām var rasties Sauda Arābijā vai Austrālijā u.c. Tāpēc Krimināllikuma 244. panta dispozīcija paredz, ka noziegums ir pabeigts tajā brīdī, kad N ir radījis un izplatījis tādu kaitīgu rīku, kura mērķis ir negatīvi ietekmēt citai personai piederošas datorsistēmas resursus.

Rietumvalstu krimināltiesību teorētiķi uzskata, ka konkrētās personas apzinātā darbība ir atzīstama par izdarītu tīši (ar nodomu), ja to pamato vairāki elementi. Šie

---

[415] Krastiņš U. Mācība par nozieguma sastāvu. Rīga- Zvaigzne ABC,1997., 62. lpp.

elementi Rietumu tiesību teorijā nosaukti par materiāliem elementiem[416]. S. Dando šos elementus raksturo: 1) pirms nodoms ir noticis, izpildītājam jāzina nozieguma elementiem atbilstošie objektīvie fakti. Pie šādiem faktiem pieskaita šo darbību subjektu, objektu un ar tiem saistītos apstākļus, sekas un cēloņus un sakarības starp tiem; 2) ja izpildītajam visi šie apstākļi nav zināmi, tad nevar runāt par to, ka nodarījums izdarīts ar nodomu. Tātad pie šādiem apstākļiem var pieskaitīt darbību vai bezdarbību bīstamo raksturu, bīstamās sekas, cēloņsakarības. Daži Rietumvalstu tiesību teorētiķi uzskata, ka nodomu raksturo arī tas, ka izpildītājam ir jāzina, ka viņa uzvedība ir saistīta ar krimināltiesisku aizliegumu[417], tomēr diezin vai šāda pazīme var tikt identificēta ar nodomu, jo personu taču nevar atbrīvot no krimināatbildības tāpēc, ka viņš nezināja par šādu krimināltiesisku uzvedības aizliegumu un soda piedraudējumu. Tomēr teorijā un praksē, īpaši tad, ja runā par nodarījumiem, kuru sekas var iestāties citas valsts teritorijā, ar šīs pazīmes interpretāciju var rasties nopietnas problēmas, jo nevienai personai taču nav jāzina visas pasaules valstu likumi. Tādējādi atzīstot to, ka „... krimināllietā nav jāpierāda, ka izpildītājs zinājis, tieši kādu normu tas pārkāpis"[418], mēs faktiski jebkuru interneta lietotāju varam padarīt par potenciālu noziedznieku.

Neapšaubāmi, ka likumu nezināšana nacionālā jurisdikcijā nevienu no atbildības nevar atbrīvot, taču autors apšauba šīs tēzes pamatotību pārrobežu tiesību kontekstā. Protams, līdzīgi kā Rietumvalstu tiesību doktrīnā izpildītāja nodoma noteikšanā praksē ņem vērā ne tikai objektīvos ar nodarījumu saistītos apstākļus, bet arī izpildītāja personības subjektīvās īpašības, piemēram, viņa profesionālās zināšanas, dzīves pieredzi, vecumu u.c. Ja profesionāls datorspeciālists izgatavo kaitīgu rīku, kura mērķis var būt tikai datorsistēmu aizsardzības sistēmu apiešana vai sagraušana un sistēmu informācijas resursu ietekmēšana, tad, izvērtējot nodarījumu, tiesa, vērtējot viņa personību, ņems vērā to nosakot sodu, jo šī persona nevar aizbildināties ar to, ka viņa nezināja, kādas sekas var iestāties. Taču cita

---

[416] Ibid., Shigemitsu Dando p.151; Substantive criminal law Wayne R.La Fave Part.2 General principles Chapter 5. Mental states // Westlaw 2003 ; Sinester A.P. ; Ibid., Sullivan G.R., pp. 115-117

[417] Substantive Criminal Law by Wayne R. LaFave Part 1. Introduction; Sources and Limitations Chapter 1. Introduction And General Considerations// Westlaw 2003

[418] Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 96 lpp.

situācija ir tad, ja persona neprasmīgi izmanto pilnīgi likumīgas programmas Word opīciju "Macros" un tā rada makrovīrusu, kas ietekmē sistēmas resursus un tāpat var nodarīt kaitējumu. Tādējādi kriminālliet̄as, kas saistītas ar nodarījumiem pret informācijas sistēmu drošību, jautājums par nodarījuma motīvu ir daudz sarežģītāks par motīvu tradicionālos nodarījumos. Tomēr, izvērtējot Rietumvalstu tiesību teoriju un praksi un Latvijas tiesību praksi noziedzīgā motīva satura novērtējumā, būtisku atšķirību nav. Kā jau iepriekš minēts, tad teorijā un praksē izšķir tiešo un netiešo nodomu.

*Tiešs nodoms (dolus directus)*

Likumdevējs KL 9. pantā ir iekļāvis noziedzīgā nodarījuma izdarīšanas ar nodomu (tīši) jēdzienu, kur tiešais nodoms saistīts ar noziedzīgā nodarījuma izpildītāja seku paredzējumu un vēlēšanos, lai tās iestātos. Tās ir sekas, ko P. Lejiņš definējis kā neizbēgamas un tīši gribētas.[419] Tomēr, kā pareizi norāda U. Krastiņš[420] un daudzi citi autori[421], tad tiešu nodomu vienmēr raksturos šādas pazīmes: 1) uzvedība (darbība vai bezdarbība) izpaužas tādā veidā, ka persona, to darot, pilnīgi apzinās tās kaitīgumu: 2) tā precīzi paredz šīs uzvedības rezultāta kaitīgās sekas: 3) obligāti vēlas, lai šīs sekas iestātos. Ja kādas no šīm pazīmēm trūkst, tad nav arī pamata runāt par tiešu nodomu. Tādējādi nodoma veids ir tieši atkarīgs no gribas momenta, proti, vai izpildītājs tieši paredzējis kaitīgo seku iestāšanos un vēlējies tās, vai paredzējis šīs sekas, bet nav tās vēlējies, tomēr pieļāvis to iestāšanos.

*Netiešais nodoms (dolus eventualis)*

KL 9. pants paredz, ka nodarījums izdarīts ar netiešu nodomu tad, ja persona, kas izdarījusi noziedzīgu nodarījumu, ir paredzējusi nodarījuma sekas, bet, kaut arī nav vēlējusies, tomēr apzināti pieļāvusi to iestāšanos. Tādējādi netiešu nodomu raksturo: 1)personas apzināta darbība; 2) apziņa, ka veiktā darbība vai bezdarbība ir kaitīga; 3) nav tieši vēlējusies seku iestāšanos, tomēr neko nav darījusi, lai tās novērstu, respektīvi, apzināti pieļāvusi, ka šādas sekas var iestāties.

---

419 Turpat, Docents Lejiņš P., 73. lpp.

420 Krastiņš U. Noziedzīgs nodarījums. Rīga: TNA, 2000., 96 lpp.

421 Советское уголовное право. Общая часть. Москва: издательство Московского университета,1981.,с.175; Наумов А.В. Уголовное право.Общая часть. Учебник для вузов. Москва: ИНФРА,1997.,с. 185 ; Ветров Н.И. Уголовное право. Общая часть.Моква: Юнити, 1999., с. 189

Piemērs. Kuldīgas rajona tiesa atzina G par vainīgu un sodīja par slepkavību, kas izdarīta ar netiešu nodomu. G . ieradās pie P. Starp viņiem radās strīds, un P. sāka lamāt G. G., lai viņu nomierinātu, ar pirkstiem saņēma aiz kakla un iegrūda gultā. Kad P. turpināja lamāties, viņš ar pirkstiem sažņaudza tās kaklu un miega artēriju, un P. apklusa. Rezultā P. mira no mehāniskās asfiksijas. G. nevēlējās P. nāvi, taču apzināti, zinot, ka P. ir problēmas ar astmu, žņaudza viņu un pieļāva P. nāves iestāšanos.[422]

Nodoma noteikšanai ir ne tikai svarīga praktiska nozīme noziedzīgu nodarījumu kvalifikācijā, bet tā ir saistīta arī ar noziedzīga nodarījuma stadiju izvērtēšanu. Ja persona izdara noziegumu ar tiešu nodomu, viņa tam gatavojas. Sagatavošanas stadijā tā veic noteiktas darbības, lai sasniegtu noziedzīgo rezultātu, piem., iegādājas nepieciešamo instrumentāriju, apgūst nepieciešamās zināšanas, izpēta vidi un rada citus labvēlīgus apstākļus noziedzīgā mērķa sasniegšanai. Tikai rīkojoties ar tiešu nodomu, vainojamā persona var tīši veikt apzinātu darbību (bezdarbību), bet nesasniegt cerēto rezultātu no savas gribas neatkarīgu iemeslu dēļ, tādējādi izdara noziedzīga nodarījuma mēģinājumu. Sagatavošanos noziegumam un nozieguma mēģinājumu likumdevējs nosaucis par nepabeigtu noziedzīgu nodarījumu. Iepriekšminētais pierāda to, ka noziedzīgos nodarījumos, kas izdarīti ar netiešu nodomu, nevar būt nepabeigts noziegums, jo šādos gadījumos vainojamā persona vienmēr ir atbildīga par faktiski izraisītām sekām, kas paredzētas Krimināllikuma sevišķā daļā.

### 5.3. Vainas interpretācijas problēmas noziedzīgos nodarījumos pret informācijas sistēmu drošību

Lielākā daļa pasaules valstu, kur krimināllikumos iekļauti noziedzīgi nodarījumi pret informācijas sistēmu drošību, paredz atbildību tikai par tīšām darbībām[423], jo, kā uzsver vairāki tiesību teorētiķi un praktiķi, tas izriet no minēto noziedzīgo nodarījumu dispozīcijas apraksta. Noziedzīgos nodarījumus, kas vērsti pret informācijas sistēmu drošību, var izdarīt tikai tīši kā ar tiešu, tā arī ar netiešu nodomu.

Tā, piemēram, Kibernoziegumu konvencijas paskaidrojošā memoranda 39.punktā īpaši uzsvērts, ka visiem Konvencijā ietvertajiem noziedzīgajiem

---

[422] 2003.gada 25. novembra Spriedums A.G. apsūdzībā pēc Krimināllikuma 116. panta un 175.panta 2.daļas.Kuldīgas rajona tiesas Krimināllieta Nr. 1250011203 ;KL19-246/03;

[423] Новое уголовное право России. Учебное пособие. Особенная часть. Под ред. Н.Ф.Кузнецовой. Москва:Зеркало ТЕИС, 1996.,с. 274

nodarījumiem jābūt tīšiem. Tomēr ievērojot to, ka starp dalībvalstīm ir atšķirīga nostāja termina "tīši" interpretācijā, tā piemērošana ir deleģējama katrai dalībvalstij.[424] Kibernoziegumu eksperti kategoriski noraidīja jebkuru iespēju par kibernoziegumiem vai noziegumiem pret informācijas sistēmu drošību atzīt nodarījumus aiz neuzmanības. Šis argumentam ir ļoti racionāls pamatojums, jo Konvencijas 15. pants noteic, ka dalībvalstīm Konvencijā aprakstīto noziedzīgo nodarījumu identifikācijā un procedūru izpildē ir jānodrošina garantijas un nosacījumi, kas pasargās personas no pārmērīgas valsts varas piemērošanas.

Kā zemākais garantiju un nosacījumu slieksnis minēti starptautiskie cilvēktiesību aizsardzības instrumenti, piemēram, 1950.gada Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija, 1969.gada Amerikas Cilvēktiesību konvencija, 1981.gada Āfrikas Cilvēktiesību un pilsoņu tiesību harta u.c. Tas nozīmē, ka valsts var noteikt ierobežojumus tikai tad, ja to prasa sabiedrības intereses un apdraudētā interese ir daudz svarīgāka par konkrētās personas tiesību ierobežojumu.

Izstrādāt vispārobligātus noteikumus par piekļūšanu datorprogrammām un informācijas sistēmu drošību, kā paredz Krimināllikuma Pārejas noteikumu 3. pants, nozīmētu rupji pārkāpt Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju, jo neviena valsts pasaulē nav spējīga izstrādāt tādus informācijas sistēmu drošības noteikumus, lai to piemērošanas gadījumā līdz minimumam samazinātu apdraudējumus visām valstī esošām informācijas sistēmām. Ja mēs pieļaujam neuzmanību kā vainas formu noziedzīgos nodarījumos pret informācijas sistēmu drošību, tad ar to pašu faktiski padarām par potenciāliem noziedznieku jebkuru personu, kam pieder informācijas sistēmas un kas atbild par to drošību. Tas ir bīstams solis un var radīt neparedzamas sekas.

Piemēram, komentējot KF KK 272. un 274. pantu, daži autori uzskata, ka atbildībai par piekļūšanu informācijai un informācijas sabojāšanu ir jāiestājas neatkarīgi no veida, kā sekas radušās, tai skaitā arī tad, ja datorinformācijas iznīcināšana vai bojāšana notikusi no atbildīgās personas gribas neatkarīgu apstākļu

---

[424] ConfCT(2001) Exp.Mem. Explanatory report to the Convention on cybercrime. Strasbourg 12 November 2001

dēļ, piemēram, ārējo faktoru, siltuma, magnētisko viļņu, mehānisko triecienu rezultātā, jo informācijas īpašniekam ir jānodrošina informācijas aizsardzības režīms, tai skaitā nosakot datorsistēmu izmantošanas noteikumus, aizsardzību no prettiesiskām darbībām, kas ierobežo nesankcionētu piekļuvi informācijas resursiem, izveido nelikumīgas pieejas novērtēšanu.[425] Tomēr veselais saprāts ir uzvarējis, un lielākā daļa speciālistu, kas pēta šos jautājumus, šādu viedokli atzīst par kļūdainu.[426]

---

[425] Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва- Юриспрудения. 1999., с. 656

[426] Коментарый к уголовному кодексу Росийской федерации. Особенная часть. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва- издательская группа Инфра · М- Норма,1996., с.413; Ibid., Волеводз А.Г., с. 66; Коментарый к уголовному кодексу Росийской федерации. Издание 3-е измененное и дополненное. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва- издательская группа Инфра · М- Норма, 2000.,с.696

## 6. Krimināllikumā ietverto noziedzīgo nodarījumu pret informācijas sistēmu drošību (turpmāk – ISD) (241- 245. pants) salīdzinošā analīze

### 6.1. Noziedzīga nodarījuma „Patvaļīga piekļūšana datorsistēmai" (līdz 01.06.2005.) un „Patvaļīga piekļuve automatizētai datu apstrādes sistēmai" (28.04.2005.) (241.pants) krimināltiesiskais raksturojums.

| **Panta nosaukums** | Redakcijā līdz 2005. gada 1. jūnijam | 2005. gada 28. aprīļa redakcija |
|---|---|---|
| **241. pants** | **Patvaļīga piekļūšana datorsistēmai** | **Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai** |
| 1. daļa | Par patvaļīgu piekļūšanu automatizētai datorsistēmai, ja ar to nepiederīgai personai radīta iespēja iepazīties ar sistēmā ievietoto informāciju,-<br><br>soda ar arestu vai ar naudas sodu līdz astoņdesmit minimālajām mēnešalgām | Par patvaļīgu (bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības) piekļūšanu automatizētai datu apstrādes sistēmai vai tās daļai, ja tas saistīts ar datu apstrādes sistēmas aizsardzības līdzekļu pārvarēšanu un ja ar to radīts būtisks kaitējums,-<br><br>soda ar brīvības atņemšanu uz trīs gadiem vai ar piespiedu darbu vai ar naudas sodu līdz piecdesmit minimālām mēnešalgām. |
| 2. daļa | Par tādām pašām darbībām, ja tās saistītas ar datortehnikas programmatūras aizsardzības līdzekļu pārvarēšanu vai ar pieslēgšanos sakaru līnijām,-<br><br>soda ar brīvības atņemšanu uz laiku līdz vienam gadam vai ar naudas sodu līdz simts piecdesmit minimālajām mēnešalgām. | Par tām pašām darbībām, ja tās izdarītas mantkārīgā nolūkā vai izraisījušas smagas sekas,-<br><br>soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar arestu, vai ar piespiedu darbu, vai ar naudas sodu līdz simts minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas. |
| 3. daļa | X | Par šī panta pirmā daļā paredzētām darbībām, ja tās vērstas pret valsts informācijas sistēmām,-<br><br>Soda ar brīvības atņemšanu līdz astoņiem gadiem vai ar naudas sodu līdz simts astoņdesmit minimālajam mēnešalgām. |

*Noziedzīgā nodarījuma objekta noteikšanas problēmas*

Noziedzīgiem nodarījumiem pret ISD ir vienots noziedzīgā nodarījuma objekts, proti, tā ir vēršanās pret personu tiesību būt drošiem par sev piederošo datorsistēmu un ISD. Profesore V. Liholaja uzskata, ka visos nodarījumos pret ISD, tai skaitā arī Krimināllikuma 241. pantā paredzētajam nodarījumam, tiešais noziedzīgā nodarījuma objekts ir vēršanās pret visām ISD pazīmēm, tas ir integritāti, konfidencialitāti un pieejamību.[427] Krimināltiesību speciālistu vidū par šo jautājumu nav vienota viedokļa, piemēram, V. Krilovs uzskata, ka nelikumīga piekļuve datorinformācijai (KF KK 272.p.) ir vēršanās pret ISD pazīmi konfidencialitāti[428], bet A. Pašins, ka apdraudētā interese ir īpašnieka un trešo personu tiesības uz informāciju.[429] A. Voļevodzs uzskata, ka patvaļīgas piekļuves objekts ir tiesiskās attiecības saistībā ar informācijas valdījumu, lietošanu un izmantošanu.[430]

Rietumvalstu tiesību pētnieku darbos šī problēma netiek akcentēta, taču, vadoties no ANO Pētījuma par informācijas nedrošību[431], Pasaules Zinātnieku Federācijas pastāvīgi darbojošās grupas informācijas drošības pārraudzībai (*World federation of scientists Permanent monitoring panel on information security*) rekomendācijām[432] un citiem starptautiskiem dokumentiem var secināt, ka KL 241. panta "Patvaļīga piekļūšana datorsistēmai" (līdz 01.06.2005.) un patvaļīga piekļūšana automatizētai datu apstrādes sistēmai" (28.04. 2005.) apdraudētā interese ir personas tiesība sev piederošā informācijas sistēmā noteikt kārtību, kā sistēmas lietotāji var izmantot sistēmas resursus. Respektīvi, tā ir vēršanās pret sistēmas īpašnieka vai viņa pilnvarotās personas noteikto kārtību likumīgam

---

427 Krastiņš U., Liholaja V., Niedre A. Krimināllikuma zinātniski- praktiskais komentārs (3) Sevišķā daļa, profesora U. Krastiņa redakcijā. – Rīga "AFS", 2003., 226.lpp.

428 Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва- Юриспрудения. 1999., с.665

429 Коментарый к уголовному кодексу Росийской федерации. Издание 3-е измененное и дополненное. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва- издательская группа Инфра · М- Норма,2000., с.696

430 Волеводз А.Г. Противодействие компютерным преступлениям. Правовые основы международного сотрудничества. Москва-Юрлитинформ, 2002.,с.62

431 Gelbstein E.,Kamal A. Information insecurity. A survival guide to the uncharted territories of cyber- threats and cyber security. New-York- United Nation ICT task force and UNITAR , 2002., p. 16;

432 Towards a universal order of cyberspace: managing threats from cybercrime to cyberwar. Report& recommendations.[b.i] August 2003 p.17-20

lietotājam vai ISD pazīmi pieejamību. Tādējādi viedoklis, ka visi noziedzīgi nodarījumi pret ISD vēršas pret visām ISD pazīmēm vienlaicīgi, no tiesību teorijas viedokļa ir kļūdains, jo katra no ISD pazīmēm satur noteiktu specifisku apakšpazīmju kopumu, kas to raksturo kā specifisku interesi. Tomēr kā jau jebkuras intereses tās ir savstarpēji saistītas, jo nav iespējams bez pieejamības nodrošināt integritāti un konfidencialitāti. Taču autors uzskata, ka KL 241. panta noziedzīgā nodarījuma objekts ir personas tiesību apdraudējums realizēt sev vēlamās pieejamības tiesības sistēmā esošiem resursiem.

*Noziedzīgā nodarījuma priekšmets*

KL 241. panta iepriekšējā redakcija "Patvaļīga piekļūšana datorsistēmai" par nodarījuma priekšmetu atzina automatizētu datorsistēmu. Datorsistēma parasti sastāv no dažādām ierīcēm, kas tradicionāli sastāv no procesora vai centrālā procesora bloka un perifērijas jeb palīgierīcēm. „Perifērijas "nozīmē ierīces, kas nodrošina speciālu funkciju izpildi mijiedarbībā ar centrālo procesora bloku, kā, piemēram, kompaktdisku ierakstītāju, drukas ierīci, ekrānu u. c. Kibernoziegumu konvencijas 1. panta a. apakšpunktā datorsistēma definēta kā „.. jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču grupa, kuras uzdevums ir programmas vadībā veikt automātisko datu apstrādes procesu."[433]

Autors uzskatīja, ka KL 241. panta definētais priekšmets „automatizēta datorsistēma" neatbilda mūsdienu prasībām. Tas nevajadzīgi radīja automātisko datu apstrādes sistēmu sadalījumu datorsistēmās un citu komunikāciju funkcionēšanu nodrošinošās sistēmās. Jautājums nav tikai tehniska rakstura. Tam ir arī juridiska nozīme, jo ar ko atšķiras patvaļīga piekļuve datorsistēmai no piekļuves digitālai telekomunikāciju sistēmai vai piekļuves iekšējam datu pārraides tīklam, tikai ar to, ka minētos priekšmetus neietver Krimināllikuma 241. panta (līdz 01.06. 2005.) paredzētais noziedzīgā nodarījuma priekšmets. Tā bija mākslīgi radīta likumdevēja problēma. Krimināltiesībās analoģijas piemērošana nav pieļaujama. Ja likumā nav precīzi norādīts, ka termins „datorsistēma" attiecas arī uz telekomunikācijām, tad to plaši piemērot nav iespējams. Tādējādi likumdevējs

---

[433] Convention on Cybercrime// www.coe.int (aplūkots 2004.gada 24.martā)

nevis risināja problēmu pēc būtības, bet neveiksmīgi mēģināja likt ielāpus uz likuma robiem. Spilgts piemērs ir noziedzīga nodarījuma – telekomunikāciju patvaļīga izmantošana- kriminalizēšana. Lai atrisinātu jautājumu par personu, kas izmanto patvaļīgi telekomunikāciju pakalpojumus, atbildību, likumdevējs patvaļīgu telekomunikāciju pakalpojumu izmantošanu ir iekļāvis XVIII sadaļā „Noziedzīgi nodarījumi pret īpašumu" (Krimināllikuma 182. pants 2002. gada 28. maija redakcijā). Minētā panta dispozīcija noteic, ka atbildība iestājas *"par elektroenerģijas, siltumenerģijas, gāzes vai telekomunikāciju patvaļīgu izmantošanu, ja ar to radīts būtisks kaitējums,-"*

Šī darba mērķis nav analizēt minētā noziedzīgā nodarījuma sastāvu. Tomēr uzskatu, ka likumdevējs paredzot kriminālatbildību par patvaļīgu telekomunikāciju pakalpojumu izmantošanu, pielīdzinot tos elektroenerģijai, gāzei vai siltumenerģijai, ir pieļāvis kļūdu. Atbilstoši Kibernoziegumu konvencijas izpratnei, ierīce, kas piešķir tiesības izmantot telekomunikāciju pakalpojumus, ir automatizēta datu apstrādes sistēma vai datorsistēma. Ja persona izmanto citai personai piederošu telekomunikāciju ierīci un ievada autorizācijai nepieciešamo informāciju, tad viņš ir realizē patvaļīgu piekļuvi telekomunikāciju sistēmai un līdz ar to viņa darbības, no tehniskā redzes viedokļa ne ar ko neatšķiras no tehniski realizētas patvaļīgas piekļūšanas datorsistēmai. Taču juridiski šī atšķirība pastāv. Galvenais iemesls ir tas, ka nav skaidrības, ko saprast ar terminu datorsistēma. Piem., profesore V. Liholaja, komentējot KL 241. panta noziedzīgā nodarījuma sastāvu norāda, ka".. noziedzīgā nodarījuma priekšmets ir datorsistēmas tehniskie un informācijas resursi" Viņa atsaucas uz Latvijas Republikas Ministru kabineta 2000. gada 21. marta Ministru kabineta noteikumos Nr. 106 "Informācijas sistēmu drošības noteikumi", ietverto skaidrojumu, ka tehniskie resursi ir informācijas sistēmas sastāvdaļa, kurā ietilpst datori, datortīklu aparatūra un citas tehniskas iekārtas, bet informācijas resursi informācijas sistēmas sastāvdaļa.[434] Autors uzskata, ka komentāra autore ir nonākusi pretrunās, jo datorsistēmu identificējusi ar informācijas sistēmu.

---

[434] Krastiņš U., Liholaja V., Niedre A. Krimināllikuma zinātniski- praktiskais komentārs (3) Sevišķā daļa, profesora U. Krastiņa redakcijā. – Rīga "AFS", 2003., 226.lpp.

Ja tas ir tā, tad absolūti nav skaidrs, kāpēc minētais pants netiek piemērots patvaļīgai piekļuvei telekomunikāciju sistēmai, jo komentāra autori atzīst, ka datorsistēma sastāv gan no tehniskiem, gan informācijas resursiem, to skaitā no sistēmas lietotājiem pieejamās informācijas. To, ka pieslēgšanās telekomunikāciju tīklam ir saistīta ar elektronisku datu apstrādi, atzīst arī profesors U. Krastiņš. Komentējot KL 182. panta nodarījuma sastāvu, viņš norāda, ka".. telekomunikāciju patvaļīga izmantošana izpaužas, piemēram, nelikumīgi pieslēdzoties telekomunikāciju tīklam. Pa telekomunikāciju tīkliem pārraidāmās informācijas saņemšana, programmu lietošana, sakarā ar datu elektronisku apstrādi u tml. notiek bez tās personas atļaujas, kas atbild par telekomunikāciju izmantošanu"[435].

KL 241. panta 1.d. (līdz 01.06.2005.) nodarījuma priekšmets bija automatizēta datorsistēma. Galvenā atšķirība ir tā, ka datorsistēma ir automatizēta datu apstrādes sistēma, kura nav integrēta ar citām datu apstrādes sistēmām, tā saucamais nošķirtais (*stand alone*) variants. Datorsistēma ir jebkurš personālais dators, kas sastāv no procesora un monitora un klaviatūras, un peles, un citām periferiālām savstarpēji savienotām datu apstrādes ierīcēm. Taču tai nav obligāts nosacījums- lietotāju pieeja, respektīvi, tā nesniedz pakalpojumus. Pareizi norāda U. Miķelsons, ka no tehniskā aspekta terminus – „informācijas sistēma" un „dators", „datorsistēma", ne vienmēr pieļaujams lietot kā līdzvērtīgus.[436] Ne tikai no tehniskā redzes viedokļa, bet arī no juridiskā šie termini nav identiski piemērojami, un tos arī nepiemēro. Likumdevējs jau ar konkrētu aktu ir noteicis, ka informācijas sistēma ir strukturizēts tehnoloģiju un telekomunikāciju aprīkojuma un informācijas resursu kopums. Apstāklis, ka Krimināllikums nenoteica precīzas termina "automatizēta datorsistēma" robežas, bija tas kritiskais punkts, kas neļāva atzīt par Krimināllikuma 241. panta nodarījuma sastāva priekšmetu „telekomunikāciju sistēmu", kaut gan no tehniskā redzes viedokļa nav nekādas atšķirības, vai patvaļīga piekļuve tiek realizēta datorsistēmai pārvarot vai apejot tās aizsardzības līdzekļus, izmantojot sakaru līnijas vai tāda pati darbība veikta, izmantojot telekomunikāciju ierīci. Pēdējās darbības rezultātā persona, realizējot patvaļīgu piekļuvi

---

[435] Turpat, Krastiņš U., Liholaja V., Niedre A.,.33.lpp.

[436] Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas īpatnības. Rīga- Turība, 2003., 19lpp.

telekomunikāciju sistēmai, iegūt citai personai piederošas tiesības un iegūst pieeju un tiesības uz telekomunikāciju pakalpojumu. Šīs tiesības viņam piešķir ne jau fiziska persona, bet gan automatizēta datu apstrādes ierīce. Tātad patvaļīgā piekļūšana telekomunikāciju sistēmām tiek realizēta, izmantojot citai personai, likumīgajam lietotājam, piešķirtu tiesību.

*Krimināllikuma 241. panta 1.d nodarījuma objektīvās puses elementi*

1. Patvaļīga piekļuve. Kā redzams no KL 241. panta dispozīcijas (līdz 1.06.2005), tad par nodarījuma priekšmetu atzina automatizētu datorsistēmu. Kā jau iepriekš minēts, tad šī panta nodarījuma priekšmets bija ļoti šaurs, un faktiski tas attiecināms uz tādām datorsistēmām, kuras nav pievienotas datu pārraides vai telekomunikāciju tīkliem un kurām nav lietotāju pieeja. Tādejādi likumdevējs šeit paredzēja atbildību par patvaļīgu piekļūšanu atsevišķi novietotai (*stand alone*) datorsistēmai. Ja datorsistēma nav savienota ar tīklu, tad vienīgā iespēja, kā piekļūt šādai datorsistēmai ir fiziski iekļūt attiecīgā telpā, kur izvietota datorsistēma un iepazīties ar tajā esošu informāciju, jo tieši šis apstāklis ir atzīts par darbību, kas veido noziedzīgā nodarījuma objektīvo pusi.

Piekļūšanai ir jābūt *patvarīgai, neautorizētai, neatļautai, nelikumīgai.* Visi iepriekšminētie vārdi pēc būtības ir sinonīmi, un to pielietojums latviešu valodā ir identisks. Šeit var izdalīt divas pazīmes: 1) fizisku tuvošanos vai ieiešanu telpā, kurā atrodas datorsistēma, un 2) ieslēgt atsevišķi novietoto datoru vai izmantot to, kad tas atstāts bez uzraudzības ieslēgtā stāvoklī, un iepazīties ar informāciju.

Tiesiska fiziska iekļūšana telpā, kurā atrodas datorsistēma, nevar tikt uzskatīta par patvaļīgas piekļuves sastāvdaļu, savukārt, ja šī iekļūšana ir prettiesiska, tad personas darbībās ir saskatāmas KL 175. panta 3. daļas paredzētā nodarījuma pazīmes. Līdz ar to ir pilnīgi skaidrs, ka KL 241. panta izpratnē patvaļīgas piekļuves saturā neietilpst personas darbības fiziski īstenojot nelikumīgu piekļuvi telpai, kur izvietota datorsistēma.

To, ka ar datorsistēmu aizsardzību likumdevējs saprot tikai tādus pasākumus, kas tiek realizēti ar programmatūras līdzekļiem, pierādīja minētā panta 2.daļas (līdz 01.06.2005.) dispozīcija. Taču šaubas rodas arī par patvaļīgo piekļuves saturu, attiecinot to uz atsevišķi novietotu datorsistēmu, jo piekļuves tiesības sastāv no

diviem elementiem: 1) personai piešķirtiem identifikatoriem un to identifikācijas; un 2) sistēmas spējas pēc šiem identifikatoriem atpazīt lietotāju, respektīvi, autorizēt, un dot tam piekļuvi attiecīgiem sistēmas resursiem.

Iepriekšminētā Kanzasas Augstākās tiesas spriedumā krimināllietā *Štats pret Alenu*, tiesa precīzi definēja, ka *piekļūšana ir brīva iespēja kaut ko lietot*, respektīvi, ja kāds vēlas ierobežot pieeju savai informācijai, tam tā ir jāaizsargā. Brīvība ir spēja izmantot savas tiesības nepastāvot ierobežojumiem. Analizējot patvaļīgas piekļuves jēdzienu, ir jāievēro princips, ka viss, kas nav aizliegts, tas ir atļauts.

Tāda patiesībā ir informācijas sistēmu drošības noteikumos definētā piekļūšanas jēga. Ja nav piekļūšanas režīma, tad nevar runāt arī par tā pārkāpšanu. Ja persona, kas ir attiecīgas iestādes darbinieks, bez atļaujas, zinot, ka viņš nedrīkst izmantot savam kolēģim atbildībā esošo datorsistēmu, izmanto viņa nolaidību un piekļūst šiem resursiem, tad viņa darbības atkarībā no nodarītā kaitējuma apmēra kvalificējamas pēc citiem Krimināllikuma pantiem, piemēram, Krimināllikuma 318. panta kā dienesta stāvokļa ļaunprātīga izmantošana u.c. Līdzīgu viedokli pauž arī A. Voļevodzs.[437]

Taču šādas darbības nevar tikt kvalificētas kā patvaļīga piekļuve KL 241. panta izpratnē, jo tādā gadījumā, apdraudētā interese nav informācijas sistēmu drošības pazīme- pieejamība, bet gan var tikt apdraudēta konfidencialitāte, integritāte un personas mantiskās intereses. Itālijas Soda likuma 635. bis pants[438] kā atbildības nosacījumu patvaļīgai piekļuvei publiski pieejamām mājas lapām atzīst tā saucamās klusējošās gribas pārkāpumu, ka īpašnieks vai lapas autors, ievietojot mājas lapā informāciju, ir izteicis savu gribu, ka viņš vēlas to redzēt tieši tādu, tāpēc nevienam nav tiesību to mainīt bez viņa piekrišanas. Tam var piekrist, taču piekļuve publiski pieejamām mājas lapām un to satura izmainīšana nesatur KL 241. panta 1.d. paredzētā nodarījuma sastāvu, jo šeit apdraudētā interese ir informācijas integritātes nodrošināšana.

---

[437] Волеводз А.Г. Противодействие компютерным преступлениям. Правовые основы международного сотрудничества. Москва-Юрлитинформ, 2002.,с.72

[438] Codici e Leggi per l'udienza penale 2004", M. Chiavario, D. Manzione, T.Padovani, edizione Zanichelli 2004".

Līdz ar to autors uzskata, ka KL 241. panta 1. d. paredzēto nodarījuma sastāvu jau no tā pieņemšanas brīža nebija iespējams piemērot. Jebkurā gadījumā, ja arī lieta nonāktu līdz tiesai un tā patiesi iedziļinātos lietas būtībā, tad secinātu, ka šī panta izpratnē nav iespējams realizēt patvaļīgu piekļuvi automatizētai datorsistēmai kārtībā un veidā, kā to paredzējis likumdevējs, jo 1.d. paredzēto nodarījumu var veikt tikai fiziski kontaktējoties ar datorsistēmu. Ja šādu darbību rezultātā sistēmas īpašniekam radīsies konkrēts kaitējums, tad atkarībā no tā arī būs vērtējama vainojamās personas atbildība.

2. Radīta iespēja trešajai personai iepazīties ar sistēmā ievietoto informāciju. KL 241. panta 1.d. (līdz 01.06.2005.) dispozīcijā minētā darbība ir iespēja iepazīties ar sistēmā ievietoto informāciju. Ar informāciju Krimināllikuma 241. panta izpratnē saprot tos datorsistēmas- slēgta konteinera resursus, kas satur informāciju. Pie tādiem pieskaita sistēmprogrammas, lietojumprogrammas, sistēmu failus, datu failus, ieskaitot tos, kas satur glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju.[439] Informācija pārtop par juridisku kategoriju divu faktoru ietekmē: 1) ja informācija rada, groza vai izbeidz tiesiskās attiecības; 2) ja informācija ir aizsargāta.

Informāciju prasmīgs likumpārkāpējs var iegūt, realizējot vairākus pieslēguma mēģinājumus sistēmai un tādā veidā atklājot sistēmas vājās vietas u.tt. Neatkarīgi no tā, vai patvaļīgā pieslēgšanās sistēmai ir bijusi *veiksmīga vai arī neveiksmīga*, pārkāpējs var iepazīties ar informāciju. Par šādu informāciju šī panta izpratnē ir jāatzīst arī loģiskās aizsardzības metodēs pielietotie identifikācijas līdzekļi, sistēmas drošības parametri u.c.

3. Sekas. Juridiskajā literatūrā nav vienota viedokļa arī par to vai patvaļīgu piekļūšanu datorsistēmai uzskatīt par formālu vai materiālu noziegumu. U. Krastiņš norāda, ka par formālu nodarījuma sastāvu uzskatāms tāds sastāvs, kurš satur vienīgi tādas pazīmes, kas raksturo pašu kaitīgo darbību neatkarīgi no kaitīgo seku iestāšanās.[440] V. Liholaja[441] uzskata, ka šim nodarījumam ir formāls raksturs, jo tas

---

439 Ķinis U. Noziedzīgi nodarījumi datortīklos. Rīga -TNA, 2000., 94.lpp.

440 Krastiņš U. Noziedzīgs nodarījums. Rīga- TNA, 2000, 24lpp.

441 Krastiņš U., Liholaja V., Niedre A. Krimināllikuma zinātniski- prakstiskais komentārs 3. sevišķā daļa U. Krastiņa redakcijā. , Rīga -AFS, 2003. 226.- 227. lpp.;

ir pabeigts ar panta dispozīcijā norādīto darbību izdarīšanu. Tomēr jautājums par to, kad ir pabeigta objektīvās puses darbība- iepazīšanās ar informāciju- bija absolūti neskaidrs. Tāpēc nevar piekrist viedoklim, ka šis nodarījuma sastāvs bija formāls. Salīdzināsim Krimināllikuma 241. panta 1.d. (līdz 01.06.2005.) redakciju ar KF Krimināl kodeksa 272. pantu "Patvaļīga piekļūšana datorinformācijai".

KF KK 272. panta 1.d. "Patvaļīga piekļuve ar likumu aizsargātai datorinformācijai, tas ir, tādai, kas atrodas datu nesējā vai elektronu skaitļojamās mašīnas (ESM) sistēmās, vai to tīklos, kā rezultātā tā sabojāta, iznīcināta, bloķēta, modificēta, vai kopēta vai saistīta ar ESM sistēmas vai datorsistēmas vai tīklu darbības traucēšanu."[442] I. Klepickis, analizējot KF ietvertos datornoziegumu sastāvus, norāda, ka tie visi, izņemot KF KK 273. p. 1. d. "Kaitīgo programmu, kas paredzētas ESM resursu ietekmēšanai, izgatavošana, izmantošana vai izplatīšana", ir atzīstami par materiāliem noziegumiem.[443] A. Voļevods norāda, ka KF KK 272. pantā paredzētais nodarījums skaitās pabeigts no brīža, kad likumā paredzētās sekas sāk iestāties[444], bet B. Jaceļenko konkrēti norāda, ka KF KK 272. panta objektīvās puses obligāta pazīme ir kaitīgu seku rašanās īpašniekam vai turētājam.[445]

Krimināllikuma 241. panta 1. daļa (līdz 01.06.2005.) neparedzēja atbildību tikai par piekļūšanu, bet piekļūšanu ar nosacījumu *"ja ar to nepiederīgai personai radīta iespēja iepazīties ar informāciju"*. Tulkojot šīs abas normas no gramatiskā viedokļa, abas tās saturēja nosacījumus pie kuriem iestājas atbildība. Faktiski abas šīs iepriekšminētās izteiksmes formas no gramatiskās tulkošanas viedokļa semantiski satur vienu un to pašu jēgu. No tā var izdarīt secinājumu, ka iepazīšanās ar informāciju bija sekas, kas seko patvaļīgai piekļuvei. Ja likumdevējs būtu vēlējies šo nodarījumu atzīt par formālu, tad pants būtu konstruējams tādā veidā, ka jebkura patvaļīga piekļuve ir uzskatāma kā datora miera traucēšana un pati par sevi ir krimināli sodāma. Tādā gadījumā autors pilnīgi piekrīt, ka šāds nodarījums būtu formāls.

---

442 Уголовный кодексс Российской Федерации. Полный сборник кодексов Российской Федерации. Москва: Аст, 1999

443 Уголовное право Российской федерации. Особенная часть. Подю ред. Б.В. Здравомыслова. Москва-Юристь, 1999.б с. 352

444 Волеводз А.Г. Противодействие компютерным преступлениям. Правовые основы международного сотрудничества. Москва-Юрлитинформ, 2002.,с.70

445 Росийское уголовное право. Особенная ч. Учебник. Под. Ред. М.П. Журавлева и С.М. Никулина. Москва- Спарк, 1998,с. 337

Formāla noziedzīga nodarījuma būtība parasti ir kāda vispārobligāta tiesiska noteikuma nepildīšana, kā rezultātā iestājas krimināalatbildība. Informāciju sistēmu drošība nav un nedrīkst būt valsts vispārobligātu tiesību normu objekts, kā, piem., „Likums par nodokļiem" u.c. Jāpiezīmē, ka likumdevējs pieņemot Krimināllikumu, bija iecerējis tieši tādu kārtību noteikt, jo Krimināllikuma Pārejas noteikumu 3.p. bija uzdots izstrādāt līdz 1998. gada 1. augustam izstrādāt un pieņemt noteikumus "Par piekļūšanu datorprogrammām un informācijas sistēmu drošību".

Autors vadīja šo darba grupu, un jau sākotnēji tika iesniegts Ministru Kabinetā priekšlikums grozīt darba grupas uzdevuma saturu, jo ir pilnīgi nepieņemami demokrātiskā sabiedrībā valstij pieņemt vispārobligātus noteikumus, kas attiektos vienādi uz visām valstī esošām informācijas sistēmām. ANO OECD 1992.gada vadlīnijas par ISD drošību[446] noteic 9 principus, kuri jāpiemēro, veidojot ISD politiku. Izcelsim divus: 1) *proporcionalitātes princips*- drošības prasības dažādām atsevišķām informācijas sistēmām atšķiras, drošības līmeņiem, izmaksām, pasākumiem, praksei un procedūrām jābūt atbilstīgām un proporcionālām informācijas sistēmu uzticamības pakāpei un līmenim, un iespējamo kaitējumu iespējamībai, smagumam un apjomam.; 2) *demokrātiskais princips*- ISD jābūt savietojamai ar datu un informācijas likumīgu lietošanu un plūsmu demokrātiskā sabiedrībā. Tas nozīmē, ka nekādā gadījumā nedrīkst pieļaut pārmērīgu valsts iejaukšanos šajos procesos. Realizējot proporcionalitātes principu, ir pilnīgi neiespējami sadalīt pēc iespējamā apdraudējuma pakāpes valstī esošās informācijas sistēmas. MK Noteikumos Nr. 106 eksperti mēģināja ietvert kā noteikumu subjektus visas IS, kas tiek finansētas no valsts vai pašvaldību budžeta, taču vēlāk noteikumi tika pildināti un attiecināti uz visām informācijas sistēmām, kas apstrādā personu datus. Tas izsauca lielu sabiedrības kritiku, un tās rezultātā šos noteikumus atcēla. Patlaban nobeiguma stadijā ir Valsts informācijas sistēmu drošības noteikumu projekts. Pārējās sistēmas pašas veido savu ISD politiku un ir par to atbildīgas tikai savu lietotāju priekšā. Taču KL 241. panta 1.d. priekšmets ir atsevišķa datorsistēma, kas parasti tiek veidota tā, ka tai ir tikai viens lietotājs.

---

[446] Informācijas un komunikāciju tiesības II. Sējums. U. Ķiņa redakcijā. Rīga- Turība, 2002., 506-511

Tāpēc arī nekāda speciāla kārtība, izņemot gadījumus, kas tiek apstrādāta informācija, kas satur valsts noslēpumu, netiek izstrādāta. Ja nav kārtības, tad nevar būt arī patvaļības. Nosacījuma formulējuma saturs – ja ar to nepiederīgai personai radīta iespēja iepazīties ar sistēmā ievieto informāciju bija ļoti plašs.

Piemērs. N. Iekļūst K kabinetā un, izmantojot to, ka darbiniece nav uzlikusi datoram loģisko aizsardzību, ierauga, ka uz ekrāna atrodas informācija, viņš šo informāciju iegaumē. N nav veicis nekādas darbības saistībā ar datoru, nav pat fiziski pieskāries tam, bet šo informāciju viņš iegaumēja. Var pierādīt, ka aizdomās turamā persona patvaļīgi iegāja K kabinetā, bet nav pierādāms, ka tā ir iepazinusies ar informāciju, jo viņš to nekur neizmanto.

V. Krilovs šādu gadījumu nosauc par nestandarta situāciju datorsistēmas darbībā un norāda, ka atbildības nosacījums var būt tikai personas rīcība, nelikumīgi izpaužot informāciju trešajām personām.[447]

Ar iepriekšminēto piemēru vēlējos pierādīt, ka iepazīšanās ar informāciju nebūt nav tik viegli definējams jēdziens, ka tam varētu piedēvēt formāla nodarījuma sastāvu, ka darbība ir pabeigta ar iepazīšanās faktu, jo, lai atzītu, ka persona ir iepazinusies ar informāciju, tad acīm redzot, nepieciešams konstatēt kādus blakus apstākļus, kas tieši vai netieši pierādītu, ka šāda iepazīšanās ir notikusi.

*Krimināllikuma 241. panta 2. daļas objektīvās puses analīze*

Krimināllikuma 241. panta 2. daļa (līdz 01.06.2005) papildus 1. d. paredzētajiem nosacījumiem paredzēja alternatīvas objektīvās puses pazīmes - patvaļīgu piekļuvi, pārvarot programmatūras aizsardzības līdzekļus vai ar pieslēgšanos sakaru līnijām.

1. Programmatūras aizsardzības līdzekļi jeb loģiskās aizsardzības līdzekļi. Kā minēts iepriekš, tad informācijas sistēmu drošība ir vispārējās drošības neatņemama sastāvdaļa. Reālā dzīvē katram īpašniekam ir jārūpējas par savas mantas saglabāšanu. To parasti veic, iegādājoties attiecīgu atslēgu vai citu aprīkojumu vai pieslēdzot telpas apsardzes firmu novērošanai. Līdzīgi pasākumi rūpīgam saimniekam ir jāveic saistībā ar informācijas sistēmu drošību, kuras aizsardzības pasākumus iedala divās grupās: 1)fiziskās aizsardzības pasākumi, kuros ietverti tie pasākumi, kas jāveic, lai pasargātu sistēmas no fiziskiem apdraudējumiem; 2) loģiskās aizsardzības pasākumi, programmatūras komplekss, kas nepieciešams sistēmu resursu aizsardzībai no apdraudējumiem, kas saistīti ar datorsistēmu

---

[447] Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва- Юриспрудения. 1999., с. 654

ekspluatāciju, lietotāju identifikāciju, risku novērtēšanu u.c. Par sistēmas aizsardzību ar programmatūras līdzekļiem var uzskatīt jebkuru paroli, piekļuves kodu vai citu loģiskās aizsardzības līdzekli. Kvalificējot darbības pēc šī nodarījuma, nav svarīgi, vai programmatiskā aizsardzība ir vienkārša vai sarežģīta. Tādēļ par datortehnikas programmatūras aizsardzības līdzekļiem jāatzīst gan tādas parole vai kods, kas sastāv no viena simbola, gan arī tādas sistēma, kur aizsardzība tiek nodrošināta ar trīskāršu identifikāciju, ugunsmūriem un citiem programmatūras līdzekļiem.

Kā minēts iepriekš, tad demokrātiskā sabiedrībā nav prakses, kur likumdevējs būtu noteicis ar vispārobligātu aktu šādas aizsardzības minimālās prasības visām valstī esošām datorsistēmām. Izņēmums ir tikai valsts informācijas sistēmas, kuru pienākums ir nodrošināt normālu valsts eksistencei nepieciešamo funkciju izpildi.[448] Tomēr šīs prasības attieksies tikai uz šauru juridisko personu loku Tāpēc tā ir katra sistēmas īpašnieka tiesība un reizē arī pienākums atbilstoši savām iespējām gādāt par sistēmas resursu loģisko aizsardzību.

2. Analizējot darbību pārvarēšana saturu, jāsecina, ka likumdevējs tieši nav norādījis, ka atbildība iestājas arī par šo līdzekļu apiešanu (*by passing*). Arī komentāros šis jautājums nav skaidrots. Ja mēs analizējam šo saturu salīdzinošo krimināltiesību aspektā, tad jāatzīst, ka darbība saistībā ar sistēmas loģiskās aizsardzības līdzekļu pārvarēšanu tiek traktēta dažādi, piem., Nīderlandes Sodu likuma 138 a. pantā „Nelikumīga piekļūšana" 2.d. ja tā izdarīta, salaužot aizsardzības sistēmu; Grieķijas Sodu likuma 370C § 2 panta dispozīcija satur nosacījumu, ja darbības, izdarītas pārvarot sistēmas aizsardzības pasākumus; Somijas Soda likuma 38. nodaļas 8. paragrāfs paredz arī krimināatbildību par „Datu traucēšanu", pārvarot tās aizsardzības pasākumus. Vairākos ASV štatos krimināllikumā ir iekļauts patvaļīgas piekļuves nosacījums sistēmu aizsardzības līdzekļu salaušana vai apiešana.

Analizējot Eiropas valstu krimināllikumus, var secināt, ka ar terminu aizsardzības sistēmu salaušana, pārvarēšana saprot arī šādu aizsardzības sistēmu

---

448 Valsts informācijas sistēmu likums. Latvijas Vēstnesis 2002.gada 25. maijs.

apiešanu nolūkā patvaļīgi piekļūt informācijas resursiem, piemēram, Trojas zirga ievietošanu datorsistēmā u.c. Tāpēc autors uzskata, ka KL 241. panta 2. d. nosacījums *„datu apstrādes sistēmas aizsardzības līdzekļu pārvarēšana"*, ietver sevī gan šo līdzekļu salaušanu, gan apmānīšanu, gan apiešanu, gan jebkādu citu iedarbību, kuras rezultātā šie aizsardzības līdzekli nespēj pildīt savu funkciju un atļauj vai atvieglina patvaļīgu piekļuvi datorsistēmas resursiem.

3. Pieslēgšanās sakaru līnijām. Redakcijā līdz 01.06. 2005.) Krimināllikuma 241. panta 2.d. paredzēja atbildību tad, ja persona piekļuvi veikusi pieslēdzoties sakaru līnijām. Kā jau minēju iepriekš, tad uzskatu, ka, nosacījums, pieslēgšanās sakaru līnijām faktiski ir tādu datorsistēmu, kas var tikt atzītas par patvaļīgas piekļuves priekšmetu, neatņemama sastāvdaļa, jo starptautisko krimināltiesību izpratnē ar patvaļīgu piekļuvi datorsistēmām saprot piekļuvi no attāluma, ko realizē tikai caur sakaru līnijām. Taču šis nosacījums bija galvenais pamats, lai varētu saukt personas pie kriminālatbildības par patvaļīgu piekļuvi datorsistēmām. Jo, ja sistēma nav pieslēgta sakaru līnijai, tad nav iespējams tai piekļūt patvaļīgi šī panta izpratnē.

Piemērs. Vidzemes apgabaltiesas prokuratūra ierosināja krimināllietu pret S.C. Viņš 2003. gada pavasarī **izveidoja datorprogrammu "D" un, izmantojot lokālo datortīklu**, ievietoja programmas tādā sistēmas direktorijā, kur tās tika automātiski palaistas, ieslēdzot datoru. S.C. **nelikumīgi ieguva** arī programmu "A" **un ieguva šīs programmas lietotāja vārdu un paroli**. Tas viņam izdevās tāpēc, ka viņš izveidoja speciālu programmu, kas savāca informāciju par cietušās G. Ā. datora tastatūrā nospiestiem taustiņiem.
Tādējādi viņš **ieguva visu informāciju**, kas notiek cietušās G.A. datorsistēmā, tai skaitā arī viņas lietotāja vārdu un paroli, **kas deva iespēju autorizēties programmā** "A", šī programma deva S.C. informāciju, ka programmas lietotājam ir apstiprināts digitālais paraksts, kas glabājas pie cietušās disketē.
Lai iegūtu digitālo parakstu, S.C. papildināja minēto monitoringa programmu ar papildus iespēju, kas ilgāk pēc noteikta laika, bet ne ilgāk kā 30 minūtes, pārbaudīja G.A. datora diskešu iekārtu un nokopēja tajā laikā ievietotās disketes saturu, datorā noteiktā vietā izveidotā direktorijā. Tas deva iespēju viņam uz sava portatīvā datora nelikumīgi uzstādīt a/s Unibanka speciāli cietušai izveidotu datorprogrammu "A" un uzdot ar šīs programmas palīdzību a/s Unibanka izpildīt maksājumu uzdevumus, kas bija parakstīti ar cietušās elektronisko parakstu. S.C. veica ari citas darbības, lai **piekļūtu Lattelekom VTN iekšējam datortīklam,** un visu šo darbību rezultātā izkrāpa no cietušās firmas 35026.80 latu.

Kā redzams no iepriekšminētā piemēra, tad šajā gadījumā S.C. nelikumīgi, bez tiesiska pamata, no attāluma, izmantojot datu pārraides tīklu, ieguva G.A. firmai piederošos identifikatorus, paroles, kodus, digitālo parakstu. Viņš iepazinās arī ar sistēmā ievietoto informāciju un izmantoja šo informāciju savām vajadzībām. Tieši tas, ka vainojamā persona izmantoja sistēmā esošo informāciju savu noziedzīgo mērķu sasniegšanai, dod mums pamatu secināt, ka iepazīšanās patiešām ir notikusi.

Piemērs. LR IeM VP GKrPP Ekonomikas policijas pārvaldes lietvedībā atrodas kriminālliета Nr. 11810014003, kas ierosināta 2003.g. 3. decembrī pēc Krimināllikuma 241. p.2 .d. par patvaļīgu piekļūšanu automatizētai datorsistēmai "tulpe.latnet.lv", **pārvarot datortehnikas programmatūras aizsardzības līdzekļus** izmantojot tam speciāli paredzētu programmatūru (skriptu "php" programmēšanas valodā), kā rezultātā lietotājs 2003. gada 21. oktobrī no IP adreses 81.198.23.148 **iepazinās ar svešu sistēmā ievietoto informāciju**.

Pirmstiesas izmeklēšanas gaitā tika noskaidrots, ka 2003. gada 21. oktobra naktī, plkst. ***01:03*** no IP adreses 81.198.23.148 nezināms lietotājs, kuru pēc identifikācijas paroles ievadīšanas sistēma **atpazina (identificēja) kā legālo mājas lapas www.antonia.lv īpašnieku**, kas reģistrēta "LATNET" (LU MII Latnet laboratorijas) serverī "Tulpe" uz N.S.vārda, veica **patvaļīgu piekļūšanu visai automatizētai Interneta datorsistēmai** www.tulpe.lv, pārvarot programmatūras aizsardzības līdzekļus, ļaunprātīgi izmantojot sevišķo klientu paplašinātās iespējas, kuras viņam izsniedza servera sistēma, kā klientam "antonia". Rezultātā viņam kļuva zināma servera www.tulpe.lv **svešu mājas lapu lietotāju privātā informācija (lietotājvārdi, paroles, mājās lapu satura informācija u.c.)**. Pēc kā lietotājs no IP adreses 81.198.23.148 2003.gada 21.oktobrī plkst. ***02:03***, izmantojot pirms tam iegūto informāciju (lietotājvārdus un paroles), veica patvaļīgu piekļūšanu (nesaņemot atļauju no mājas lapu īpašniekiem) svešām mājas lapām, tādā veidā **iepazīdamies ar citu servera www.tulpe.lv lietotāju privāto informāciju un saglabājot to savā datorā** (lejupielādējot).

21.10.2003. plkst.06:08:24 lietotājs no IP adreses 81.198.23.148, no e-pasta kastītes acidus@acidus.lv, sevi identificējot kā "K | NG", nosūtīja e-pasta vēstuli uz e-pastu info@pods.lv, ar nolūku publicēt publiski pieejamā interneta mājas lapā www.pods.lv informāciju, ka "LATNET" (tulpe.lv) nav pienācīgi aizsargāts, kā arī informāciju, kādā veidā bija iespējams šo aizsardzību pārvarēt, izklāstot tieši, kā iespējams piekļūt citu servera lietotāju informācijai, veicot izmaņas "PHP" skriptā, aprakstot tā darbības principu. 24.10.2003. plkst.02:38:28 publiski pieejamā interneta forumā "journal.bad.lv" viens no pastāvīgajiem apmeklētājiem ar iesauku "kenins" norādīja, ka serveriem www.tulpe.lv un www.sisenis.lv ir iespējams nolasīt jebkuru sistēmas failu, norādīja arī to, ka ir pieejams sistēmas paroļu fails. Ievietojot šo rakstu lietotājs "kenins" sevi identificēja kā "K | ING", norādot savu e-pasta adresi acidus@acidus.lv.

24.10.2003. plkst. 06:58 no IP adreses 81.198.23.145 **tika veiktas izmaiņas servera** www.tulpe.lv lietotāja "BDG" piederošās mājas lapas failā "index.php", kā rezultātā katru reizi, kad kāds apskatīja mīnēto mājas lapu, tika nosūtīta vēstule uz "LATNET" e-pastu latnet@latnet.lv ar pārmetumiem par to, ka "LATNET" ir slēdzis viņam piederošo direktoriju "www.ltn.lv/~wde/; mājas lapu www.acidus.lv.

Arī piemērā par patvaļīgu piekļūšanu datorsistēmai "tulpe. latnet. lv" redzams, ka aizdomās turamā persona pieslēgumu izdarījusi no attāluma. Tā ir rīkojusies patvaļīgi, jo izmantojusi citai personai piederošus identifikatorus, pārkāpusi likumīgam lietotājam piešķirto tiesību apjomu, piekļuvusi tādiem informācijas apgabaliem, uz kuriem pieeja tai nebija atļauta. Līdz ar to abos gadījumos personu darbības ir kvalificētas pēc KL 241. panta 2. daļas, jo viņu darbībās saskatāmas visas KL 241. panta 2.d daļas dispozīcijā paredzētās pazīmes. Tās ir vienas no pirmajām nopietnākajām lietām mūsu valstī, kas ierosinātas pēc KL 241. panta 2.d.

KL 241. panta noziedzīgā nodarījuma sastāvs ir materiāls sastāvs, jo atbildība iestājas tikai tad, ja ir pierādīta cēloņsakarība starp patvaļīgu piekļuvi un sekām, ka persona ir iepazinusies ar informāciju un ka šī iepazīšanās ir notikusi tieši tāpēc, ka

persona ir īstenojusi patvaļīgo piekļuvi, to skaitā arī ar pieslēgšanos sakaru līnijām vai pārvarot sistēmu drošību.

*Krimināllikuma 241. pants Patvaļīga piekļūšana automatizētai informācijas sistēmai (28.04.2005.)*

2005.gada 28. aprīlī Saeima pieņēma būtiskus grozījumus Krimināllikumā, to starp arī Krimināllikuma 241- 244 pantos. Šo grozījumu nepieciešamību noteica tas, ka Latvija ir vairāku starptautisku organizāciju dalībvalsts. Vairākas no tām, to skaitā Eiropas Padome, Eiropas Savienība, Pasaules Tirdzniecības organizācija, ANO, veic lielu darbu, lai izstrādātu rekomendācijas, konvencijas un citus normatīva rakstura dokumentus ar mērķi izveidot vienotu stratēģiju kibernoziegumu[449] apkarošanā. Tāpēc, izstrādājot grozījumus Krimināllikumā un konstruējot jaunus noziedzīga nodarījuma sastāvus, darba grupai bija jāizmanto visa starptautisko organizāciju uzkrātā pieredze šo noziedzīgo nodarījumu apkarošanā. Īpaši jāizceļ Eiropas Padomes Kibernoziegumu Konvencija, kura tika parakstīta 2001. gada 23. novembrī Budapeštā, un Eiropas Savienības Padomes ietvarlēmums „Par uzbrukumiem informācijas sistēmām". Tāpēc īpaši pievērsīsišos šo dokumentu analīzei, jo patlaban norit aktīvs darbs, lai Latvija pievienotos Kibernoziegumu konvencijai un to ratificētu, kā arī likumdošanas pasākumiem, lai saskaņotu Latvijas likumus ar Eiropas Savienības prasībām.

*Eiropas Padomes Kibernoziegumu konvencija*

Kibernoziegumu konvencija datorsistēmu definē kā ierīci, kas sastāv no tehniskiem un programmatiskiem līdzekļiem, kas nepieciešami digitālo datu automātiska apstrādes procesa nodrošināšanai. Tā var ietvert datu ievades, izvades un saglabāšanas iespējas. Tā var būt novietota atsevišķi vai savienota tīklā ar citām līdzīgām ierīcēm. Termins „automātisks" nozīmē, ka tā funkcionē bez tiešas cilvēka iejaukšanās. Termins „datu apstrādes process" nozīmē to, ka sistēmā esošās datorprogrammas savu paredzēto instrukciju robežās iedarbojas uz sistēmā esošiem datiem.[450]

---

[449] Noziedzīgu nodarījumu, kas saistīti ar automatizētu datu apstrādes sistēmu un datortīklu izmantošanu, starptautiskais *sui generis* apzīmējums// http://www.onelook.com/?w=cybercrime&ls=a (aplūkots 2004.gada 22. martā).

[450] Cybercrime Convention Explanatory report.CM ( 2001) 144. addendum, para 23

Tīkls ir mijiedarbība starp divām vai vairākām datorsistēmām. Tīkls var būt ikdienišķs (vads vai kabelis), radio (radio, infrasarkano staru, satelīta) vai abi. Tīkls var būt izvietots mazā ģeogrāfiskā vietā (lokālais datortīkls) vai savienots ar plašu ģeogrāfisku apvidu (plaša apgabala tīkls), un šādi tīkli var atrasties savstarpējā mijiedarbībā. Internets ir globāls tīkls, kas atrodas mijiedarbībā ar daudziem tīkliem, kas lieto vienus un tos pašus protokolus[451]. Datorsistēmas tīklā var būt savienotas kā gala termināli vai arī kā ierīces, lai nodrošinātu tīkla pārraidi. Svarīgākais kvalifikācijai ir tas, lai tīkli tiktu izmantotu datu pārraidei.[452]

Modernu telekomunikāciju sistēmu vada centrālā procesora bloks, kas pilnīgi autonomi veic telekomunikāciju tīklā pārraidāmo datu apstrādes procesu. Tas pārraida un nodrošina savienojumus, līdz ar to nav nepieciešams nodalīt datorsistēmu no telekomunikāciju sistēmas, datortīklu no telekomunikāciju tīkla utml. Šobrīd jau attīstās digitālā televīzija, bet tas nozīmē, ka sabiedrībai tiks piedāvāts "universālais pakalpojums" autorizēta lietotāja iespēja caur vienu kabeli no viena pieejas punkta piekļūt un izmantot vairākus pakalpojumu veidus vienlaicīgi. Līdz ar to nevar izslēgt gadījumus, kad personas vēlēsies patvaļīgi piekļūt arī universālo pakalpojumu nodrošinošai sistēmai.

Juristam ir svarīgi izprast tos principus, kas ir datorsistēmas, telekomunikāciju sistēmas, datortīkla, telekomunikāciju tīkla uzbūves pamatā, bet ne izprast, kā darbojas katrs sistēmas mezgls vai kā uzbūvēts procesors. Datortīklu un datorsistēmu uzbūves principi nemainīsies pat straujā informācijas un tehnoloģijas zinātniskā progresa ietekmē. Jo vispārīgāka būs šī tehniskā resursa definīcija, jo vieglāk tā būs piemērojama tiesību praksē. Tāpēc viena no svarīgākajām atziņām, kas bija jāievēro, konstruējot jauno Krimināllikuma 241. panta redakciju, ka nav nepieciešams speciāli nodalīt telekomunikāciju sistēmu un telekomunikāciju pārraides tīklu no datorsistēmas un datortīkla.

---

451 Lai dators varētu strādāt internetā, vai kā datorspeciālisti žargonā saka, "runāt tīkla valodā", tika izstrādāti speciāli protokoli, kas nodrošina interneta darbību. Raksturīgākie protokoli, kas nodrošina datora darbību interneta ir TCP/IP Transmission control protocol/Internet protocol; HTTP –hiperteksta pārraides protokols; SMTP protokols- parastā pasta pārraides protokols; FTP –failu pārraides protokols u.c.

452 Convention on cybercrimes Explanatory report CM (2001) 144 addendum, para 24

Tulkojot konvencijas tekstu pēc tās jēgas, var secināt, ka termins „datorsistēma" šeit tiek piemērots paplašināti. Konvencijā ir speciāli izdalīti nodarījumi pret informācijas sistēmu drošību. Līdz ar to ir skaidrs, ka speciālisti šeit runā par plašāku priekšmetu, kas ietver sevī tehniskos resursus, piem., automatizētas datu apstrādes ierīces un programmatiskos resursus, kas nepieciešami gan tehnisko resursu loģiskai aizsardzībai, gan arī sistēmas apritē esošās informācijas apstrādes nodrošināšanai, to skaitā informācijas pārsūtīšanai pa datortīkliem, distances informācijas pakalpojumu sniegšanu u.c. Konvencijā patvaļīgā piekļūšana netiek attiecināta uz gadījumiem, kad persona fiziski piekļūst atsevišķi izvietotai datorsistēmai, neizmantojot piekļuvi caur datortīkliem. Tādējādi, jāsecina, ka lielākā daļa valstu par krimināli sodāmu atzīst tikai tādu patvaļīgu piekļūšanu datorsistēmu resursiem, kas izdarītas no attāluma, izmantojot datu pārraides vai telekomunikāciju tīklus.

Ja runā par informācijas sistēmu drošību, tad apdraudētai vienībai jābūt informācijas sistēmai, kas ietver sevī gan datorsistēmas, gan tīklus, gan telekomunikācijas un citus elementus, kas nepieciešami datu apstrādes procesa nodrošināšanai.[453]

*ES Padomes ietvarlēmums par uzbrukumiem informācijas sistēmām*

Latvijai kā ES dalībvalstij ir ļoti svarīgi saskaņot savu krimināltiesisko bāzi ar tām prasībām, ko izvirza Eiropas Savienība savām dalībvalstīm. Kaut gan krimināltiesisko attiecību sfēra nav tiešs ES vadošo institūciju regulējuma objekts, taču aizvien vairāk pasākumu tiek veikti, lai visā ES teritorijā panāktu likumu vienveidīgu piemērošanu, kas savukārt dotu iespēju pastiprināt cīņu pret organizēto noziedzību, terorismu, netīrās naudas atmazgāšanu, ekonomiskiem noziegumiem, to skaitā arī kibernoziegumiem.

ES Padomes ietvarlēmumā par uzbrukumiem informācijas sistēmai 1.a punkts definē informācijas sistēmu kā savstarpēji savienotu ierīču grupu, tai skaitā arī jebkuru elektronisko komunikāciju tīklu, kas izveidotas ar mērķi veikt automatizēto datu apstrādi. Minētā dokumenta paskaidrojošā memoranda 1.1. punktā norādīts, ka

---

[453] Valsts informācijas sistēmas likums. Latvijas Vēstnesis.2002.gada 22. maijs.

termins *„informācijas sistēma"* šajā dokumentā tiek lietots plašākā nozīmē un attiecas gan uz savstarpēji savienotiem tīkliem gan arī datus saturošām sistēmām. Šajā izpratnē jēdziens „informācijas sistēma" ietver sevī atsevišķi novietotus datorus, personālos digitālos organizētājus, telefonus, mobilos telefonus, intranetus, ekstranetus, serverus un citu interneta infrastruktūru.[454]

Šāda nostādne pilnīgi atbilst Latvijā izstrādātajam informācijas sistēmu drošības regulējumam. Jāatzīst, ka vairākas ES dalībvalstis, piem., Nīderlande, Dānija, Somija, Lielbritānija un Zviedrija, neatbalsta formulējumu, ka informācijas sistēmas definīcijā tiek iekļauti arī datortīkli, jo tas ir pretrunā ar Kibernoziegumu konvencijas 1.p. a. doto datorsistēmas definīciju.[455] Par šo viedokli var diskutēt, jo, kā jau minēts iepriekš, tad konvencija paredz kriminalizēt nodarījumus pret informācijas sistēmu drošību. Latvija pilnīgi atbalsta ES viedokli par informācijas sistēmas jēdziena saturu, jo līdzīga pieeja jau ir normatīvi nostiprināta Valsts informācijas sistēmu likumā.

Tādējādi apdraudējuma priekšmets ir nevis automatizēta datorsistēma, kas neietver sevī ne telekomunikācijas, ne tele un datu pārraides tīklus, bet gan informācijas sistēma. Tomēr, iekļaujot likuma tekstā terminu „informācijas sistēma" var rasties zināmas interpretācijas problēmas, jo faktiski informācijas sistēma ir jebkura uzņēmuma lietvedība, kas sastāv no fiziskiem resursiem - plauktiem, galdiem - un informācijas resursiem.

Tāpēc, izstrādājot Krimināllikuma 241. panta jauno redakciju, autors ieteica izmantot terminu **"automatizētā datu apstrādes sistēma" (ADAS)**. Argumenti, kāpēc tika izvēlēts šāds termins ir šādi:

1) šis termins precīzi apzīmē to, ka Krimināllikuma 241.- 244 pantā nodarījuma priekšmets ir tikai tās sistēmas, kas veic automatizētu datu apstrādes procesu, tas ir, šo datu apstrādes procesu vada un organizē fiziska persona, pamatojoties uz programmu, kas spējīga veikt automātisko datu apstrādi;

---

454 Proposal for a Council framework decision on attacks against information systems. Explanatory memorandum Brussels COM (2002) 173 Final 19.04.2002 2002/0086 (CNS)

455 Proposal for a Council framework decision on attacks against information systems. Brussels 11.02.2003. Nr.6236/03

2) jebkurā ADAS ir savstarpēji saistīti jeb integrēti informācijas un tehniskie resursi, tādējādi, mēs nodalām no nodarījumiem pret informācijas sistēmu drošību piekļūšanu publiski pieejamām mājas lapām vietās, kur to funkcionēšanu nodrošina atbalsta tehnoloģijas nolūkā tās sabojāt vai izmantot citos noziedzīgos nolūkos, piem., krāpniecisku darbību veikšanai, goda un cieņas aizskaršanai, huligānisku darbību izdarīšanai u. c.;

3) termins „automatizēta datu apstrādes sistēma" ietver sevī gan individuālu datoru, datorsistēmu, gan mobilās un stacionārās telekomunikāciju iekārtas, gan arī tele un datu pārraides tīklus;

4) tas ir tehnoloģiski neitrāls termins, kura saturu nevar ietekmēt moderni zinātnes sasniegumi tiktāl, kamēr vien pastāvēs automatizēts datu apstrādes process. Konstruējot Krimināllikumā noziedzīga nodarījuma sastāvus pret informācijas sistēmu drošību, ir jāievēro divi faktori: Pirmkārt, šiem nodarījumiem nereti ir starptautisks raksturs. EP Kibernoziegumu Konvencijas preambulā[456] un ES Padomes priekšlikumos par ietvarlēmumu[457] par uzbrukumiem informācijas sistēmām īpaši uzsvērta nepieciešamība veidot ES teritorijā koordinētu pasākumu kompleksu cīņai ar šiem apdraudējumiem. No tā izriet otrais nosacījums, ka šo noziedzīgo nodarījumu sastāviem ir jābūt tādiem, kas saskaņoti ar iepriekšminētajiem starptautiskajiem dokumentiem. Konstruējot šos noziedzīgo nodarījumu sastāvus, tie ir jāveido tā, lai tos varētu piemērot arī pret personām, kas uzbrukumus Latvijas teritorijā esošām ADAS veic no citu valstu teritorijas.

Piemērs. 2001. gada 21.-23. novembra Kibernoziegumu konferencē Budapeštā, Polijas pārstāvis, Torunas universitātes profesors A. Adamskis savā ziņojumā norādīja, ka 1998. gadā no 1000 valstī reģistrētiem informācijas sistēmu apdraudējumiem 400 bija izdarīti no citas valsts teritorijas[458], bet Japānas delegācijas ziņojumā bija norādīts, ka 2001. gadā no 959 patvaļīgas piekļuves informācijas sistēmām gadījumiem 418 bija izdarītas no citas valsts teritorijas.[459]

Saskaņā ar Konvencijas prasībām šādu personu saukšanai pie atbildības un izdošanai nepieciešamais nosacījums ir duālā jurisdikcija, tas ir, lai darbība tiktu

---

456 www.coe.int (aplūkots 2005.gada 12. janvārī).

457 Proposal for a Council framework decision on attacks against information systems. COM (202) 173 final

458 Computer crime in Poland: three years' experience in enforcing the law. Contribution by Andrzej Adamski Conf CY (2001) Nat 14

459 Conference on cybercrime. Budapest 22. November 2001. National report Japan. Conf CY (2001) Nat.1

atzīta par noziedzīgu nodarījumu gan Latvijā, gan arī valstī, no kuras teritorijas uzbrukums veikts. Izstrādājot jauno Krimināllikuma 241. panta redakciju, bija svarīgi noteikt tās prioritātes, kas skaidri un nepārprotami tiesību akta piemērotājam noteiktu, kas ir uzskatāms par patvaļīgu piekļuvi.

Pantā nav iespējams iekļaut visus kritērijus, kas raksturotu šo darbību, tāpēc svarīgi bija izcelt un iekļaut tieši likuma tekstā divas pazīmes: 1) patvaļība ir cieši saistāma ar lietotājam piešķirto tiesību apjomu piekļūt ADAS resursiem; 2) patvaļība ir arī tad, ja persona izmanto citai personai piešķirtu tiesību piekļūt ADAS resursiem. Tādējādi ar šīm divām pazīmēm, nesaistot tās ar tehniskām metodēm, ko persona izmanto, īstenojot patvaļīgo piekļuvi, radīti priekšnoteikumi, lai likums aptvertu visu iespējamo lietotājam piešķirto piekļuves tiesību apjomu. Šis apjoms ietver sevī gan tiesības lietot pilnvarotas personas piešķirtus identifikatorus, gan arī pienākumu nelietot citai personai piešķirtus identifikatorus.

2004. gada februāra beigās Latvijas Tieslietu ministrijas darba grupa izstrādāja grozījumus Krimināllikumā ar mērķi saskaņot Krimināllikumā iekļauto noziedzīgo nodarījumu pret informācijas sistēmu drošību redakcijas ar EP Kibernoziegumu konvencijas prasībām. Šobrīd 241. panta „patvaļīga piekļuve automatizētai datu apstrādes sistēmai" redakcija jau ir stājusies likumīgā spēkā. Taču izstrādes procesā, darba grupa saņēma nevienu vien kritiku par izstrādāto projektu. Piemēram, Latvijas Republikas Iekšlietu ministrija ar 2004. gada 24. februāra vēstuli Nr. 1/31-494 „Par likumprojektu „Grozījumi Krimināllikumā" (VSS-208) 9. punktā ierosināja izslēgt no Krimināllikuma 241. panta 1.daļas redakcijas vārdus "bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības", motivējot ar to, ka jēdziens patvaļīgs jau izskaidro, ka darbība notiek bez atļaujas. Šāds viedoklis atbalstu neguva un tika pamatoti noraidīts. Latvijā nav neviena normatīvā akta, kur būtu definēts vispārobligātā veidā jēdziens „piekļūšana". Līdz ar to katrs sistēmas īpašnieks izstrādā savu sistēmas drošības kārtību un piešķir tiesības. Šis tiesību apjoms no sistēmas uz sistēmu var atšķirties, taču jebkurš piekļuves tiesību kopums bāzējas uz diviem galvenajiem kritērijiem, kas minēti 241. panta 1. daļā. Darba grupas uzdevums bija šos kritērijus materializēt, tādējādi dodot jēdzienam

„patvaļīga piekļuve" konkrētu saturu. Tāpēc to izslēgšana atkal radītu problēmas šī likuma piemērošanā.

Piemērs. 2004. gada 4. martā ASV Senāta Juridiskā komisija veica izmeklēšanu par ar gadījumu, kad 2003. gada 14. novembrī žurnālā "*Wall street journal*" publicēja 4 izvilkumus no pieciem dokumentiem, ko žurnāla redaktors apzīmēja ar demokrātu partijas darbinieku dienesta vēstulēm par partijas stratēģijas jautājumiem.
Nākamajā dienā *Washington times* paziņoja, ka viņu rīcībā ir 14 šādas demokrātu partijas darbinieku dienesta vēstules, kas bija paredzētas iekšējai lietošanai. Avīze īpaši norādīja, ka tās nav nākušās no Senāta darbiniekiem.
2003. gada 15. novembrī Senāta augstākā administratīvā amatpersona ziņoja, ka ir konstatēti robi Senāta juridiskās komisijas informācijas sistēmā, kā dēļ notikusi patvaļīga piekļuve nepubliskotiem demokrātiskās partijas dokumentiem un tie nodoti atklātībai.[460]
ASV Kibernoziegumu izmeklēšanas speciālisti, analizējot šo ziņojumu, bija pārsteigti par to, ka Senātā darbinieki bieži lietoja citu darbinieku paroles, ka paroles bija glabātas datoru failos, kur bija brīva pieeja, ka sistēmas, kas apstrādā konfidenciālu informāciju, arhitektūra bija veidota tā, ka tajā brīvi varēja ielādēt arī informāciju no citiem publiski pieejamiem informācijas resursiem un izdarīt citus pārkāpumus.
Taču lielākā daļa ekspertu atzīst, ka minētajā gadījumā **nav saskatāmas patvaļīgas piekļuves pazīmes**, jo kārtība nebija pašā sistēmā. Tomēr, analizējot šo pašu informāciju ir arī cits viedoklis, proti, ka šis incidents ir patvaļīga piekļuve datorsistēmai un par to ir jāierosina krimināllieta.

Šo piemēru izmantoju tāpēc, lai pierādītu, ka patvaļīga piekļuve vispirms ir vērtējama no sistēmas īpašnieka vai tā pilnvarotās personas piešķirto tiesību apjoma un lielā mērā juridiskais vērtējums ir atkarīgs no sistēmas īpašnieka subjektīvās attieksmes pret pārkāpumu. Ja šādas tiesības ir piešķirtas nekonkrētā formā, tās nav saistītas ar tiešu pienākumu un saistību izpildi, un tad arī nevar runāt par patvaļīgu piekļuvi Krimināllikuma 241. panta izpratnē.

Iekšlietu ministrijas speciālisti arī norādīja, ka citai personai piešķirto tiesību izmantošana pēc būtības ir datu apstrādes sistēmas līdzekļu pārvarēšana, jo lietotāju identifikācija datu apstrādes sistēmā un identifikācijas datu glabāšanas un neizpaušanas pienākums ir viens no datu apstrādes sistēmas aizsardzības pasākumiem. Šo argumentu autors pilnīgi noraida, jo citai personai piešķirto tiesību izmantošana nu nekādi nav saistāma ar sistēmas aizsardzības līdzekļu pārvarēšanu, jo no sistēmas resursu viedokļa piekļuve sistēmai tiek piešķirta likumīgi. Nelikumīga tā ir no sistēmas īpašnieka viedokļa. Tādi patiesībā ir visi gadījumi, kad personas izmanto citai personai esošu telekomunikāciju aprīkojumu un autorizējas

---

460 Testimony United States Senate Committee on the judiciary. Executive business meeting. Report on the investigation into
improper access to the Senate Judiciary Committee's computer system. March 4. 2004//
http://news.findlaw.com/hdocs/docs/senate/pickle30404rpt1.html (aplūkots 2004.gada 22. martā)

sistēmā kā attiecīgā telekomunikāciju aprīkojuma īpašnieks, kurš ir reģistrēts Lattelekom abonents.

Kā redzams no Krimināllikuma 241. panta, tad, panta redakcijā iestrādāti nosacījumi, kas paredz, ka krimināltbildība par patvaļīgu piekļuvi tiek saistīta ar konkrētām materiālām sekām, tas ir, krimināltbildība iestāsies tikai tad, ja tiks pārvarēti sistēmas aizsardzības līdzekļi un ja ar šīm darbībām sistēmas īpašniekam nodarīts būtisks kaitējums. Savukārt Krimināllikuma 241. panta 2. daļā atbildība par patvaļīgu piekļuvi iestājas tad, ja ar šādām darbībām nodarīti zaudējumi lielos apmēros vai nodarījums izdarīts mantkārīgā nolūkā.

Tas darīts divu iemeslu dēļ: 1) lai izslēgtu iespēju šo noziedzīgā nodarījuma sastāvu saukt par formālu un 2) lai krimināltbildību piemērotu tikai nopietniem nodarījumiem kā galējo valsts piespiedu ietekmes līdzekli. Paredzot šādu nodarījumu skaita pieaugumu, valstij jāparedz arī citi atbildības līdzekļi par analogām darbībām, kad nav iestājušās Krimināllikumā paredzētās sekas.

*Patvaļīgas piekļuves automatizētām datu apstrādes sistēmām, atbildības nosacījumu analīze*

1. Sistēmas aizsardzības līdzekļu pārvarēšana.

Kā redzams no šīs pazīmes, tad netiek atzīts par noziedzīgu nodarījumu patvaļīgas piekļuves fakts sistēmai, kurai nebūs attiecīgu aizsardzības līdzekļu. Ar šiem aizsardzības līdzekļiem saprot, speciālos ADAS loģiskās aizsardzības līdzekļus. Tāpēc ADAS drošības parametriem ir jābūt ieprogrammētiem tā, lai šai personai būtu pilnīgi un nepārprotami skaidrs, ka viņas pieslēgšanās ADAS vai tās daļai ir patvaļīga un neatļauta. Ja persona, zinot to, ka viņam nav tiesību piekļūt ADAS resursiem, izmanto speciālās metodes un salauž vai apiet loģiskās aizsardzības līdzekļus, tad tā ir saucama pie krimināltbildības pēc Krimināllikuma 241. panta, ja ir iestājušās attiecīgās sekas.

*Sekas*

1. Būtisks kaitējums. Disertācijā jau ir iepriekš analizēts jēdziena „būtisks kaitējums" mantiskais saturs, tādēļ neatkārtošos. Personai veicot patvaļīgo piekļuvi datorsistēmai un sabojājot vai apejot sistēmas aizsardzības līdzekļus, zaudējumi sistēmas īpašniekam rodas ne tikai tiešā materiālā izteiksmē, bet galvenokārt

zaudējums rodas tāpēc, ka apdraudētas ir pārējo sistēmas lietotāju piekļūšanas tiesības. Tieši šis faktors nereti ir daudz kaitīgāks nekā tieši nodarītais zaudējums. Piemēram, kad V. Levins iekļuva *Citibank* un nolaupīja lielu naudas summu, tad banka pēc šī notikuma publiskošanas katru dienu zaudēja apmēram 5% iepriekšējo ienākumu.[461] Tas arī izskaidro, kāpēc patvaļīgas piekļuves gadījumā tik ļoti maz cilvēku vēršas pēc palīdzības policijā, jo pazaudēto biznesa reputāciju ne vienmēr var izmērīt naudas izteiksmē. Tāpēc kriminalizācijas nosacījumiem ir jābūt pietiekami stingriem un sodiem pietiekami bargiem.

2. ES ietvarlēmums par uzbrukumiem datorsistēmām izvirza ES dalībvalstīm prasību paredzēt kā atbildību pastiprinošus apstākli patvaļīgas piekļuves gadījumā ja darbības izraisījušas smagas sekas. Smagu seku jēdziens definēts Likuma „Par Krimināllikuma spēkā stāšanās laiku un kārtību" 24. pantā.

3. Darbības izdarītas mantkārīgā nolūkā. Iepriekš aprakstītajā Vidzemes apgabaltiesas prokuratūras lēmumā par S. C. saukšanu pie kriminālatbildības ir redzams, ka apsūdzētais savas darbības, kas saistītas ar patvaļīgu piekļuvi datorsistēmai, izdarīja mantkārīgu tieksmju dēļ. Praksē patvaļīga piekļuve ADAS resursiem ir cieši saistīta ar šo resursu izlaupīšanu vai citādu izmantošanu mantkārīgu tieksmju dēļ, jo darbības nereti saista vēlēšanās gūt sev vai citai personai ekonomisku labumu. Tāpēc svarīgi bija pastiprināt atbildību par patvaļīgu piekļuvi gadījumos, ja persona izmanto patvaļīgo piekļuvi mantkārīgos nolūkos.

*Papildus kriminalizācijas nosacījumi*

Kā jau minēts, tad Latvijā ir pieņemts Valsts informācijas sistēmu likums. Likuma 3. pants:

*(1) Likums attiecas uz valsts informācijas sistēmām, kuras lietojot tiek nodrošināta informācijas aprite normatīvajos aktos un Latvijai saistošos starptautiskajos līgumos noteikto funkciju izpildei.*
*(2) Likums attiecas arī uz informācijas sistēmām, ko pašvaldību institūcijas veido un uztur kā valsts informācijas sistēmas sastāvdaļu.*

Kā redzams no likuma mērķa un tajā paredzēto subjektu loka, tad par valsts informācijas sistēmu nākotnē tiks atzīta jebkura valsts vai pašvaldību iestādes

---

461 The US response to criminal exploitations of the Internet and other new technologies presentation by Michael A. Sussman. Money Laundering and Cybercrime: The EU Response to Criminal exploitation of new technologies. Academy of European law. Trier, Germany 20-22. february 2003.

informācijas sistēma, kas apstrādās informāciju, kuras apriti noteic gan Latvijas Republikas likumi, gan arī Latvijai saistošie starptautiskie līgumi. Tādējādi minētais likums reglamentē visu to informācijas sistēmu darbību, kas nepieciešama valstij svarīgu funkciju realizācijā.

Šim likumam ir specifiski objekti, respektīvi, šī likuma regulējuma priekšmets ir tās informācijas sistēmas, kas apkalpo valsts attīstībai īpaši svarīgas informācijas sfēras un kuras tiks iekļautas valsts informācijas sistēmu reģistrā. Minētā likuma pieņemšana saskaņota ar Latvijas Republikas nacionālās drošības koncepciju[462], tādējādi veidojot vienotu normatīvo aktu bloku, kura uzdevums ir izstrādāt pasākumus, lai novērstu valstij kritiskus informācijas sistēmu apdraudējumus. Personām, kuras profesionāli vai amatieru līmenī nodarbojas ar patvaļīgu piekļūšanu datorsistēmām, viens no uzbrukuma mērķiem ir informācijas sistēmas, kas nodrošina valstij svarīgu funkciju izpildi. Tā pasaulē ir ļoti izplatīta parādība.

Piemērs. 1995. gadā ASV Aizsardzības ministrija[463] paziņoja, ka ASV Pentagona datorsistēmām, pēc Aizsardzības Informācijas drošības aģentūras (DISA) ziņām, 1995. gada laikā notikuši līdz 250 000 uzbrukumu, no kuriem 65% bijuši veiksmīgi. Aģentūras ziņojumā norādīts, ka šādu iebrukumu skaits ar katru nākamo gadu dubultojas.

Valstīs, kur visa ekonomika, politika un sadzīve ir atkarīga no informācijas un komunikācijas tehnoloģiju darbības, noziedznieks ar tastatūras palīdzību 5 minūšu laikā var iznīcināt valsts ekonomiku un radīt īstu paniku valsts iedzīvotājos. Tāpēc pastāv reāla iespēja, ka teroristi savu uzbrukumu var veikt ar datorsistēmu palīdzību. Iepriekšminētais, manuprāt, rada pamatu, lai Krimināllikuma 241. panta sastāvā iekļautu trešo daļu, kurā paredzētu atbildību par šādām darbībām, ja tās vēstas pret valsts informācijas sistēmu.

Par noziedzīgā nodarījuma objektīvo pusi noteikt 1. daļā paredzētos nosacījumus, tas ir, ja patvaļīgās piekļuves rezultātā ir pārvarēta ADAS drošības sistēma un ar šīm darbībām nodarīts būtisks kaitējums. Uzskatu, ka pati par sevi piekļūšana valsts informācijas sistēmām pārvarot sistēmu aizsardzību, jau automātiski būtu atzīstama par būtisku kaitējumu.

---

462 Latvijas Republikas nacionālā drošības koncepcija// http://www.lato.lv/html/nato/dokumenti/26000.html (aplūkots 2004.gada 22. martā)

463 Information Security: Computer Attacks at Department of Defence Pose Increasing Risks (Chapter Report, 05/22/96, GAO/AIMD–96–84), sk. http://www.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=wais.access.gpo.gov&filename=ai96084.txt&directory=/diskb/wais/data/gao (aplūkots 2002.gada 20. februārī).

**Subjekts.** Likumdevējs nav paredzējis krimināllikumā īpašus nosacījumus vainojamai personai. Tāpēc visiem noziedzīgiem nodarījumiem pret informācijas sistēmu drošību (Krimināllikuma 241- 244. pants) par subjektu var būt jebkura 16 gadu vecumu sasniegusi, pieskaitāma fiziska persona. Taču tas neizslēdz gadījumus, ka pie atbildības par šī veida nodarījumiem var saukt arī amatpersonas.

**Subjektīvā puse**. Kā jau minēju iepriekš, tad kibernoziegumu var izdarīt tikai tīši ar tiešu vai netiešu nodomu, tādējādi krimināllikuma 241- 244. panta ietverto noziedzīgo nodarījumu subjektīvā puse vienmēr izpaudīsies tīšas darbības veidā.

6.2. Datortehnikas programmatūras neatļauta iegūšana. KL 242. pants (līdz 01.06. 2005.)

*(1)Par datortehnikas programmatūras, faila vai datortehnikas atmiņā esošās datu bāzes neatļautu kopēšanu, ja ar to radīts būtisks kaitējums,-*

*soda ar arestu vai naudas sodu līdz astoņdesmit minimālajām mēnešalgām.*

*(2) Par tādām pašām darbībām, ja tās izdarītas atkārtoti vai ja tās saistītas ar datortehnikas programmatūras aizsardzības līdzekļu pārvarēšanu vai ar pieslēgšanos sakaru līnijām,-*

*soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar naudas sodu līdz 150 minimālajām mēneša algām.*

Šim nodarījumam bija divi objekti:

1. Nodarījums bija vērsts pret informācijas sistēmu drošības pazīmi – konfidencialitāti, jo neatļauti kopējot informācijas resursus, tiek aizskarta personas interese dot iespēju iepazīties ar informāciju tikai tām personām, kam uz to nav tiesības.

2. Nodarījums vērsts pret personas intelektuālajām tiesībām, jo programmatūru, datu bāzu izmantošanu aizsargā Autortiesību likums.

Noziedzīgā nodarījuma priekšmets ir sistēmas informācijas resursi, kuri satur, tādus elementus kā programmatūras, atsevišķas programmu daļas, failus un sistēmas atmiņā esošās datu bāzes.

*Fails* ir datu kopa, tekstuāls vai grafisks dokuments, ko glabāšanas, pārsūtīšanas vai apstrādes procesā uzskata un identificē kā vienotu veselumu un kas parasti sastāv no vienādas struktūras ierakstiem.

*Datu bāze-* neatkarīgu darbu, datu vai citu materiālu krājums, kas sakārtots sistemātiski vai metodiski un individuāli pieejams elektroniskā vai citā veidā[464]. Pēc būtības visi šie komentējamā panta speciālie priekšmeti ir saistīti ar intelektuālā īpašuma aizsardzību.

*Datorprogramma* ir vārdos, kodos, shēmās vai citā formā izteikts informācijas nesējā ierakstīts instrukciju kopums, ko dators spēj nolasīt un kas datoru aktivizē kādai noteiktai darbībai vai kāda noteikta uzdevuma veikšanai, vai rezultāta sasniegšanai.[465] Patiesībā šī definīcija nav zaudējusi savu aktualitāti, jo vairākas vārdnīcas, piem., Foldoc, Hačkinsona[466] enciklopēdija u.c., datorprogrammu definē kā ierakstītu instrukciju un kodu sistēmu, kas aktivizē datoru kāda konkrēta uzdevuma izpildei.

Lai atzītu nodarījuma priekšmetu par *datu bāzi* vai *datorprogrammu*, praksē būs jāpiemēro divu kritēriju kopsumma, un tas ir:

1) objektīvie kritēriji, ka tiesību aktu piemērošanas speciālisti, izmantojot tiesu ekspertīžu metodes, kas būs balstītas uz starptautiskiem standartiem atbilstošu izpētes metodiku, atzīs, vai konkrētais krimināpārkāpuma priekšmets ir datorprogramma vai datu bāze;

2) subjektīvie kritēriji, kur cietušais uzskata, ka nelikumīgās darbības mērķis ir datu bāze vai datorprogramma. Ievērojot to, ka tiesas procesā ekspertīze ir tikai viens no pierādījumiem, tad cietušā viedoklis par sava darba vērtējumu var būt ļoti nozīmīgs.

Autors uzskata, ka nevar izslēgt nevienu no šiem kritērijiem, tikai mums vispirms ir jārada tāda neatkarīga institūcija, kas atbilstoši starptautiski atzītiem standartiem un metodikai, spēj šādus slēdzienus dot.

Minētajā pantā inkriminētās darbības varēja izdarīt tikai ar tīši. Tātad tā ir aktīva darbība, kas sastāvēja no tā, ka persona, kurai bija likumīgas tiesības lietot datorsistēmas informācijas resursus, pārkāpa sava pilnvarojuma robežas un neatļauti kopēja pantā minētos priekšmetus. Analizējot KL 242. panta

---

464 Autortiesību likuma 1.p. 3.p., pieņemts 2000.gada 6. aprīlī. Latvijas Vēstnesis 2000.gada 24. aprīlis

465 "Likums par autortiesībām un blakus tiesībām" pieņemts. 1993.gada 11.maijā. 1.pants. NAIS (spēkā no 1993.gada līdz 2000.gada 11. maijam)

466 One look dictionary search// www.onelook.com (aplūkots 2004.gada 20. martā).

„Datortehnikas programmatūras neatļauta iegūšana" jēgu, ir skaidrs, ka nodarījums neparedzēja atbildību par failu tehnisku kopēšanu sistēmas resursu ietvaros. Šeit patiesībā rodas nesamierināma problēma starp darbības tehnisko un juridisko saturu. Ja tehniski kopēšanu izdara ar to brīdi, kad ieslēdz datoru, tad juridiski kopēšana ir darbība, kuras rezultātā informācija tiek pārnesta uz citu datu nesēju un tiek izveidota kopija, kura vairs neatrodas sistēmas īpašnieka tiesiskā valdījumā vai īpašumā.

Piemērs. Kā redzams no Vidzemes tiesu apgabala prokuratūras apsūdzības raksta S.C. lietā, tad S.C. nolūkā veikt krāpšanu, nokopēja a/s "Unibanka" speciāli veidoto datorprogrammu"A", izveidojot tās kopiju citā datu nesējā, proti, savā portatīvajā datorā, un papildus izveidoja programmu "A1", un veica ar to attiecīgas manipulācijas un rezultātā izkrāpa cietušai naudu vairāk kā 35 000 latu.
Dotajā piemērā, darbības nav kvalificētas pēc KL 242. panta 2. daļas, tomēr spriežot pēc celtās apsūdzības, tās pilnīgi satur visas KL 242. panta 2. daļā paredzētās noziedzīgā nodarījuma pazīmes, proti, neatļautu datorprogrammas "A" kopēšanu uz cita nošķirta datu nesēja. Šī darbība izdarīta, pieslēdzoties cietušā datortīklam, respektīvi, izmantojot sakaru līnijas un veikta apejot sistēmas aizsardzības līdzekļus, jo ar speciāli izveidotu programmu S.C. ieguva informāciju un nokopēja citā datu nesējā cietušai personai piešķirto digitālo parakstu. Darbību rezultātā cietušai tikai nodarīts būtisks kaitējums, jo iegūtā programma tika izmantota krāpšanā, kuras rezultātā tika nodarīti zaudējumi vairāk kā 35 000 latu apmērā.

No minētā piemēra skaidri redzams, kādas sekas šeit paredz likumdevējs. Tās iestājas pie nosacījuma, ja pantā norādīto informāciju ir ieguvusi savā valdījumā cita persona, tādā veidā gūstot iespēju iepazīties ar cietušajam piederošo vai valdījumā, glabāšanā nodoto informāciju.

Tāpēc autors nepiekrīt V. Liholajas viedoklim, aprakstot kopēšanu, jo šī panta izpratnē darbība par kopēšanu var tikt atzīta tikai tad, ja tā ir radījusi noteiktas tiesiskās sekas- kaitējumu cietušajam, respektīvi, kopiju savā valdījumā nelikumīgi ir ieguvusi trešā persona. Līdzīgu viedokli atbalsta arī A. Voļevods[467], norādot, ka personu nevar sodīt par to, ka tā tikai iepazinies ar informāciju, jo kopēšana ir informācijas pārnešana no ADAS citā datu nesējā, saglabājot nemainīgu pirmatnējo informāciju. Tāpat viņš norāda, ka no kopēšanas jānošķir informācijas pavairošana, jo, pēc viņa domām, pavairojot informāciju tā tiek saglabāta tajā pat datu nesējā, piem., diska cietajā atmiņā, un paliek sistēmas īpašnieka rīcībā un neatstāj sistēmas resursus.

---

[467] Волеводз А.Г. Противодействие компютерным преступлениям. Правовые основы международного сотрудничества. Москва-Юрлитинформ, 2002.,с.70

KL. 242. panta 2. d. objektīvo pusi veidoja aktīva darbība, kurai jāsastāv no divām atsevišķām darbībām: 1) personai, izmantojot sakaru līdzekļus, bija patvaļīgi jāpieslēdzas datorsistēmām pārvarot sistēmas programmatūras aizsardzības līdzekļus. Šajā gadījumā paši informācijas resursi, un ne tikai sistēma kopumā, varēja tikt nodrošināta ar speciālām aizsardzības metodēm, piemēram, kriptogrāfiju, šifriem, piekļūšanas kodiem, identifikatoriem u. c. Ja lietotājs, zinot to, ka viņam nav tiesības uz šiem informācijas resursiem, pārvarēja loģiskās aizsardzības metodes un piekļuva informācijai, tad viņa darbība uzskatāma par patvaļīgu pieslēgšanos datorsistēmai; 2) personai ir jāizdara neatļautā kopēšana, tas ir, jāiegūst savā valdījumā informācijas priekšmets, kas minēts iepriekš. Tikai abu šo darbību rezultātā iestājās kaitīgās sekas. Kā jau minēts iepriekš, tad informācijas īpašniekam vai valdītājam ir tiesības noteikt sistēmā pieejamās informācijas lietošanas statusu.

Sistēmas resursu īpašniekam ir tiesības prasīt pantā minēto seku aizskāruma novēršanu tikai tad, ja lietotājam nepārprotami ir pateikts, ka piekļūšana šiem informācijas resursiem nav atļauta. Ja persona to ignorē un nelikumīgi kopē informāciju, tās darbībās bija saskatāmas KL 242. pantā paredzētā nodarījuma pazīmes. Otra pazīme ir, ja šīs darbības tiek izdarītas atkārtoti. KL 25. pantā ir teikts:

*„Noziedzīgu nodarījumu atkārtotība ir tad, kad viena persona izdara divus vai vairākus nodarījumus, kas paredzēti vienā un tai pašā likuma pantā, vai arī divus vai vairākus noziedzīgus nodarījumus, kas paredzēti dažādos šā likuma pantos, ja atbildība par atkārtotību paredzēta šajā likumā."*[468]

Praksē krimināllietas par šādu nodarījumu nav. Kad tika veikta Krimināllikuma saskaņošana ar Kibernoziegumu konvencijā un ES ietvarlēmumā par uzbrukumiem informācijas sistēmām prasībām, autors ierosināja, šo noziedzīgā nodarījuma sastāvu izslēgt no Krimināllikuma. Pasaulē krimināltiesību teorijā ir vērojama tendence dekriminalizēt tos noziedzīgo nodarījumu sastāvus, kas pēc būtības dublē citus noziedzīgu nodarījumu sastāvus. Līdzīgi tas ir, analizējot KL 242. panta lietderību. Nenoliedzami, ka panta 1. daļā paredzēto informācijas resursu neatļauta kopēšana ir nodarījums, par kuru jāparedz krimināalatbildība, taču, kā jau minēju,

---

[468] Krimināllikums Prof Dr. hab.jur. U.Krastiņa un Dr.iur..A. Niedres komentāri. Rīga- TNA, 1998., 13.lpp.

tad šī panta izpratnē noziegums ir pabeigts ar to brīdi, kad persona neatļauti ir izgatavojusi attiecīgās informācijas fizisku kopiju un šo kopiju izņēmusi no sistēmas īpašnieka valdījuma. Tādējādi šī kopija ir atstājusi sistēmas īpašnieka datorsistēmas resursus un līdz ar to nepakļaujas tā kontrolei. Tā kā minētais nodarījums ir krimināIpārkāpums, tad saskaņā ar KL 15.p. 6. punktu par mēģinājumu izdarīt krimināIpārkāpumu persona nav sodāma. Tādēļ atbildība var iestāties tikai par pantā minētās informācijas kopēšanu uz cita, tehniski no sistēmas resursiem nošķirta datu nesēja.

Krimināllikuma 148. pants paredz krimināIatbildību par autortiesību un blakustiesību pārkāpšanu, bet 149. pants -nelikumīgas darbības ar autortiesību un blakustiesību objektiem.

Krimināllikuma 148. pants "Autortiesību un blakustiesību pārkāpšana"

*(1) Par autortiesību tīšu pārkāpšanu, ja tā izdarīta, pārkāpjot autoru tiesības uz darba izmantošanu vai blakustiesību tīšu pārkāpšanu,-*
*(2) Par tām pašām darbībām, ja tās izdarītas atkārtoti vai ja tās izdarījusi personu grupa pēc iepriekšējas vienošanās - soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar arestu vai ar naudas sodu līdz simt piecdesmit minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas.*
*(3) Par autorības vai autortiesību piesavināšanos vai līdzautorības uzspiešanu- soda ar brīvības atņemšanu uz laiku līdz trīs gadiem vai ar arestu vai ar naudas sodu līdz divsimt minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas.*
*(4) Par piespiešanu ar vardarbību vai ar tās draudiem, vai ar šantāžu atteikties no autorības vai par līdzautorības uzspiešanu- soda ar brīvības atņemšanu līdz pieciem gadiem vai ar naudas sodu līdz divsimt minimālajām mēnešalgām, konfiscējot mantu vai bez mantas konfiskācijas.*

Intelektuālā īpašuma aizsardzības un autortiesību aizsardzības tiesiskā bāze ir Bernes Konvencijas, ES un Eiropas Padomes pieņemtie starptautiskie normatīvie akti intelektuālā īpašuma aizsardzības jomā un 2000. gada 6. aprīlī pieņemtais Autortiesību likums[469]. Minētā nodarījuma objekts ir Latvijas Republikas Satversmes 113. pantā garantētās autora personiskās tiesības un intereses, kā arī to personu tiesības un intereses, kuras uz likumīga pamata izmanto zinātniskos,

---

469 http://www.autornet.lv/tiesibas/likumi/autort.dr.php (aplūkots 2004.gada 23. martā).

literatūras, mākslas darbus, muzikālos sacerējumus, uzstājoties jebkādā veidā plašas auditorijas priekšā[470].

Autortiesību likuma IV nodaļa reglamentē autortiesību aizsardzības apjomu:

1. Autora personiskās tiesības, kas satur tiesības uz autorību, izlemšanu, vai darbs tiks izziņots un kad tas tiks izziņots, darba atsaukšanu, tiesības pieprasīt, lai vārds būtu norādīts visās kopijās, darba neaizskaramību- tiesības atļaut vai aizliegt izdarīt jebkādus pārveidojumus, grozījumus un papildinājumus gan pašā darbā, gan nosaukumā, un mantiskās tiesības, tas ir tiesības uz darba publicēšanu, reproducēšanu, izplatīšanu utt.

2. Saskaņā ar Autortiesību likumu šī nodarījuma iekļautie priekšmeti ir arī – datorprogrammas, datu bāzes, pusvadītāju integrālās shēmas, mikroshēmas. Tādējādi minēto priekšmetu izmantošanas, lietošanas un pavairošanas kārtību noteic autortiesību likums, un jebkura darbība, kas saistīta ar šo priekšmetu nelikumīgu kopēšanu, ir tīšs autortiesību pārkāpums. Autors uzskata, ka pati jautājuma nostādne, ka datorprogrammu kopēšana KL 242. panta izpratnē ir noziedzīgs nodarījums, ja tas veikts bez sistēmas īpašnieka vai pilnvarotās personas piekrišanas, ir kļūdaina. Jo nereti sistēmas īpašnieks arī būs tikai šādas programmas licences turētājs.

*Autortiesību likuma 29. pants. „Ierobežojumi attiecībā uz datorprogrammu reproducēšanas, translēšanas, adaptēšanas un jebkādas citādas pārveidošanas tiesībām" noteic:*
*(1) Ja līgumā nav paredzēts citādi un datorprogrammas izmantošanas tiesības iegūtas likumīgi, tās reproducēšanai, translēšanai, adaptēšanai vai jebkādai citādai pārveidošanai un šo darbību rezultātu reproducēšanai nav nepieciešama īpaša autortiesību subjekta atļauja, ja vien šīs darbības (arī kļūdu labošana) ir nepieciešamas datorprogrammas lietošanai paredzētajam mērķim.*
*(2) Datorprogrammas izmantošanas tiesību likumīgajam ieguvējam, slēdzot līgumu, nedrīkst aizliegt izgatavot rezerves kopiju, ja šī kopija nepieciešama datorprogrammas lietošanai.*
*(3) Persona, kurai ir tiesības lietot datorprogrammu, bez autortiesību subjekta atļaujas drīkst novērot, pētīt vai pārbaudīt, kā programma funkcionē, lai atklātu idejas un principus, uz kuriem balstīti jebkādi datorprogrammas elementi, ja šī persona attiecīgās darbības veic, datorprogrammu ielādējot, izvadot uz displeja, izpildot, pārraidot vai noglabājot datora atmiņā.*

---

[470] Krastiņš U., Liholaja V., Niedre A. Krimināllikuma zinātniski- praktiskais komentārs (2) Sevišķā daļa. Profesora U. Krastiņa redakcijā. Rīga- "AFS", 2003, 278-279 lpp.

*31. pants. Ierobežojumi attiecībā uz datu bāzēm*
*(1) Likumīgs datu bāzes vai tās eksemplāra lietotājs bez datu bāzes autora atļaujas var veikt darbības, kas vajadzīgas, lai piekļūtu datu bāzes saturam un to izmantotu. Ja datu bāzes likumīgajam lietotājam ir atļauts izmantot tikai daļu no datu bāzes, iepriekšminētais noteikums attiecas tikai uz šo daļu.*
*(2) Vienošanās, kas ir pretēja šā panta noteikumiem, nav spēkā.*

Līdz ar to šāda atļauja kopēt datorprogrammu vai citai personai piederošu, bet sistēmā glabātu datu bāzi, lai to nodotu citām personām ir nelikumīga un nevar būt informācijas sistēmas drošības apdraudējuma pamats, bet ir Autortiesību un blakustiesību pārkāpšana. Tāpēc šādas darbības ir kvalificējamas pēc KL 148. panta.

KL 242. panta 2.d. paredzēja atbildību par tām pašām darbībām, ja tās izdarītas atkārtoti vai ja tās saistītas ar datortehnikas programmatūras aizsardzības līdzekļu pārvarēšanu vai ar pieslēgšanos sakaru līnijām. Līdzīgs atbildības nosacījums bija paredzēts KL 241. panta 2.d. redakcijā (līdz 01.06.2005.), tādējādi likumdevējs vienus un tos pašus nosacījumus atzinis gan par patvaļīgas piekļūšanas nosacījumu, gan arī par patvaļīgas datortehnikas programmatūras iegūšanas nosacījumu. Ar 2005.gada 28. aprīļa likumu, šo nodarījumu no Krimināllikuma izslēdza.

6.3. Datortehnikas programmatūras bojāšana (līdz 01. 06. 2005.) un "Automatizētās datu apstrādes sistēmas darbības traucēšana un nelikumīgā rīcība ar šajā sistēmā iekļauto informāciju"(28.04.2005.) KL 243. pants

| **Pants 243.** | Redakcijā līdz 1.06. 2005.<br><br>**Datortehnikas programmatūras bojāšana** | 28. 04. 2005. redakcijā<br><br>**Automatizētās datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju** |
|---|---|---|
| 1. daļa | Par automatizētā datorsistēmā ievietotās informācijas neatļautu modifikāciju, grozīšanu, bojāšanu vai iznīcināšanu vai apzināti nepatiesas informācijas ievadīšanu automatizētā sistēmā, vai informācijas nesēju, datortehnikas programmatūras vai aizsardzības sistēmu apzinātu bojāšanu vai iznīcināšanu, ja ar | Par automatizētā datu apstrādes sistēmā esošās informācijas neatļautu grozīšanu, bojāšanu, iznīcināšanu vai aizklāšanu vai apzināti nepatiesas informācijas ievadīšanu automatizētā datu apstrādes sistēmā, ja ar to tiek bojāta vai iznīcināta aizsardzības sistēma vai radīts būtisks kaitējums,-<br>soda ar brīvības atņemšanu līdz pieciem gadiem vai ar |

| | | |
|---|---|---|
| | to radīts būtisks kaitējums,-<br>soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar naudas sodu līdz piecdesmit minimālajām mēnešalgām. | piespiedu darbu, vai ar naudas sodu līdz simt piecdesmit minimālajām mēnešalgām. |
| **2. daļa** | X | Par automatizētās datu apstrādes sistēmas darbības apzinātu traucēšanu, ievadot, pārnesot, bojājot, izdzēšot, pasliktinot,, izmainot vai aizklājot informāciju, ja ar to tiek bojāta vai iznīcināta aizsardzības sistēma vai nodarīti zaudējumi lielos apmēros,-<br>soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar piespiedu darbu, vai ar naudas sodu līdz simt piecdesmit minimālajām mēnešalgām. |
| 3. daļa | X | Par pirmajā un otrajā daļā paredzētajām darbībām, ja tās izdarījusi organizēta grupa vai tās izdarītas mantkārīgos nolūkos, vai tās izraisījušas smagas sekas,-<br>soda ar brīvības atņemšanu uz laiku līdz astoņiem gadiem vai ar naudas sodu līdz simt astoņdesmit minimālajām mēnešalgām. |
| 4. daļa | X | Par šā panta pirmā un otrā daļā paredzētajām darbībām, ja tās vērstas pret valsts informācijas sistēmām,-<br>soda ar brīvības atņemšanu uz laiku līdz astoņiem gadiem vai ar naudas sodu līdz divi simti minimālajām mēnešalgām. |

*Noziedzīgā nodarījuma objekts un priekšmets*

Noziedzīgā nodarījuma objekts ir informācijas sistēmu drošība, bet speciālais objekts interese - nodrošināt sistēmā esošo informācijas resursu integritāti jeb veselumu. Tas nozīmē, ka informācijas īpašnieks ir ieinteresēts, lai viņam piederošā

vai valdījumā nodotā informācija netiktu ietekmēta bez viņa atļaujas. Kā pareizi norāda V. Liholaja, tās var tikt apdraudētas ar vairākām alternatīvām darbībām.[471]

Analizējot KL 243. panta (līdz 01.06. 2005.) nosaukumu un panta saturu, rodas zināma neskaidrība par mērķi, ko likumdevējs vēlējies sasniegt, ietverot krimināllikumā šo noziedzīgā nodarījuma sastāvu. Panta nosaukumā bija ietverti vārdi „datortehnikas programmatūras bojāšana". Kā iepriekš minēts, tad datorprogrammatūra ir autortiesību likuma aizsardzības objekts, un ne katra sistēmā glabāta vai apritē esoša informācija var tikt atzīta par datorprogrammu. Līdz ar to šeit bija vērojama zināma nekonsekvence ar pašu panta saturu, jo pantā minēti kā apdraudējuma priekšmeti minēti faktiski visi sistēmas informācijas resursi, to skaitā datorprogrammas. Valsts informācijas sistēmu drošības noteikumu projektā[472] informācijas resursi definēti kā valsts informācijas sistēmas sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, sistēmdatne un datu datne (arī tās, kas satur valsts informācijas sistēmā glabājamo, apstrādājamo un valsts informācijas sistēmas lietotājiem pieejamo informāciju).

Likumdevējs nezin kādu iemeslu dēļ bija izdalījis kā atsevišķu priekšmetu datortehnikas aizsardzības sistēmu, jo kibernoziegumu kontekstā to saprot, kā datorprogrammatūras kompleksu. Līdz ar to ir absolūti neloģiski bija vienus programmatiskos resursus izcelt starp citiem. Vēl lielāka neskaidrība bija par priekšmeta „informācijas nesēji" saturu. Ar terminu „informācijas nesējs" tradicionāli saprot vidi, mediju, kur tiek ierakstīta informācija.[473] Savukārt datorvārdnīcā šis termins izskaidrots „vide", „medijs", kas uztur mašīnlasāmus datus, piemēram, magnētiskā lente, kompaktdisks (CD), cietais disks un disketes u. c.[474] Izņemot cieto disku, kas ir jebkuras datorsistēmas neatņemama sastāvdaļa, pārējie datu nesēji ir absolūti autonomas vienības, ko var pievienot jebkurai datorsistēmai. Līdz ar to nav skaidrs, ko likumdevējs ir domājis ar terminu

---

[471] Krastiņš U., Liholaja V., Niedre A. Krimināllikuma zinātniski- praktiskais komentārs (3) Sevišķā daļa. Profesora U. Krastiņa redakcijā. Rīga- "AFS", 2003, 229..lpp.

[472] MK Noteikumu Valsts informācijas sistēmas drošības noteikumi, projekts.

[473] American heritage. Dictionary of English language: Forth edition 2000// http://www.bartleby.com/61/54/D0035400.html; (aplūkots 2005.gada 10. janvārī)

[474] High tech disctionary// http://www.computeruser.com/resources/dictionary/definition.html?lookup=8250 (aplūkots 2004.gada 28. decembrī).

informācijas nesējs. Nekādu skaidrību šajā jomā praktiķiem nesniedz arī šī panta komentāru autori, jo komentāra tekstā ir vienkārši pārrakstīti pantā uzskaitītie noziedzīgā nodarījuma priekšmeti.[475]

*Noziedzīga nodarījuma- informācijas sistēmu un datu traucēšana kaitīguma raksturojums*

Kaitīgums ir ikviena noziedzīga nodarījuma pamatpazīme. Tā nozīmē, ka delikts nodara vai var radīt kaitējumu sabiedrības interesēm.[476] A. Judins uzskata, ka mūsdienu prasībām neatbilst nostādne, ka viss, kas aizliegts ar krimināllikumu, ir noziedzīgs nodarījums, bet pārējais nav krimināls un tādēļ nav jēgas runāt par nodarījuma bīstamību. Viņš uzskata, ka šāda pozīcija nav mūsdienīga, jo tā ir pārāk formāla un neatklāj konkrēto cēloni, kāpēc tā vai cita norma tiek kriminalizēta.[477] Šim viedoklim var piekrist tikai daļēji. Nav šaubu, ka jebkurš delikts, jebkura atkāpšanās no morāles normām rada kaut kādu kaitējumu. Taču tas nenozīmē, ka šāda rakstura darbībai jākļūst par krimināli sodāmu tikai tāpēc, ka kāds to vērtē kā sliktu. Gluži otrādi, modernā krimināltiesību teorija izvirza prasību, ka krimināatbildība ir jāpiemēro pēc subsidiaritātes principa kā galējais ietekmēšanas līdzeklis, ja citi ietekmēšanas līdzekļi nav bijuši efektīgi.[478] Tas nozīmē, ka krimināltiesību teorētiķiem laiku pa laikam jāierosina likumdevējam izslēgt no krimināllikuma tos pantus, kuros apdraudēto interesi var aizsargāt ar citām metodēm.

Par raksturīgu piemēru autora paustā viedokļa aizstāvībai var kalpot tieši noziedzīgu nodarījumu pret informācijas sistēmu drošību izvērtējums. Šādi nodarījumi jau bija pazīstami kopš 1960. gada, taču līdz pat 1985. gadam neviena valsts nebija paredzējusi par šādām darbībām krimināatbildību. Nav šaubu, ka katra no šādām darbībām radīja kaitējumu, taču tas nebija globāli visaptverošs un tāpēc netika uzskatīts par tik sabiedriski bīstamu, ka atbildība par šādu nodarījumu

---

475 Krastiņš U., Liholaja V., Niedre A. Krimināllikuma Zinātniski- praktiskais komentārs. (3) Sevišķā daļa. U. Krastiņa redakcijā. Rīga: AFS", 2003, 229-230.lpp.

476 Judins A. Krimināatbildības izslēdzamības apstākļi. Rīga: TNA, 2000., 18.lpp.

477 Turpat, Judins A., 19.lpp.

478 Council of Europe Legal affairs Computer related crime prefased bt August Bequai. European Committee on Crime problems, Strasbour. 1900. Recommendation No (89)9 on computer related crime and final report of the European Committee on Crime Problems, p. 24

jāparedz krimināllikumā. Datorspeciālisti nereti izsaka viedokli[479], ka pašreizējā krimināltiesību doktrīna ir novecojusi un nav piemērojama jaunā tipa noziedzīgo nodarījumu tiesiskam regulējumam. Šī viedokļa piekritēji to pamato šādi:

1) kibernoziegumi ir jauna tipa noziedzīgi nodarījumi, kuri tiek veikti jauna tipa vidē- kibertelpā. Šo noziedzīgo nodarījumu priekšmets ir informācija, kas sagatavota elektroniskā veidā. Šādi sagatavotai informācijai nav materiālas substances, līdz ar to tā nevar būt par konvencionālo krimināltiesību regulējuma priekšmetu;

2) kibernoziegumi nereti tiek izdarīti vienā valstī, bet sekas iestājas citā;

3) kibertelpai nav vienota noteikta regulējuma, tāpēc arī grūti saskaņā ar konvencionālo krimināltiesību doktrīnu noteikt, kas ir un kas nav atzīstams par noziedzīgu nodarījumu.

Nenoliedzami, ka tradicionālās krimināltiesības neaptver pilnībā jaunā tipa nodarījumus. Taču vienmēr jāpatur prātā, ka par noziedzīgu nodarījumu atzīst tādu, kas savā attīstībā ir sasniedzis tādu pakāpi, kad būtiski sāk ietekmēt sabiedrības likumīgās intereses. Situācija kardināli mainījās, attīstoties globāliem datu pārraides tīkliem, jo tad ielaušanās ADAS vai datortīklu darbības bloķēšana ieguva pilnīgi citu raksturu un līdz ar to sabiedriskās bīstamības pakāpi. Eiropola direktors internetu definēja ļoti īsi, bet kodolīgi : " Tā ir jauna dzīves sfēra un jauna vieta noziegumiem"[480]. ANO Informāciju tehnoloģiju speciālā komiteja savā ziņojumā atzīmē, ka 2004. - 2005. gadā interneta lietotāju skaits var sasniegt vienu miljardu, bet no pasaules preses apskata analīzes viņi var secināt, ka apmēram 80% no kompānijām, kas lieto internetu, ir cietušas no dažādiem uzbrukumiem, ieskaitot krāpšanu, izspiešanu, pakalpojumatteices uzbrukumus, datorvīrusus u.c. veida apdraudējumiem. Tāpēc katrai sistēmai var piemeklēt veidu, kā apiet tās aizsardzības līdzekļus, jo nav vēl pasaulē radīta perfekta datorprogramma

Viens no šādiem uzbrukumiem ir sistēmu darbību traucēšana, izmantojot pakalpojumatteices uzbrukumu (*denial service attacks*). Tas ir trieciens datortīklam,

---

479 Belardo John and Savage Stefan Denial of service attacks: real vulnerabilities and practical solutions. San Diego- Department of Computer science and engineering University of California,[b.g.] p. 4

480 Gelbstein E., Axmad K. Information insecurity a survival guide to the uncharted territories of cyber- threats and cyber-security. New york -United nation IT task force. UNITAR „ 2002., p. 8

ko veido tā pārpludināšana ar tādu papildpieprasījumu skaitu, kas ievērojami palēnina normālo trafiku vai to pat pilnīgi pārtrauc. Pakalpojumatteices uzbrukums parasti uz zināmu laiku pārtrauc tīkla pakalpojumus.[481] . Lai veiktu pakalpojumatteices uzbrukumu, uzbrucējs var izmantot bez lietotāja ziņas šīm mērķim citai personai piederošu un tīklam pieslēgtu ADAS, pārvēršot to par tā saucamo "spoka" (*zombie*) datoru, un iesaista to uzbrukumā, kad vien tas nepieciešams. Šim nolūkam nereti tiek izmantota pilnīgi likumīga programma *Ping*. Pēc sava tiešā mērķa tā ir paredzēta tīkla savienojuma pārbaudei. Šo programmu nereti izmanto uzbrucējs nolūkā pārslogot par upuri izvēlēto sistēmu ar datu paketēm. Ar speciālu programmu palīdzību uzbrucēji spēj pārņemt kontroli pār jebkuru galalietotāja datorsistēmu bez tā īpašnieka ziņas. Ievadot šajā sistēmā speciālu programmu, tā pārņem attiecīgās sistēmas vadību un izmanto to kā uzbrukuma rīku. Šādas programmas var būt datortārpi vai speciāli šīm mērķim izstrādātas programmas.

Piemērs. 2004. gada 17. martā aģentūra Novosti ziņoja, ka Igaunijas Hanza bankas preses sekretārs ziņojis, ka pret banku īstenots iespējams Baltijā lielākais plaša mēroga pakalpojumatteices uzbrukums. Divu dienu laikā uz Hanza bankas elektronisko pastu bija nosūtīti tūkstošiem automatizētu pieprasījumu, kā rezultātā Hanza bankas informācijas sistēma tika pārslogota un uz laiku pārtraukta tās interneta bankas darbība. [482]

Šobrīd vairāki autori, piemēram, E. Grīnbergs (*E. Greenberg*), D. Ļeonovs[483] šo uzbrukuma veidu pēc apdraudējuma bīstamības ierindo pirmajā vietā. Kā liecina CSI/FBI 2003[484] gada aptauja, tad šādu uzbrukumu skaits ar katru gadu palielinās. Tā 1999. gadā 33 % no aptaujātiem ziņoja par šādiem uzbrukumiem, 2003. gadā - 43 %; 2004- 17%.[485] Lai kriminalizētu šo nodarījumu, ir jāizstrādā kvalitatīvi jauna noziedzīgā nodarījuma formula, un šis nodarījums nelīdzinās nevienam no līdz šim kodeksā esošajiem konvencionālajiem noziedzīgajiem nodarījumiem. Jāatzīst arī tas, ka nekad nebūs iespējams sasniegt stāvokli, kad Krimināllikums paredzēs

---

481 http://www.termini.lv/index.php?term=denial%20of%20service%20attack&lang=EN&terms=denial%20service%20attacks (aplūkots 2004.gada 30. maijā).

482 The largest bank of Estonia under hacker attack by Dmitri Kramarenko// http://www.crime-research.org/news/17.03.2004/137 (aplūkots 2004.gada 22. martā).

483 Greenberg Eric Mission critical Security Planner. Creating Customised strategies.Indianapolis- Willey Publishing Inc., 2003. p.40; Леонов Д.Г., Лукацкий А.В., Медведовский И.Д., Семянов Б.В. Атака из Интернет. Аспекты защиты. Москва-Соломон-Р, 2002., с. 231;

484 2003 CSI/FBI Computer crime and security survey

485 2004 CSI/FBI Computer crime and security survay

atbildību par visiem iespējamiem kibernoziegumiem. Tāpēc jāpiekrīt P. P. Robiksam (*P. Robichaux*)[486], ka pilnīgi aizsargāt sistēmu no iespējamiem uzbrukumiem nav iespējams, jo arī uzbrucēji pastāvīgi pilnveido savus darbības veidus.

Kā redzams no iepriekšminētā, tad visi šie apdraudējuma veidi ir vērsti pret ADAS resursiem. Šos apdraudējumus var veikt tikai no attāluma un tikai tajās datorsistēmās, kas ir pieslēgtas internetam. To pierāda arī notikumi Latvijā, ka 2004. gada februāra beigās vairāku sistēmu darbība, daļēji arī Apollo, tika paralizēta, jo sistēmas resursu darbību ievērojami traucēja kāds datorvīruss. Diemžēl oficiālas informācijas par nodarītiem zaudējumiem nav, bet spriežot pēc tā, cik lēns šajā laikā bija kļuvis datu pārraides tīkls un ka 2004.gada 27. un 28. februāri Apollo rīkoja profilaksi, zaudējumi Latvijas informācijas sistēmām bija ievērojami. Tas tikai apliecina, ka Latvija ir cieši saistīta ar visiem ADAS apdraudējumu veidiem un tāpēc prasība harmonizēt mūsu Krimināllikumu atbilstoši starptautisko tiesību prasībām ir pilnīgi pamatota.

Lai izprastu krimināllikumā izdarīto grozījumu būtību, nepieciešams ir problēmu par datu un sistēmu traucēšanu apskatīt dziļāk arī no starptautisko tiesību viedokļa.

*Datu un sistēmu traucēšanas aspekti salīdzinošo tiesību skatījumā*

Dažas valstis, piemēram, Vācija, Francija, Igaunija u.c. būtisku, nelikumīgu traucējumu nodarīšanu datorsistēmai pielīdzina sabotāžai. ES pētījumā *Comcrime* datorsabotāža atzīta par vienu no bīstamākajiem noziedzīgākiem nodarījumiem informācijas jomā.[487] Kā norāda U. Sībers, tad patlaban interneta izmantošana rada jaunas iespējas manipulēt ar datorsistēmas resursiem, kā, piemēram, IP, DNS,[488] un WWW traucēšanu, ko sauc par *spoofing* jeb mānīšanos. Problēma ir tā, ka līdz šim brīdim vairākas valstis nav izdarījušas nepieciešamos grozījumus krimināllikumos, un tāpēc spēkā esošās tiesību normas, kas piemērojamas taustāma, kustama vai

---

[486] Distributed denial of service attacks by P. Robichaux // http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/ddosatku.asp (aplūkots 2004.gada 22. martā).

[487] Legal aspects of computer- related crime in the Information Society – Comcrime- study- prepared for the European Commission by prof. Dr. Ulrich Sieber University of Wurzburg, Version 1.0 of 1st January 1998., p.159.

[488] Sīkāk par IP,DNS un WEB apdraudējuma iespējam skatīt Legal aspects of computer- related crime in the Information Society – Comcrime- study- prepared for the European Commission by prof. Dr. Ulrich Sieber University of Wurzburg, Version 1.0 of 1st January 1998., p. 41 - 42.

nekustama īpašuma aizsardzībai, piemēram, mantas sabojāšana, iznīcināšana, nav attiecināmas uz datorsistēmā esošās informācijas iznīcināšanu, ja nav fiziski bojāta medija materiālā substance. To var attiecināt arī uz Krimināllikuma piemērošanu. Ja eksperti spēja vienoties par to, ka konvencijā ir jāietver nodarījums „datu un sistēmu nelikumīga traucēšana", tad līdz šim vienotības kā sasniegt Konvencijā paredzēto rezultātu, nav. Katra dalībvalsts cenšas risināt šo problēmu atbilstoši savām krimināltiesību tradīcijām. Autors pētot šo problēmu izdala sekojošus risinājuma veidus:

1. Pielīdzināt ADAS datu un sistēmu darbības traucēšanu parastai mantas bojāšanai. Šādu pieeju atbalsta Norvēģija, Austrija, Vācija, Japāna, Zviedrija, Somija, Spānija un citas valstis[489]. Piemēram, Amerikas valstu pastāvīgās padomes organizētā aptaujā Argentīna, Brazīlija, Meksika, Peru atbildēja, ka personas, kas veic darbības, kas saistītas ar automatizēto datu apstrādes sistēmu un datu traucēšanu vai iznīcināšanu, atbild par mantas bojāšanu. Savukārt citas organizācijas valstis atzina, ka par šādiem nodarījumiem krimināatbildība nav paredzēta[490].

2. Atzīt šīs darbības par sabotāžu- kaitniecību un krimināllikumos iestrādāt nosacījumu, ka Krimināllikumā ietvertais noziedzīgā nodarījuma sastāvs sabotāža-kaitniecība attiecas arī uz datu un sistēmu darbības nopietnu traucēšanu[491], piemēram, Vācija (StGB 88. pants)[492]. Dažas EP dalībvalstis, piemēram, Igaunija (KK 270. pants)[493], Ukraina (KK 362.pants), paredz atbildību par datorsabotāžu[494]. 1996. gada 17. februārī tika pieņemts Neatkarīgo Valstu Savienības (NVS) Paraugkrimināl kodekss[495]. Minētā kodeksa 228. pantā ir reglamentēta atbildība par datorsabotāžu. Šī panta 1. punkts paredz krimināatbildību par datorinformācijas vai

---

489 Legal aspects of computer- related crime in the Information Society – Comcrime- study- prepared for the European Commission by prof. Dr. Ulrich Sieber University of Wurzburg, Version 1.0 of 1st January 1998., p. 76

490 Permanent Council of Organisation of American States.responses received to the questionnaire prepared at the first meeting of government experts on cyber crime. GE/REMJA/doc.47/99, 5 October 1999, p.18.

491 Substantive criminal law. Contribution by Mr. M. Möhrenschlager. Committee of Experts on crime in Cyberspace. PC-CY (97) 50 , p. 7

492 Criminal code (Strafgezetzbuch STGB) http://www.iuscomp.org/gla/statutes/StGB.htm (aplūkots 2004.gada 22. martā).

493 Penal code of Estonia http://www.crime-research.org/eng/library/Criminal_Codes.html (aplūkots 2004.gada 22. martā).

494 Responsibility for computer crimes provided by CIS and Baltic countries' criminal law. Computer crime research center. http: www.crime-research.org/eng/library/Criminal_Codes.html (aplūkots 2004.gada 22. martā).

495 Панфилова Е. И. ,Попов Ф. Н. Компютерные преступления Санкт-Петербург 1998., стр. 43 - 46.

programmatūras, vai datorsistēmas tehnisko resursu bojāšanu, bloķēšanu, iznīcināšanu vai to padarīšanu par lietošanai nederīgiem. Minētais formulējums ir pietiekami plašs un aptver arī tādas darbības, ko izdara sistēmas likumīgi lietotāji. Tomēr, jāatzīst, ka NVS valstīs nav vienota pieeja, jo pēc šī kodeksa līdzīgas nostādnes krimināllikumā ir iekļāvušas tikai Baltkrievija (KK 351. pants) un Tadžikistāna (KK 300. pants).

Autors neatbalsta viedokli, ka šīs darbības pielīdzinātu kaitniecībai. Nenoliedzami, ka datu un sistēmas traucēšanai ir zināma līdzība ar šo nodarījumu, tomēr ir arī noteiktas atšķirīgas pazīmes, kas dod pamatu secināt, ka datu un sistēmas traucēšana ir savrups noziedzīgs nodarījums ar sev raksturīgām nodarījuma pazīmēm, kas atšķiras no Krimināllikumā paredzētā nodarījuma kaitniecība. Apskatīšu, kādas ir kopīgās un atšķirīgās pazīmes, kas noteic nepieciešamību šo nodarījumu nodalīt no kaitniecības.

Krimināllikuma 89. pants "Kaitniecība":

*Par darbību vai bezdarbību, kas vērsta uz finansu sistēmas, rūpniecības, transporta, lauksaimniecības, tirdzniecības vai citu tautsaimniecības nozaru, kā arī iestāžu vai organizāciju darbības graušanu nolūkā kaitēt Latvijas Republikai,-*
*soda ar brīvības atņemšanu uz laiku no pieciem līdz divpadsmit gadiem, konfiscējot mantu.*

Kaitniecība ir sevišķi smags noziegums, un šī nodarījuma apdraudētā interese ir Latvijas Republikas ekonomiskās sistēmas stabilitātes apdraudējums. Kā norāda U. Krastiņš, tad kaitniecībai raksturīga slepena, nomaskēta darbība vai bezdarbība. Kaitniecība nav vērsta vienīgi uz kādas konkrētas mantas iznīcināšanu vai bojāšanu, bet aptver plašāku kaitējumu kādai tautsaimniecības nozarei, iestādei vai organizācijai.[496]

Datu un sistēmu traucēšana, gluži otrādi, ir aktīva, redzama darbība. Tā parasti tiek vērsta pret konkrētu nodarījuma objektu un saistīta ar konkrētu zaudējumu nodarīšanu. Nereti pakalpojumatteikuma un kaitīgo rīku uzbrukumi tiek īstenoti plašā mērogā un vērsti uz lielu zaudējumu nodarīšanu, un, protams, mērķis ir traucēt attiecīgo sistēmu darbību, ierobežot iespēju saņemt pakalpojumus un veikt citas likumīgas darbības. Taču ar datu un sistēmu traucēšanu apdraudētā interese ir

---

[496] Krastiņš U. Liholaja V. Niedre A. krimināllikuma zinātniski- praktiskais komentārs (2) Sevišķā daļa. U. Krastiņa redakcijā. Rīga: AFS, 2003., 45.lpp.

informācijas sistēmu drošība un personu mantiskās intereses. Līdz ar to var secināt, ka minēto nodarījumu pamatā nevar pielīdzināt krimināllikumā paredzētai kaitniecībai.

Ņemot vērā pēdējā laika notikumus, ES kopīgo politiku cīņai pret terorismu un organizēto noziedzību, uzskatu, ka gadījumi, kad persona veic šādus uzbrukumus pret valsts informācijas sistēmu, faktiski pēc sekām ir jāvērtē kā vēršanās pret Latvijas Republikas drošības interesēm, jo šāds nodarījums var apdraudēt gan Latvijas Republikas ekonomisko stabilitāti, gan arī valsts un tās iedzīvotāju drošību, un vērtējumam ir jāizpaužas paredzētajā sodā. Taču vienmēr šī nodarījuma rezultātā apdraudētā interese būs informācijas sistēmu drošība. Līdz ar to Kibernoziegumu konvencijas 4. un 5. pantā paredzētie nodarījumi ir jākonstruē kā savrups atsevišķs noziedzīgs nodarījums, nesaistot to ar kaitniecību.

3. Pielīdzināt šīs darbības kādam citam noziedzīga nodarījumam. Piemēram, Lielbritānija 2000. gadā pieņēma Likumu "Par terorismu". [497]Minētā Likuma 1. panta e. punktā ir teikts, ka "par terorismu ir atzīstama darbība, kas saistīta ar nopietnu elektronisko sistēmu darbības traucēšanu vai sagraušanu." Šo likumu piemēro, saucot pie krimināltatbildības personas, kas veic pakalpojumatteices uzbrukumu "*distributed denial service attack*", tas ir, nosūtot milzīgu daudzumu vēstuļu, piemēram, uz premjerministra e- pastkastīti, ar daždažādiem jautājumiem, kā dēļ sistēmas darbība tiek bloķēta. To, ka šādi gadījumi notiek arī citās valstīs, pierāda nesenie notikumi Zviedrijā, kad ebreju aizstāvji no visas pasaules draudēja bloķēt Zviedrijas premjerministra elektronisko pastu, nosūtot tūkstošiem protesta vēstuļu.

4. Radīt jaunu krimināllikuma pantu, kur atbildība būtu tieši paredzēta par datu un sistēmu traucēšanu. Patiesībā šis ir ļoti būtisks jautājums, un īpaši svarīgi bija atrast kopīgu risinājumu, lai kriminalizētu jauna veida noziedzīgu darbību- pakalpojumatteices uzbrukumu. Kā pareizi norāda S. Brennere, tad pakalpojumatteice, kaut arī rada milzīgus zaudējumus kibertelpā izvērstai komercijai, nenodara nevienam no apdraudētiem mērķiem fiziskus zaudējumus.

---

[497] UK Terrorism act 2000// http://www.hmso.gov.uk/acts/acts2000/00011--b.htm#1 (aplūkots 2005.gada 12. janvārī).

Tāpēc šīs darbības nevar kvalificēt kā tradicionālos mantiskos noziedzīgos nodarījumus, piemēram, zādzību, mantas bojāšanu. Šāds uzbrukums nevar tikt kvalificēts arī kā patvaļīga piekļūšana, jo faktiski šāda nodarījuma pazīmju nav. Tāpēc visracionālākais risinājums ir izstrādāt tādu krimināllatbildības pamatu, kas tiktu vērsts tieši pret šo apdraudējuma veidu, tas ir, aizsargājot ADAS datus un sistēmu kopumā no to darbības traucēšanas.[498] Tomēr jautājums nav tik vienkāršs, ka tam uzreiz iespējams atrast vienotu risinājuma formulu. Pat ASV teritorijā ne visu štatu likumdevēji atbalsta šādu pieeju. Kā norāda S. Brennere, tad lielākā daļa ASV štatu ir paredzējuši krimināllatbildību par datoru traucēšanu un ar to saistīto zaudējumu nodarīšanu, bet traucējuma regulējums dalīts divās grupās: 1)ļaunprātīga izmantošana, piem., kriminalizējot tīšu nelikumīgu piekļuvi ADAS un 2) datorvandālisms, ja piekļuves rezultātā ir traucēta vai sagrauta sistēmas darbība.[499]

Vairākas NVS valstis, piemēram, Azerbaidžāna (KK 271.pants), Gruzija (KK 284.pants), Kazahstāna (KK 227. pants), Kirgizstāna (KK 289. pants), Turkmenistāna (KK 334. pants), Krievijas Federācija (KK 272. pants), paredz atbildību par patvaļīgu piekļuvi datorinformācijai un atbildību par sistēmas resursu bojāšanu vai traucēšanu. Kā jau minēts iepriekš, tad autors neatbalsta šādu pieeju, jo pakalpojumatteices uzbrukums nav tieši saistīts ar patvaļīgu piekļuvi ADAS, līdz ar to šīm valstīm praksē var rasties problēmas krimināllatbildības piemērošanā par šāda rakstura nodarījumiem. Šobrīd tikai Ukrainas Krimināl kodeksa 361. pants paredz atbildību par nelikumīgu sistēmu un tīklu traucēšanu, ja tā rezultātā pārtraukta vai sagrauta sistēmas darbība. Kā norāda Ukrainas kibernoziegumu centra vadītājs V. Golubevs, tad šī redakcija pamatā atbilst Kibernoziegumu konvencijas nostādnēm.[500]

---

[498] Cybercrime investigation and prosecution: The role of the penal and procedural law by S. W. Brenner// E-law – Murdoch University Electronic journal of law.Vol. 8 Nr.2 (June 2001) http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html (aplūkots 2004.gada 22. martā).

[499] State cybercrime legislation in the United States of America: A. Survay by S. W. Brenner// Richmond Journal Law & Technology 28. (Winter 2001), http://www.richmond.edu/jolt/v7i3/article2.html (aplūkots 2004.gada 22. martā).

[500] Criminal and legal aspects of fighting crime by V. Golubev. http://www.crime-research.org.library/Golubev_nov.html (aplūkots 2004.gada 22. martā).

ES Komisijas Informācijas sabiedrības ģenerāldirektorāta izstrādātajā rokas grāmatā[501] par datoru un tīklu ļaunprātīgas izmantošanas juridiskām procedūrām atzīmēts, ka līdz 2002. gadam no ES dalībvalstīm par noziedzīgiem nodarījumiem pret informācijas sistēmu drošību kriminālatbildību neparedzēja Austrija, Grieķija un Īrija. Pārējās ES dalībvalstis paredzēja kriminālatbildību par visiem noziedzīgiem nodarījumiem pret informācijas sistēmu drošību.

Iepriekšminētais liecina par nepieciešamību ietekmēt šo procesu ar starptautisko tiesību līgumiem un Eiropas Savienības valstīs ar speciālu normatīvo aktu- ES Padomes ietvarlēmumu, jo, neskatoties uz to, ka Konvencijas izstrādāšanā piedalījās gan Austrijas, gan Grieķijas, gan arī Īrijas pārstāvji, tomēr šo valstu teritorijas šobrīd veidojas kā "miera ostas" personām, kas izdara noziedzīgus nodarījumus pret informācijas sistēmu drošību, jo joprojām kriminālatbildība par šādiem nodarījumiem nav paredzēta.

*Datu traucēšanas (Krimināllikuma 243. panta 1.daļa) objekts un priekšmets*

Spēkā esošā KL 243. panta 1.d. redakcija pēc būtības nemaina ne, iepriekšējā (līdz 01.06.2005.) noziedzīgā nodarījuma sastāva grupas, ne arī speciālo objektu. Šis noziedzīgais nodarījums tieši ir vērsts pret informācijas drošības pazīmi- integritāti, jo likumdevējs ir paredzējis atbildību par nelikumīgām darbībām ar sistēmā esošo informāciju, tas nozīmē, ka jebkura nelikumīga darbība ar sistēmas resursiem ir tieši vērsta pret sistēmas īpašnieka vai likumīgā valdītāja interesi saglabāt sistēmas informācijas resursu veselumu (integritāti). Izmainoties panta redakcijai, mainās tikai noziedzīgā nodarījuma sastāva priekšmets, jo par to atzīta ir automatizētā datu apstrādes sistēma.

*Automatizētās datu apstrādes sistēmas darbības traucēšana (Krimināllikuma 243. panta 2.daļa) objekts un priekšmets*

Kā minēts iepriekš, tad noziedzīgs nodarījums automatizētās datu apstrādes sistēmas darbības traucēšana, iekļauts krimināllikumā, lai valsts spētu aizsargāt personu pret uzbrukumiem, kas tiek veikti no eletroniskiem tīkliem. Lai kā arī

---

[501] Handbook of legislative procedures of computer and network misuse in EU countries. Study for the European Commission Directorate-General Information society (2002) Rand Europe. © ECSC-EC-EAEC, Brussels-Luxembourg 2003, p. 18.

juristi negribētu iedziļināties minētā nodarījuma tehniskajās detaļās, taču bez to analīzes, kas dota iepriekš, nav iespējams noteikt apdraudēto interesi. Kā jau autors minējis iepriekš, tad Rietumvalstu zinātnieki lielu vērību apdraudējuma objekta noteikšanai nepievērš. Arī Krievijas zinātnieki īpaši nav analizējuši šajā pantā paredzēto noziedzīgā nodarījuma objektu. Tas izskaidrojams ar to, ka vēl daudzas valstis nav veikušas nepieciešamos grozījumus krimināllikumā, lai saskaņotu to ar Kibernoziegumu konvencijas prasībām.

Analogu prasību ES dalībvalstīm izvirza ES Padomes priekšlikums ietvarlēmumam par uzbrukumiem informācijas sistēmām.[502] Minētā lēmuma 3. pants noteic, ka „..katrai dalībvalstij jāveic nepieciešamie pasākumi, lai paredzētu krimināalatbildību par nelikumīgām darbībām, kas saistītas ar tīšu nopietnu informācijas sistēmu funkcionēšanas traucēšanu vai pārtraukšanu, ievadot, nosūtot, bojājot, iznīcinot, pasliktinot, pārveidojot, noklusējot vai padarot nepieejamus datordatus". Minētā lēmuma 4. pants pieprasa atzīt par krimināli sodāmām analogas darbības, kas vērstas pret informācijas sistēmā esošiem datiem. Kā redzams no izvirzītiem nosacījumiem šo darbību kriminalizācijai, tad apdraudētā interese ir informācijas sistēmas resursu integritāte. Daļēji šīm prasībām atbilst Krimināllikuma 243. pants. Taču, lai atklātu, kādi labojumi ir nepieciešami Krimināllikumā, jo ietvarlēmuma 12. punkts noteic dalībvalstīm, tai skaitā arī topošajām dalībvalstīm, veikt nepieciešamos juridiskos pasākumus šī Lēmuma izpildē līdz 2004. gada 31. decembrim, ir nepieciešams aplūkot citu valstu pieredzi šo problēmu risināšanā.

Daļa pasaules valstu par šāda veida nodarījumu sauc personas pie atbildības par kaitniecību[503]. Nenoliedzami, ka zināma līdzība starp abiem šiem nodarījumu veidiem pastāv, tāpat kā patvaļīgai piekļūšanai ar zādzību no dzīvokļa u.c. Viss mūsu dzīvē ir relatīvi kaut kādā veidā saistīts, un, ja arī ir radītas kaut kādas atšķirības ar zinātnes sasniegumu izmantošanas palīdzību, tad visas tās tāpat kā likumus ir radījis cilvēks. Starpība ir tikai tā, ka tehnoloģiski ir iespējams jebkuras ierīces savietot un pēc tam lietot kompilācijā ar reālā vidē esošo infrastruktūru, bet

---

[502] Proposal for a Council framework decision on attacks against information systems. COM (202) 173 final

[503] International response to cybercrimes Ch.2. by Tonya L. Putnam, David D. Eliot Huver Press,[b.g] p.39

jurisprudencē šīs atšķirības ir grūtāk pārvaramas, tāpēc joprojām pastāv objektu dalījums ķermeniskos un bezķermeniskos, lietu iedalījums mantiskās un nemantiskās, taustāmās un netaustāmās utt. Lai mainītu to vai citu juridisko kritēriju piemērošanu, nepieciešama politiska griba, kuras reizēm pietrūkst. Neskatoties uz to, ka noziedzīgiem nodarījumiem pret informācijas sistēmu drošību galvenā apdraudētā interese ir personas tiesības izmantot savus ADAS resursus, tomēr nevar izslēgt arī personu apdraudētās mantiskās intereses. Kā minēts ES Komisijas priekšlikumā par ietvarlēmumu par uzbrukumiem informācijas sistēmām[504], tad šī nodarījuma bīstamība izpaužas tieši tajā apstāklī, ka tas apdraud augsta profila informācijas resursus, kā portālus, vortālus, kuri veidoti kā attiecīgās personas uzņēmējdarbības sastāvdaļa, kā piemērā ar uzbrukumu Igaunijas Hanza bankas resursiem, kuru rezultātā banka bija spiesta pārtraukt interneta bankas pakalpojumus.

Piemērs. Microsoft Baltija organizētajā preses konferencē 2004. gada 14. februārī tika publiskoti dati, ka *spam* rezultātā mazs uzņēmums, kurā ir tikai septiņi darbinieki, mēnesī zaudē apmēram 700-800 latu. Tas ir laiks, ko attiecīgā uzņēmuma darbinieki ir spiesti patērēt, lai attīrītu savu datoru no drazu pasta. Cik lielus zaudējumus cieš tādas sistēmas, kas sastāv no 100 un vairāk datorsistēmām, tikai parasta "drazu pasta" rezultātā, ir diezgan viegli aprēķināt.

Speciālisti kā raksturīgākos pakalpojumatteices uzbrukuma mērķus[505] nosauc šādus:

1) mēģinājumi pārpludināt tīklu, tādejādi traucējot un ietekmējot tīkla darbības spējas;
2) mēģinājumi pārtraukt savienojumus starp divām sistēmām, tādā veidā traucējot tiesības uz pakalpojuma pieejamību;
3) mēģinājumi traucēt konkrētu indivīdu saņemt informācijas pakalpojumu;
4) mēģinājumi pārtraukt konkrētai personai piederošu sistēmas darbību.

No iepriekšminētiem pakalpojumatteices uzbrukuma mērķiem, var secināt, ka apdraudētā interese ir sistēmas resursu integritāte, kas izpaužas informācijas aprites traucēšanā, datortīklu pārslogošanā, bloķēšanā utt. Protams, ka var tikt apdraudēti arī citi ISD elementi, kā konfidencialitāte un pieejamība, taču prioritāri darbība ir vērsta pret ieprogrammēto sistēmas resursu darbības veselumu, tas ir integritāti. Tāpēc par galveno tiešo apdraudējuma objektu atzīstama resursu integritāte.

---

504 Proposal for a Council framework decision on attacks against information systems. COM (202) 173 final

505 CERT coordination center. Denial of service attacks// http://www.cert.org/tech_tips/denial_of_service.html (aplūkots 2004.gada 22. februārī).

Kā norādīts Konvencijas paskaidrojošā memorandā, šie abi iepriekšminētie panti tika iestrādāti tādēļ, lai datu vai datorsistēmas bojājuma gadījumā tai nodrošinātu tādu pašu aizsardzību, kas paredzēta par tīšu zaudējumu nodarīšanu ķermeniskām lietām.[506] Aizsargātā juridiskā interese šeit ir pienācīga datorprogrammu un datu lietošana.[507] Tāpēc arī minētā panta 3.daļa paredz kvalificējošu pazīmi, atbildību, ja 1. un 2.d. paredzētais nodarījums veikts mantkārīgu tieksmju dēļ. Tas nepieciešams, lai aizsargātu arī personu mantiskās intereses.

Apdraudējuma priekšmets. Autors pilnīgi piekrīt, piem., V. Golubevam[508], kurš uzsver, ka, runājot par tiešo apdraudējuma priekšmetu, noziedzīgos nodarījumos pret informācijas sistēmu drošību, īpaši jāuzsver un jāskaidro tiesību speciālistiem, ka par tādiem atzīstami tikai integrēti, tas ir savstarpēji nesaraujami saistīti ADAS resursi. Līdz ar to nav papildus dalāmi informācijas nesējos, datortehnikas programmatūrā un citos tehniskos elementos. Jo tas tikai un vienīgi var radīt kolīzijas tā vai cita priekšmeta elementa satura noteikšanā un lietojuma interpretācijā. Šādu pieeju atbalstīja arī likumdevējs formulējot Krimināllikuma 243. panta redakciju. Krimināllikuma 243. panta 2. daļa paredz atbildību par sistēmu darbības traucēšanu. Šis nodarījums ir vērsts pret ADAS resursiem kopumā, to skaitā tīkliem, programmatūru, sistēmblokiem, rūteriem un citām datu apstrādi nodrošinošām ierīcēm. Līdz ar to par šī noziedzīgā nodarījuma priekšmetu atzīstami sistēmas resursi plašākā izpratnē. Tāpēc pareizi ir likumdevēja pieeja, nosakot, ka atbildība iestājas par apzinātu visas sistēmas resursu kopuma darbības traucēšanu, ja ar to tiek sabojāta aizsardzības sistēma vai nodarīti zaudējumi lielos apmēros. Tikai KL 243. panta 4.daļā paredzētā nodarījumā darbības priekšmets būs automatizētā datu apstrādes sistēma, kurai valsts ar normatīvu aktu, noteikusi speciālu aizsardzības režīmu, atzīstot to par valsts informācijas sistēmu un iekļaujot to attiecīgā valsts informācijas sistēmu reģistrā.

---

506 Cybercrime Convention. Explanatory report CM (2001) 1444 addendum, para 65.

507 Explanatory report CM (2001) 144 addendum. p.18

508 Голубев В.Типология преступлений в сфере использования ЭВМ. http://www.crime-research.ru/library/Golubev1203.html (aplūkots 2004.gada 22. martā).

1. Darbība. Krimināllikuma 243. pantā paredzēto nodarījumu var izdarīt tikai ar tīšu darbību. Šīs darbības var tikt izdarītas tikai izmantojot citu automatizētu datu apstrādes sistēmu, un veiktas no attāluma. Par šādu darbību atzīstama jebkura rīcība, ja tās rezultātā tiek pasliktināta, bojāti vai pilnīgi iznīcināti sistēmas resursi. Kibernoziegumu konvencija un ES Komisijas „Priekšlikums Padomes ietvarlēmumam par uzbrukumiem informācijas sistēmām"[509] noteic dalībvalstīm pienākumu paredzēt krimināalatbildību par darbībām, kas izsauc būtiskus sistēmas darbības traucējumus un pārtraukumus. Eiropas Savienības komisija 2001. gada 5. oktobrī publiskoja dokumentu „Priekšlikumi Padomes ietvarlēmumam par nopietnu uzbrukumu, kas vērti pret informācijas sistēmām apkarošanu" *(on combating serious attacks against information systems e Eiropa 2002.*" Minētā dokumenta 1.1.b. pantā " sistēmu sagraušana" norādīts, ka sistēmu sagraušanu var veikt, izdarot dažādu veidu ļaunprātīgus uzbrukumus, piemēram, ar pakalpojumu atteikuma uzbrukumu vai ietekmējot to serveru darbību, kas veic operācijas ar domēnu vārdu sistēmām, pārtraucot vai vadot to maršrutēšanu. Sevišķi bīstami šie uzbrukumi ir augsta profila mājas lapām, piemēram, portāliem.[510]

**Sistēmu un datu traucēšana**. Traucēšana Konvencijas izpratnē ir tīša, prettiesiska nopietna datorsistēmas darbības funkciju traucēšana, kavēšana, ievadot, pārsūtot, bojājot, iznīcinot, pasliktinot, modificējot datordatus.[511] Traucējums ir jebkurš nevēlams signāls, kas ierobežo vai pasliktina ierīces spēju veikt tai paredzētās funkcijas.[512]

Viens no ceļiem ko bija iespējams izvēlēties konstruējot šī noziedzīgā nodarījuma sastāvu bija izteikt panta redakciju vispārīgā formulējumā, piemēram, "par automatizētā datu apstrādes sistēmā esošas informācijas neatļautu **traucēšanu**

---

509 Proposal for a Council framework decision on attacks against information systems. COM (202) 173 final

510 Commission of the European Communities. Proposal for a Council framework decision on combating serious attacks against information systems. eEirope 2002// http://cryptome.org/eu-antihack.htm (aplūkots 2004.gada 22. martā).

511 Convention on cyber-crime. Budapest, 23.XI.2001

512 USA Federal Communication Commission Compliance& Information bureau Interferrence handbook. http://www.fcc.gov/cib/Publications/tvibook.html (aplūkots 2003.gada 12. aprīlī).

**vai iznīcināšanu**, ja ar to bojāta vai sagrauta aizsardzības sistēma vai nodarīts būtisks kaitējums". Pētot šo problēmu, kā arī ievērojot Kibernoziegumu konvencijas nostādnes, jāatzīst, ka šāds panta formulējums būtu pārāk vispārīgs un pretrunīgi interpretējams. Tādējādi rastos grūtības tā praktiskā piemērošanā. Raksturīgākie skaidrojumi: traucēšana - kavēšana[513], oponenta bloķēšana[514]; darbības, kas izmaina, pārtrauc, modificē[515]. Patiesībā kavēšana arī aptver visus šobrīd Krimināllikuma 243. panta projekta 1. daļā ietvertās pazīmes. To, kā sekmēsies likuma piemērošana parādīs tikai prakse. Noziedzīgā nodarījuma ADAS traucēšana objektīvo puse ir pilnīgi analoga Krimināllikuma 243. panta 1. daļā aprakstītai, jo visas pantā ietvertās darbības iekļaujas termina "traucēšana" saturā. Jāatzīmē, ka tā saucamie interneta uzbrukumi var būt kombinēti, tas ir ne tikai sūtot liela apjoma datu paketes, bet arī sūtot speciāli inficētas ar vīrusu datu paketes un tādā gadījumā šāda uzbrukuma sabiedriskā bīstamība ievērojami palielinās. Kā minēts iepriekš, tad šī nodarījuma pamatā ir aktīva darbība. Persona izstrādā uzbrukuma stratēģiju, izvēlas konkrētu mērķi un realizē savu nodomu.

Nodarījuma objektīvo pusi: veido panta redakcijā uzskaitītās darbības. Jāatzīst, ka tas nav visai labs risinājums pantā uzskaitīt konkrētas darbības, jo diezin vai būs iespējams jebkad krimināllikumā ietvert pilnīgi izsmeļošu tādu darbību uzskaitījumu, kas var ietekmēt vai sagraut sistēmas informācijas resursus un aizsardzības līdzekļus. Īsi aplūkošu dažus minētā nodarījuma sastāva objektīvās puses elementus.

1. *Datu dzēšana (erasure).* Traucējumi datorsistēmā, kas radīti, dzēšot datus, var tikt pielīdzināti ķermeniskas mantas bojāšanai, to apstiprina arī termina izdzēšana *deletion* saturs, proti, ka datu vai datorprogrammu datu dzēšana ir darbība, kas izposta, sagrauj datus vai datorsistēmu, respektīvi, padara tos par neatpazīstamiem un nelietojamiem. Mantas bojāšana reālā pasaulē tāpat rada sekas, ka mantu nevar izmantot tam mērķim, kam tā bija domāta.
2. *Aizklāšana (supression).* Aizklāšana nozīmē jebkuru darbību, kas beidz

---

513 Onelook dictionary search// http://www.onelook.com/?w=interference&ls=a (aplūkots 2004.gada 13. martā).

514 Merriam Webster On-line// http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=interference (aplūkots 2004.gada 12. martā).

515 WikipediA The free Encyclopedya // http://en.wikipedia.org/wiki/Interference (aplūkots 2004.gada 22. martā).

pieeju datorsistēmā vai medijā saglabātiem datiem. Šis termins satur divas nozīmes: 1) ka dati ir nodzēsti un tie vairs fiziski neeksistē; 2) ka tie padarīti nepieejami, tas ir, šiem datiem nevar piekļūt un tie ir ekspluatācijai nederīgi.

3. *Datu pārveidošana* (*alteration*). Ar datu pārveidošanu (*alteration*) saprot jebkuru esošo datu modifikāciju, kas sevī ietver arī tādas darbības kā, piemēram, datu un sistēmas vai ar pārraidi saistīto datu viltošanā (*spoofing*), ko sauc par mānīšanos. Tas ietver saturā pašu par sevi likumīgu ziņojumu gatavošanu, kuru identifikācija ir viltojums. Tā ietver sevī arī šifrēšanu, kas padara datus par nesalasāmiem, bet ne nepieejamiem.[516]
4. *Bojājumus, ko sistēmai nodara kaitīgas programmas*, tajā skaitā vīrusi un citas tiem pielīdzinātas programmas[517]. Kā atzīmēts ES Komisijas 2001. gada 5. oktobra priekšlikuma 1.1.c. pantā, tad apmēram 11% no visiem Eiropas Savienības personālo datoru lietotājiem atzinuši, ka viņu datorsistēmu darbību ietekmējušas kaitīgās programmas[518]. CSI/FBI 2004.gada veikta aptauja parādīja, ka joprojām 78% no aptaujā iesaitītām sistēmām bija cietušas no kaitīgu programmu iedarbības.
5. *"Konservēšana"* (*spamming*). Datorsistēmu lietotājiem nereti tiek piesūtīti liela apjoma elektroniskā pasta ziņojumi, ko speciālisti žargonā sauc par „drazu pastu" *spamming*.[519] Drazu pasta problēmu juridiski mēģina ierobežot vairākas valstis, kā, piemēram, ASV, Austrālija, Lielbritānija u.c. Nevēlama uzmākšanās, izmantojot e - pastu (*unwanted solicitation*), tiek apzīmēta ar kopīgu terminu „*spam*", tā var ievērojami traucēta datu apriti un sistēmas darbību un ievērojami ietekmēt e- komercijas attīstību pasaulē.[520]

---

516 Cybercrime Convention Explanatory report CM (2001) 144 addendum, para 61

517 Konvencijas izpratnē pie šādām programmām pieskaita jebkuru datorprogrammu vai ierīci, kuras mērķis ir traucēt datordatus vai sistēmas resursus. *Inter alias* programmām speciālisti pieskaita datorvīrusus, graujošas programmas kā tārpi (*worm*) un datorindes (*computer contaminant*) Sk. Substantive criminal law contribution by Mr.M. Möhrenschlager (Ministry of Justice Germany) PC-CY 997)50, p. 13

518 Commission of the European Communities. Proposal for a Council framework decision on combating serious attacks against information systems. eEirope 2002// http://cryptome.org/eu-antihack.htm (aplūkots 2004.gada 12. martā).

519 Par *spamming* uzskatāma jebkura darbība, kad persona, tīši, izmantojot IT e - pasta veidā vai pa faksu sūta dažāda veida anonīmas nelūgtas reklāmas, par lizinga, nomas, tirdzniecības pakalpojumu iespējām, ja tās apjoms var traucēt datorsistēmas vai tīkla darbību. Cyber- crime Model Code §2.04.2 Dayton University USA.

520 U.S. House Committee Passes Anti-Spam Bill by Dave Murhy. http://dgl.com/itinfo/2000/it000323.html (aplūkots 2001.gada 12. maijā).

2004. gada 22. janvārī[521] ES Padome pieņēma paziņojumu Eiropas Parlamentam, Padomei, Eiropas Ekonomiskajai un sociālajai komitejai un Reģionu komitejai par surogātpastu vai „*spam*". Paziņojumā uzsvērts, ka neprasīta sazināšanās pa e-pastu komerciālos nolūkos jeb „*spam*" ir sasniedzis satraucošus apmērus, jo 2001. gadā tas bija tikai 7% no globālā e-pasta trafika, bet pašlaik „*spam*" ir vairāk kā 50% no tā. *Spam* apdraud informācijas privātumu, patērētāju tiesības, nepilngadīgos un cilvēka cieņu, biznesa izmaksas un produktivitātes kāpumu.[522] Minētā dokumenta 2.3. paragrāfā uzsvērts, ka *spam* tehnoloģija tiek izmantota arī, lai izdarītu tādus kibernoziegumus kā patvaļīga piekļuve, iegūstot informāciju par datora lietotāja identitāti, un tā apkarošanas pasākumi ir ietverti Eiropas Komisijas priekšlikumā ietvarlēmumam par uzbrukumiem informācijas sistēmām, kas tuvākā laikā tiks oficiāli apstiprināts.

Piemērs. Izmantojot "drazu pasta" tehnoloģiju, uzbrucējam ir iespējams iegūt informāciju par sistēmas lietotāju un tādējādi īstenot patvaļīgu piekļuvi sistēmai, izmantojot paša sistēmas īpašnieka identifikatorus.[523] Savukārt, izmantojot citu kaitīgu rīku (*computer contaminant*)[524], uzbrucējam ir iespējams nelikumīgi nokopēt sistēmā esošu informāciju un to atklāt citām personām. Prakse pierāda, ka nereti kaitīgo rīku ietekme ir vērsta uz sistēmas aizsardzības rīku sagraušanu, tādējādi sagraujot arī sistēmas īpašnieka noteikto pieejamības kārtību.

Jāatzīst arī, ka ne visi speciālisti šo darbību skaidrojumus un Konvencijā ietvertās definīcijas atzīst par pareizām, piemēram, Š. Hopkinsa (*Shannon L. Hopkins)* [525] uzskata, ka Konvencijā ietvertās definīcijas ir neskaidras un pārāk plaši tulkojamas, kas var radīt nepareizu dalībvalstu priekšstatu par problēmas risinājuma ceļiem. Tomēr autors uzskata, ka Konvencijā un ES ietvarlēmuma priekšlikumā dotie darbību skaidrojumi, ir pietiekami objektīvi un tos var piemērot arī Krimināllikumā. Domājot par "pakalpojumatteices" nozīmi kā datorsistēmas darbības traucēšanas veidu, uzmanība jāpievērš apstāklim, ka šādu sistēmas traucējumu var nodarīt arī tad, ja persona, kas sūta "pakalpojumatteici", ir likumīgs

---

[521] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or "spam" COM (2004) 28 final

[522] Informācijas sabiedrības birojs.Instrukcija par padomes secinājumu projects "par surogātpastu" jeb" spam".

[523] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or "spam" COM (2004) 28 final

[524] Substantive criminal law. Contribution by Mr. M. Möhrenschlager. Committee of Experts on crime in Cyberspace. PC-CY (97) 50 , p. 13

[525] Cybercrime Convention : A Positive beginning to a long road ahead. Shannon L. Hopkins//Journal of high technology law, 2003.

sistēmas resursu lietotājs, tāpēc Konvencija noteic, ka dalībvalstīm ir jāparedz krimināl atbildība tikai par būtisku elektronisko komunikāciju darbības traucējumu. To, ka arī likumīgs sistēmas lietotājs var, sūtot "pakalpojumatteikumus", būtiski traucēt datorsistēmu darbību, pierāda pēdējie notikumi, kur šādu darbību rezultātā uz vairākām stundām tika kavēta tādu informācijas gigantu kā *CNN*[526] un piemērā minētās Igaunijas Hanza bankas un citu IS darbība. Šie uzbrukumi liecina, ka kibernoziegumi kļūst aizvien izsmalcinātāki, un, kā norāda vairāki tiesību speciālisti, tad šie jaunie *modus operandi* atklāj aizvien jaunus un jaunus „caurumus" dalībvalstu krimināl likumdošanā. Latvija arī nav izņēmums. Ar „pakalpojumatteici"[527] ievadot liela apjoma datus datorsistēmā, persona īsteno zināmu kontroli pār informācijas resursiem un tādā veidā apzināti traucē sistēmas darbu. Tomēr tā tieši neīsteno patvaļīgu piekļuvi, jo kontrole pār sistēmas resursiem nozīmē to, ka tiek bloķēta pieeja sistēmas sniegtajiem pakalpojumiem, pārslogojot pārraides tīklus, un tādējādi tiek traucēts sistēmas normāls darbs.

Analizējot Krimināllikuma 243. panta 3. daļas noziedzīgā nodarījuma sastāvu, jāņem vērā, ka atbildība par šo nodarījumu iestājas tikai tad, ja persona ir veikusi Krimināllikuma projekta 243. panta 1. vai 2. daļā paredzēto nodarījumu atbildību pastiprinošos apstākļos. Minētā panta 3. daļas iekļaušana Krimināllikumā ir saistīta ar to, ka gan Kibernoziegumu konvencija, gan arī ES priekšlikums ietvarlēmumam 7. pants un tā paskaidrojošais memorands par šādiem apstākļiem ieteic atzīt gadījumus, ja nodarījums veikts organizētā grupā vai mantkārīgos nolūkos, vai nodarījuma rezultātā iestājušās smagas sekas.[528] Īstenojot pakalpojumatteices uzbrukumu vai ietekmējot sistēmas darbību kaitīgām datorprogrammām vai rīkiem, noziedzīgi nodarījumi tiek veikti plašā mērogā, piemēram, uzbrukums veikts no vairākām vietām vienlaicīgi.

---

526 Attīstās tādi jauni noziegumu veidi, kā, piemēram, tā sauktie DDOS uzbrukumi (*distributed denial of service*), kur nav nepieciešams piekļūt datorsistēmai, lai izdarītu nopietnu postošu darbību.Sk. Crimes related to computer networks-Some legal aspects by Hans G. Nilson[b.g][b.i].

527 Kibernoziegumu Konvencijas paskaidrojošā memorandā termins *spamming* definēts kā darbības, kas saistītas ar datu nosūtīšanu konkrētai personai tādā formā un apjomā vai biežumā, ka tie atņem saņēmējam iespēju izmantot pilnīgi vai daļēji sistēmas resursus vai pārslogo sistēmu ar "drazu pastu (*junk mail*), kas var padarīt sistēmu par darboties nespējīgu. Tas attiecas arī uz "*denial sercice attacks*), kur tiek sūtīts liels daudzums lūgumu vai pieprasījumu un tādā veidā tiek pārslogota datorsistēma. Šada darbība pati par sevi var būt likumīga, bet veids, kādā tā tiek darīta, ir nelikumīgs. Sk.Draft RM EXPC-CY (2001) 1 rev, 12 p..

528 Proposal for a Council framework decision on attacks against information system. COM (2002)173 final Explanatory report, p. 21

Piemērs. V. Golubevs apraksta šādu tipisku plaša mēroga ielaušanās shēmu. Ja viena persona mēģina uzlauzt datorsistēmas aizsardzību, to ir diezgan viegli pamanīt. Tāpēc elektroniskā laušana notiek no vairākām vietām vienlaicīgi. Piemēram, vienā šādā uzbrukumā ir iesaistītas vienlaicīgi 10 ADAS. No visiem datu apstrādes termināliem tiek veikts ielaušanās mēģinājums. Tas noved pie tā, ka dažus no uzbrucējiem sistēmas drošība atšķeļ, bet citi iegūst nepieciešamo pieeju. Viens no uzbrucējiem bloķē sistēmas tīkla statistiku, kas fiksē piekļuves gadījumus. Līdz ar to sistēmas drošības līdzekļi vairs nespēj atklāt un fiksēt uzbrucējus. Pēc tam daļa no uzbrucējiem uzsāk nepieciešamā informācijas sektora uzlaušanu, bet citi nodarbojas ar fiktīvām darbībām ar mērķi dezorganizēt sistēmas darbu un slēpt nozieguma pēdas.[529] Ar līdzīgu uzbrukuma shēmu Ukrainas hakeri uzlauza Skotijas Karaliskās bankas (*Royal bank of Scotland*) maksājumu sistēmu un sagrāva to, kā rezultātā hakeri ieguva informāciju par 27 000 bankas klientu visā pasaulē, kas norēķinās ar VISA un MasterCard, un citām elektroniskām maksājumu formām.

Krimināllikuma 48. pants par atbildību pastiprinošiem apstākļiem atzīst gan to, ka noziedzīgs nodarījums izdarīts personu grupā, gan arī to, ka noziedzīgais nodarījums izdarīts mantisku tieksmju dēl, gan arī to, ka nodarījums izraisījis smagas sekas.

1. Organizētā grupa.

*21.pants. Organizēta grupa*

*(1) Organizēta grupa ir vairāk nekā divu personu izveidota apvienība, kura radīta nolūkā kopīgi izdarīt noziedzīgus nodarījumus vai smagu vai sevišķi smagu noziegumu un kuras dalībnieki saskaņā ar iepriekšēju vienošanos sadalījuši pienākumus.*

*(2) Atbildība par nozieguma izdarīšanu organizētā grupā personai iestājas šajā likumā paredzētajos gadījumos par grupas izveidošanu un vadīšanu, piedalīšanos smaga vai sevišķi smaga nozieguma sagatavošanā vai noziedzīga nodarījuma izdarīšanā neatkarīgi no personas lomas kopīgi izdarītajā nodarījumā.*

A. Niedre norāda, ka noziedzīgs nodarījums ir izdarīts personu grupā neatkarīgi no tā, vai tas ir izdarīts grupā ar vai bez iepriekšējas vienošanās, kā arī vai to izdarījusi organizēta grupā.[530] Līdzīgu viedokli, komentējot Krimināllikuma 175. pantu, pauž arī U. Krastiņš, norādot, ka zādzība ir izdarīta personu grupā pēc iepriekšējas vienošanās, ja vismaz divas personas pirms zādzības sākšanas vienojušās par tās izdarīšanu kopīgi un zādzību arī izdarījušas.[531] Līdz ar to ir jāpiekrīt viedoklim, ka, lai atzītu par konstatētu faktu, ka personas ir izdarījušas noziedzīgu nodarījumu organizētā grupā, ir nepieciešams konstatēt, ka nodarījumā ir iesaistītas vismaz divas personas un ka tām jau pirms nodarījuma izdarīšanas bija

---

[529] Голубев В.Типология преступлений в сфере использования ЭВМ. http://www.crime-research.ru/library/Golubev1203.html (aplūkots 2004.gada 22. martā).

[530] Krastiņš U., Liholaja V. Niedre A. Krimināllikuma zinātniski- praktiskais komentārs (1) Vispārīgā daļa. U. Krastiņa redakcijā. Rīga: AFS, 2003., 159. lpp.

[531] Turpat, Krastiņš U., Liholaja V. Niedre A, 2003.,9.lpp.

vienošanās izdarīt noziedzīgās darbības, kuras tika arī realizētas. Kā redzams no iepriekšminētā piemēra, tad, organizējot plaša mēroga uzbrukumu konkrētai informācijas sistēmai, personas ir precīzi sadalījušās uzdevumus un lomas, līdz ar to faktiski var runāt par stabili izveidotu organizētu noziedzīgu grupu Krimināllikuma 21. panta izpratnē. No aprakstītā piemēra redzams, ka šādas grupas plānotam un realizētam uzbrukumam vienmēr raksturīgs paaugstināts kaitējums, līdz ar to pamatoti arī starptautiskās institūcijas izvirza šo pazīmi noteikt kā atbildību pastiprinošu.

2. Mantkārīgais nolūks. Mantkārīgais nolūks ir atzīts par atbildību pastiprinošu apstākli daudzos Krimināllikuma sevišķās daļas pantos, un jāpiekrīt A. Niedrem, ka par mantkārīgu nolūku atzīstams jebkurš gadījums, kad persona, kas izdara noziedzīgu nodarījumu, vēlas iegūt jebkura veida materiālus vai cita rakstura ekonomisku labumu sev vai citai personai.[532] Tādējādi, ja persona, kas īsteno uzbrukumu informācijas sistēmai, piemēram, lai sagrautu konkurenta darba spējas un tādā veidā gūtu priekšroku uzņēmējdarbībā, iegūst sev vai citai personai noteikta veida ekonomisku labumu. Tādā gadījumā persona ir veikusi nodarījumu mantkārīgos nolūkos.

*Sekas.* Likumdevējs Krimināllikumā 243. pantā paredzēto nodarījumu veidojis kā materiālu noziegumu sastāvu, jo atbildība šeit iestājas tikai pie konkrētiem nosacījumiem. Minētā panta 1.daļā atbildība iestājas tikai tad, ja darbības saistītas ar aizsardzības līdzekļu pārvarēšanu vai būtiska kaitējuma nodarīšanu sistēmas resursu īpašniekam vai tiesiskajam valdītājam.

*1.Ja tiek bojāta vai iznīcināta ADAS aizsardzības sistēma.* Aizsardzības sistēma ir programmatūra, kas pasargā sistēmu no resursu traucēšanas vai bojāšanas. Ja aizsardzības sistēma strādā paredzētā režīmā, tad tas var nodrošināt sistēmas resursu aizsardzību vismaz par 50%, taču, ja aizsardzības sistēma tiek vājināta, sagrauta, tad šāds stāvoklis ir pielīdzināms pamestai mājai, kurā jebkurš interesents var ieiet, apskatīties telpas un mierīgi no tās iziet, palaikam paņemot arī kādu tur atstātu lietu vai vērtību. Tāpēc, autoraprāt visos noziedzīgos nodarījumos pret

---

[532] Turpat, Krastiņš U., Liholaja V. Niedre A., 161. lpp.

informācijas sistēmu drošību ir svarīgi izcelt sistēmas drošības līdzekļus kā īpašu noziedzīgā nodarījuma priekšmetu.

2. Mantiskās sekas. Likumdevējs Krimināllikuma 243.1.d. pantā paredzēto atbildību ir saistījis arī ar būtiska kaitējuma radīšanu. Šis jautājums ir apskatīts iepriekš. Nenoliedzami, ka viena no būtiska kaitējuma sastāvdaļam ir mantiskais elements un tāpēc var droši teikt, ka likumdevējs, kā vienu no atbildības nosacījumiem ir paredzējis mantisku seku iestāšanos, būtiska kaitējuma, lielu zaudējumu vai smagu seku veidā. Līdz ar to analizējot Krimināllikuma 243. panta 3. daļā ietverto nodarījumu, var izdarīt secinājumu, ka minētais nozieguma sastāvs vērsts ne tikai uz ADAS resursu integritātes aizsardzību, bet arī uz sistēmas īpašnieku mantisko tiesību aizsardzību. Tas tikai apliecina šī nozieguma sastāva komplekso raksturu.

6.4. Datora vīrusa izplatīšana (līdz 01.06. 2005.) un nelikumīgas darbības ar automatizētās datu apstrādes sistēmu resursu ietekmēšanas ierīcēm" (28.04.2005.) KL 244. pants )

| KL 243. pants | Redakcijā Līdz 1.06. 2005.<br><br>**Datora vīrusa izplatīšana** | 28. 04. 2005. redakcijā<br><br>**Nelikumīgas darbības ar automatizētās datu apstrādes sistēmu resursu ietekmēšanas ierīcēm** |
|---|---|---|
| 1. daļa | Par datora vīrusa, tas ir, tāda programmas līdzekļa apzinātu izplatīšanu, kas izraisa datortehnikas programmatūras vai informācijas nesankcionētu iznīcināšanu vai grozīšanu, vai kas sabojā informējošo iekārtu vai sagrauj aizsardzības sistēmu, vai par jauna veida vīrusa ievadīšanu datortehnikas programmatūras vidē-,<br>soda ar brīvības atņemšanu uz laiku līdz četriem gadiem vai ar naudas sodu līdz divsimt minimālajām mēnešalgām. | Par tādas ierīces (arī datorprogrammas) neatļautu izgatavošanu, pielāgošanu izmantošanai, realizēšanu, izplatīšanu vai glabāšanu, kura paredzēta automatizētās datu apstrādes sistēmas resursu ietekmēšanai nolūkā izdarīt noziedzīgu nodarījumu,-<br>soda ar brīvības atņemšanu līdz četriem gadiem vai ar piespiedu darbu, vai ar naudas sodu līdz simt piecdesmit minimālajām mēnešalgām. |
| 2.daļa | Par tādām pašām darbībām, ja ar tām radīts būtisks kaitējums,-<br>soda ar brīvības atņemšanu uz laiku līdz 10 gadiem. | Par tām pašām darbībām, ja tās izraisījušas smagas sekas,-<br>soda ar brīvības atņemšanu uz laiku līdz desmit gadiem vai ar naudas sodu līdz divsimt minimālajām mēnešalgām |

Lai precīzi noteiktu šī nodarījuma **objektu**, ir nepieciešams noskaidrot, kāda ir tā interese, ko apdraud kaitīgās ierīces izgatavošana, neatļauta izgatavošana,

pielāgošana izmantošanai, realizēšana, izplatīšana vai glabāšana nolūkā izdarīt noziedzīgu nodarījumu. Faktiski atšķirības izpaužas divos aspektos: 1) teorētiskās terminoloģijas izpratnē, apzīmējot objektu ar sabiedriskām attiecībām vai apdraudēto interesi. Lielākā daļa Krievijas zinātnieku šī noziedzīgā nodarījuma objektu apzīmē ar sabiedriskām attiecībām. bet Rietumvalstīs, par nozieguma objektu atzīst apdraudētās likumīgās intereses. 2) objekta satura robežas. Iepriekš jau es minēju, ka Latvijas tiesību doktrīna par noziedzīgā nodarījuma objektu atzīst apdraudēto tiesisko interesi. Cik plašas var būt apdraudētās intereses robežas? Arī šajā jautājumā nav īstas vienprātības, jo daļa autoru uzskata, ka tās ir tikai attiecības, kas saistītas ar informācijas aizsardzību sistēmas iekšienē[533], bet ir arī autori, kas uzskata, ka aizsargātai sabiedriskai attiecībai jāattiecas arī uz informācijas pārraides procesu datortīklos, piemēram, pārraidot informāciju citam lietotājam[534]. Patiesībā tas ir jautājums par to, ko mēs saprotam ar apdraudēto resursu robežām. Kā minēts iepriekš, tad viens no Krimināllikuma no labojumu mērķiem ir novērst juridiskās atšķirības starp dažādām ierīcēm, vai ierīču grupām, kuru mērķis ir veikt automatizētu datu apstrādi un kas savienotas ar elektroniskiem sakaru tīkliem. Ja ADAS ir savienota ar elektronisku sakaru tīklu, tad šīs robežas ir tik tālu, cik tīkls integrējas pašā sistēmā. Piemēram, Kanādas kibernoziegumu eksperts D. Piragofs (*Donald Piragoff*) definē teritoriālo principu kibertelpā atbilstīgi tīkla „ģeogrāfijai", ka".. tās ir robežas, kas nodala tīkla lietotājus, kuri ir tīkla sastāvdaļa, no tiem, kas atrodas ārpus tā".[535] Tādējādi aizsargājamā interese aptver informācijas sistēmas drošību jebkurā tās fāzē. Līdz ar to, paplašinot ADAS saturu, faktiski zūd robeža starp informācijas aizsardzību sistēmā integrētos datu nesējos un tīklā. Citiem vārdiem runājot, objekts apzīmē interesi būt drošam par sistēmas datu aizsardzību no sabojāšanas un iznīcināšanas, izmainīšanas vai citas ietekmes.

---

[533] Росийское уголовное право. Особенная ч. Учебник. Под. Ред. М.П. Журавлева и С.М. Никулина. Москва: Спарк, 1998.,с.336

[534] Ibid, Волеводз А.Г. с.72

[535] PC-CY (97) 40 Computer- related investigations:serch and seizure. Options paper by Donald K. Piragoff and Larisa L. Easson Canada, September 1997., p.2.

Ja mēs analizējam KL 244. panta dispozīciju, tad šeit faktiski apdraudētā interese ir informācijas sistēmas drošības pazīme- integritāte. Par to liecina likumdevēja vēlme fokusēt panta dispozīciju uz darbību aprakstu, kas apdraud informācijas resursu veselumu, piemēram, iznīcināšana vai bojāšana, grozīšana, aizsardzības sistēmas sagraušana utt. Analogu viedokli izsaka arī V. Krilovs, norādot, ka KPFSR KK 273. panta "Kaitējumu nesošu programmu izgatavošana un izplatīšana" objekts ir sabiedriskās attiecības, kas rodas, aizsargājot ESM esošas informācijas integritāti no ārējās ietekmes.[536] Līdzīgu viedokli izsaka arī I. Klepickis, norādot, ka objekts ir īpašnieka tiesība uz sistēmas un sistēmā glabātās informācijas neaizskaramību (programmatisko nodrošinājumu).[537] Tomēr jāatzīst, ka šī apdraudējuma objekta noteikšanā vienota viedokļa nav. Piemēram, A.Voļevodzs norāda, ka šī nodarījuma objekts ir tiesiskās attiecības informācijas aprites drošības jomā, neminot konkrētu apdraudējuma pazīmi[538], bet A. Pašins norāda, ka šī nodarījuma objekts ir datorsistēmu izmantošanas lietisko un intelektuālo līdzekļu drošība.[539] Autors atbalsta A. Voļevodza viedokli, ka ar datorvīrusu izplatīšanu tiek apdraudēta informācijas sistēmas drošība kopumā. Jo ar to palīdzību var tikt īstenota gan patvaļīga piekļūšana datorsistēmai, gan apdraudēta sistēmā esošo informācijas resursu integritāte, gan ar datorvīrusa palīdzību var atklāt informāciju tām personām, kam uz to nav tiesību, respektīvi, pārkāpt arī konfidencialitāti.

Piemēram, R. Standlers (R.B. Standler) apraksta, ka 1999. gadā Melisa vīruss inficēja kādā sistēmā glabātu slepenu dokumentu un šo dokumentu automātiski kopā ar vīrusa programmu nosūtīja citām personām. Viņš norāda, ka šie jaunā tipa bīstamie vīrusi ir jauns veids, kā ietekmēt gan konfidencialitāti, gan integritāti, gan arī pieejamību.[540]

Analogu viedokli atbalsta arī Kibernoziegumu ekspertu komiteja. Kibernoziegumu konvencijas paskaidrojošā ziņojuma 71. punktā[541], norādot, ka

---

536 Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва: Юриспрудения. 1999.,с. 658.

537 Уголовное право Российской федерации. Особенная часть. Под. ред. Б.В. Здравомыслова. Москва: Юристь, 1999., с. 357

538 Ibid, Волеводз А.Г. с. 73

539 Коментарый к уголовному кодексу Росийской федерации. Издание 3-е измененное и дополненное. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва: издательская группа Инфра · М- Норма, 2000., с. 704

540 Computer crime by R. B. Standler// http://www.rbs2.com/ccrime.htm#anchor111111 (aplūkots 2002.gada 22. martā).

541 Explanatory report. CM (2001) 144 addendum, para 71

kaitīgās ierīces ir paredzētas visu noziedzīgo nodarījumu pret informācijas sistēmu drošību veikšanai. Līdz ar to var izdarīt secinājumu, ka Krimināllikuma 244. panta objekts ir visu informācijas sistēmu drošības elementu (integritātes, konfidencialitātes un pieejamības) apdraudējums.

*Noziedzīgā nodarījuma rīka (datorvīruss) noteikšanas problēmas*

Likumdevējs bija gājis vienkāršāko ceļu un noteicis atbildību tikai par datorvīrusa izplatīšanu, uzskatot, ka šis termins, ko nereti izmanto kā žargonu izmanto datorprogrammu speciālisti, pilnīgi aptver arī jebkuru kaitīgo programmu, kas var ietekmēt sistēmā esošās informācijas neatļautu modifikāciju, iznīcināšanu vai sistēmas darbības kavēšanu. Šādu viedokli atbalsta arī V. Liholaja, kas datora vīrusu identificē ar jebkuru kaitīgu programmu.[542] Šādam viedoklim autors nevar piekrist, jo vīrusi ir maza daļa - apmēram 10%[543] no visu kaitīgo programmu klāsta, kas var kaitīgi iedarboties uz datorprogrammām.

M. Kolombels (*Mark R. Collombel*) [544] norāda, ka datorvīruss ir speciāli veidota datorprogramma ar mērķi ietekmēt informācijas sistēmas resursus. Datorvīrusa uzdevums nosaka viņa programmētājs. R. Standlers apraksta šādas datorvīrusa darbības iespējas ietekmēt sistēmā esošo izpildprogrammu darbību, piemēram, tas var parādīt tikai ievadinformāciju monitorā, var iznīcināt pilnīgi vai daļēji sistēmas cietajā diskā esošo informāciju vai grozīt tās saturu.[545]

J. Čirilo norāda, ka vīruss ir pasīva forma iekļūšanai cietušā datorsistēmā, un tos klasificē: 1) *sektora* vīrusi, kas tiek pārnēsāti disketēs un pielīp datorsistēmai tad, kad diskete pievienota sistēmai; 2) *programmu* vīrusi jeb *failu* vīrusi atrodas failos, kuros paplašinājums ir *exe* vai *com.* Atverot šos failus, datorvīruss pielīp citām programmām; 3) *polimorfie vīrusi* (*polimorhic virus*) [546], piemēram, vīruss, kurš izgatavots tādā veidā, ka var mainīt uzdevumu, inficējot jaunas datorsistēmas vai to daļas; 4) *daudzdalījumu vīruss* (*multi partite virus*), piemēram, „*Raseks*" ietekmē

---

[542] Krastiņš U., Liholaja V., Niedre A. Krimināllikuma Zinātniski- praktiskais komentārs. (3) Sevišķā daļa. U. Krastiņa redakcijā. Rīga: AFS", 2003, 231..lpp.

[543] M. Mohrenschlager "Substantive criminal law" PC- CY ( 97) 50 p.13

[544] The legislative response to the evalution of computer viruses by: Mark R. Collombel .The Richmond journal of law and technology. Vol. VIII, Issue 3, Spring 2002.

[545] Computer crime by R. B. Standler// http://www.rbs2.com/ccrime.htm#anchor111111 (aplūkots 2002.gada 22. martā).

[546] Polimorhic virus // http://www.fcs.uga.edu/~mhazen/projects/re95/polymorph.html (aplūkots 2004.gada 22. martā).

sistēmas pamatdatnes sāknēšanas ierakstus un nodara citu kaitējumu.[547]; 5) „*Trojas zirgs*" maskējoties kā labdabīga programma, pieprasa atbrīvot datoru no vīrusa, bet vienlaikus atbrīvo ceļu kaitīgajai programmai; 6) *makrovīruss* izplatās mazas programmiņas veidā un noglabājas datorā, kad tiek atvērts jebkurš fails. Makrosa programmu savā datorā var izveidot jebkurš lietotājs, bet, neuzmanīgi rīkojoties ar šo programmu, viņš pats var radīt vīrusu.[548] Kā redzams, tad šeit nav uzskaitītas visas iespējamās kaitīgās programmas. Taču šajā uzskaitījumā ir apvienotas programmas, kurām ir līdzīgi darbības principi.

Šie darbības principi ir tas iemesls, kas attur krimināltiesību speciālistus no idejas apvienot ar vārdu "datorvīruss" visas kaitīgās datorprogrammas. Šie darbības principi ir: 1) programmu spēja pašām sevi kopēt un pavairot, un ietekmēt datus un informāciju, to modificējot; 2) nespēja izpildīt uzdevumus patstāvīgi. Vīrusu datorsistēma parasti saņem ar elektronisko pastu ar pielikumu (*attachment*). Tikai pēc tam, kad lietotājs, nepārliecinoties par sistēmas drošību, atver pielikumu, vīruss uzsāk savu kaitīgo darbību un iedarbojas uz sistēmas resursiem.

V. Krilovs juridiski korekti kaitīgās programmas pēc to apdraudējuma rakstura ir klasificējis trīs klasēs: *Pirmā klase* –spēj pastāvīgi vairoties, ne vienmēr rada būtiskus kaitējumus IS, bet dažreiz var modificēt informāciju, dažreiz bloķē IS darbību. Izstrādātāji neuzskata šo kaitējumu nesošo programmu par sevišķi bīstamu. *Otrā klase*- bīstamie vīrusi, kas sagrauj informācijas sistēmu un nodara būtisku kaitējumu. *Trešā klase*- paredzēti, lai organizētu nelikumīgu pieeju informācijai. Tādas kaitīgās programmas, kas nodrošina pieeju sistēmai un priviliģētu darbības režīmu ar to sauc par "lūkām" (*back door*). Pēdējie nodara būtisku kaitējumu IS resursiem.[549]

---

547 Virus information library// http://vil.nai.com/vil/content/v_98229.htm (aplūkots 2004.gada 22. martā ).

548 Chirillo John Hack attacks encyclopedia. A complete history of hacks, cracks, phreaks and spies over time. New-York-Willy Computer Publishing. John Willey & Sons Inc., 2001., p.300

549 Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва: Юриспрудения. 1999.,с.659

ASV datortiesību speciālisti visas šīs kaitējumu radošās, destruktīvās programmas apzīmē ar jēdzienu „kaitīgs kods" (*malicious code*)[550]. Šo *sui generis* apzīmējumu piemēro tāpēc, ka šodien neviens nezin, kādas kaitīgas programmas veidu var izstrādāt nākotnē, taču kods apzīmē jebkuru programmu.

Runājot par kaitīgām programmām, autors nevar nepieminēt tādus programmu veidus: 1) kā "*tārps*", (*worm*). Šobrīd tieši datortārpi nodara vislielākos zaudējumus un rada vislielāko sabiedrisko bīstamību. Galvenā atšķirība starp vīrusu un tārpu ir tā, ka "tārps" var pats sevi kopēt un lietot atmiņu, bet, pretēji vīrusam, pats nevar pieķerties citai programmai; 2) loģiskās bumbas, kuru darbība uzsākas noteiktos apstākļos; 3) speciāli radītas programmas ar mērķi apiet drošības sistēmu un veikt sistēmā konkrētu programmētāja noteiktu darbību.

Piemērs. Viens no pazīstamākajiem ASV kibernoziegumu ekspertiem Dons Parkers (*Don Parker*) ir izpētīja tādu datornoziegumu paveidu, ko viņš nosaucis par „automatizētu noziegumu" (*automated crime*).Viņš norāda, ka programmai, kas izdara šo noziegumu, ir jāizdara ne mazāk kā sešas darbības: 1)skanēt un meklēt datoru, kas satur uzbrukumam nepieciešamo vērtību; 2) atklāt izvēlētās sistēmas vājās vietas un sagatavot sistēmu uzbrukumam, 3) izmantot šo vājo vietu kā ieejas vārtus sistēmā un piekļūt pie informācijas resursiem, 4) savienot tos ar konkrētām kriminālām darbībām, 5) konvertēt savas darbības mantiska labuma formā noziedzniekam vai kaitējuma veidā cietušajam; 6) likvidēt pierādījumus, kas liecinātu par kriminālām darbībām.
Parkers norāda, ka šī programma noziegumu izdara 1/1000 daļā sekundes un ka pēc tā izdarīšanas nav atrodamas pēdas, un tā ir tālu no tā, lai to vienkārši varētu atzīt par datorvīrusu [551], bet neapšaubāmi tā ir kaitīga programma, kas programmēta ar mērķi izdarīt noziegumus.

Šos piemērus autors min tāpēc, lai pierādītu, ka *burtiski* tulkojot KL 244. pantā terminu „vīruss", nav iespējams saukt pie atbildības personas, kas izmantos citas destruktīvas programmas. 244. panta redakcijā līdz 2005.gada 1. jūnijam, likumdevējs šo problēmu risināja ar terminu- *jauna veida vīrusa ievadīšana datortehnikas programmatūras vidē*. V. Liholaja norāda, ka par jauna veida vīrusa ievadīšanu jāsaprot jebkuras jauna veida destruktīvas programmas ievadīšana sistēmā, tās kopēšana, reproducēšana un izplatīšana.[552] No tā var secināt, ka komentāra autore par jauna veida vīrusu atzīst jebkuru **destruktīvu** programmu. Tomēr, kas ir jauna veida destruktīva programma, V. Liholaja nav atbildējusi.

---

[550] Computer crime by R. B. Standler// http://www.rbs2.com/ccrime.htm#anchor111111 (aplūkots 2004.gada 22. martā); Understanding incident response// http://www.fedcirc.gov/library/documents/understanding.html (aplūkots 2004.gada 22. martā).

[551] Cybercrime &Security compilled & edited by A.Brill Oceana, 1998. booklet 1.1. by Donn Parker Automated crime 1.1-1-1.1.9.

[552] Krastiņš U., Liholaja V., Niedre A. Krimināllikuma Zinātniski- praktiskais komentārs. (3) Sevišķā daļa. U. Krastiņa redakcijā. Rīga: AFS", Rīga, 2003, 231.lpp.

Autors jau ir izteicis viedokli, ka komentārs tāpat kā teorija ir viena vai vairāku lietpratēju vīzija vai viedoklis par apskatāmo problēmu. Tāpēc nenoliedzami rodas jautājums, kāpēc likumdevējs konstruējot Krimināllikuma 244. panta 1. daļu, paredzēja atbildību: 1) par datora vīrusa- tāda programmatiskā līdzekļa, kas izraisa datortehniskas programmatūras nesankcionētu iznīcināšanu vai grozīšanu, izplatīšanu; 2) par jauna veida vīrusa ievadīšanu datortehniskas programmatūras vidē. Domāju, ka īstas skaidrības nav arī iepriekšminētā komentāra autorei, jo terminus „datorvīruss" gan „jauna veida vīruss" viņa ir skaidrojusi faktiski identiski, proti, kā destruktīvas programmas. Analizējot vārdu kopu, *jauna veida vīruss*, autors saskata iespēju par šī nodarījuma priekšmetu atzīt un līdz ar to saukt pie atbildības jebkuru personu, kas ievada sistēmā jebkuru programmu, kas nenoliedzami ar ievadīšanas brīdi ietekmē sistēmas programmatisko vidi.

Šīs bažas tikai apstiprinās ar to, ka par šādu jauna tipa vīrusu V. Liholaja atzīst arī sīkdatni (*cookies*[553]). Problēma rodas tāpēc, ka praksē ir pietiekami daudz programmatisku resursu, kas, izmantojot kādu pakalpojumu, automātiski tiek ievadīti pakalpojuma saņēmēja sistēmas informācijas resursos un zināmā mērā ietekmē arī programmatisko vidi, piemēram, *cookies*, *deep links, hipersaites* un citi. Šie programmatiski resursi, izgatavoti pilnīgi likumīgiem mērķiem. Sīkdatne (*cookies*), atrodama ikvienā datorsistēmā, ja dators strādā tiešsaistes režīmā, to iedarbība uz datorsistēmu nav pilnībā izpētīta, kaut gan speciālisti nenoliedz šīs sīkdatnes kaitīgo ietekmi uz sistēmu. Ja mēs ejam šādu ceļu, tad teorētiski jebkuru datorprogrammu var izmantot kaitīgos nolūkos, bet tāpēc jau neviens visas datorprogrammas neuzskata par kaitīgām. Tā ir pretrunā ar Kibernoziegumu konvencijas nostādnēm, kuras autors analizēs turpinājumā. Ļoti precīzi problēmu ir raksturojuši ANO pētnieki, norādot, ka pasaulē nav tehniski nevainojamu datorprogrammu, jo katrā programmā ir jau iekodētas tādas kļūdas, kas ietver jau vīrusus. Praksē pierādījumus guvuši šādi atzinumi: 1) jauna datorprogramma nozīmē jaunus tehniskus defektus; 2) vecie tehniskie defekti nav vienmēr izlaboti; 3) labojumi ne vienmēr ir uzinstalēti; 4) arī labojumi var veicināt tehnisku defektu

---

[553] Krastiņš U., Liholaja V., Niedre A. Krimināllikuma Zinātniski- praktiskais komentārs. (3) Sevišķā daļa. U. Krastiņa redakcijā. Rīga: AFS", Rīga, 2003, 231.lpp.

iespējamību, bet jebkurš tehnisks defekts - tā ir jauna vīrusa attīstības iespējamība.[554]

*No datora vīrusa līdz kaitīgai ierīcei vēsturiskais apskats*

Modernā datora "tēvs" Džons Van Noimans (*John Van Neuman*) jau kopš 1948. gada loloja ideju par pašreproducējošu datorprogrammas koda izstrādāšanu. 1970. gadā notika pat speciālas mācības datorvīrusu rakstīšanā. Šīs programmas nosauca (*Core wars*), un to uzdevums bija mākslīgi radītā vidē cīnīties vienai pret otru.[555]

1972. gadā Džons Drapers (*John Drapper*) atklāja, ka plastmasas svilpe, ieliekot to brokastu pārslu pakā, ģenerē 2600 hercu toni, kā rezultātā radās *hakeru* tehnoloģija, ko pazīst ar nosaukumu *blue box,* kas izmanto toņa ģenerēšanu, lai piekļūtu ASV telekompānijas AT&T tīkliem un iegūtu brīvu pieeju pakalpojumiem.

1979. gadā Kseroksa firmas inženieri izstrādāja mazu programmu- datortārpu, kuras uzdevums bija pārmeklēt datortīklu nolūkā atrast bojātus un nestrādājošus procesorus. Šī programma ir priekštecis tām kaitīgajām ierīcēm- datortārpiem, kas paredzētas ADAS informācijas resursu traucēšanai vai iznīcināšanai.[556]

Katra diena var būt sākums jaunas informācijas tehnoloģijas ierīces radīšanai. Piemēram, V. Krilovs, komentējot KF Krimināl kodeksa 273. "Kaitējumu radošu programmu izgatavošana un izplatīšana" pantu, norāda, ka".. agrāk literatūrā lietoja terminus „datorvīruss" un „informatīvās infekcijas", taču, lai paplašinātu priekšstatu par šāda veida programmām, KF likumdevējs ir izvēlējies šo apdraudējuma veidu saistīt ar kaitējumu nesošu programmu (*вредоносная программа*)[557]. S. Pašins norāda, ka „.. programma tiek uzskatīta par atbilstošu KK 273. panta aizliegumam tad, ja tā rada negatīvas sekas, tas ir, izsauc informācijas

---

554 Gelbstein E., Kamal A. Information insecurity. A survival guide to the unchartered theritories of cyber-threats and cyber security.- New York Published by the United Nations ICT Task Force and the United Nations Institute for Training and Research, 2002, p. 17

555 General viruses issues // http://macsupport.miningco.com/compute/macsupport/msub4.htm ; (aplūkots 2001.gada 10. februārī). http://macsupport.about.com/compute/macsupport/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.symantec.com%2Favcenter%2Fvinfodb.html (20.05.2001.) ; http://macsupport.miningco.com/compute/macsupport/msub4.htm (aplūkots 2001.gada 10. februārī).

556 A short history of computer viruses and attacks by Brian Krebs// http://www.securityfocus.com/news/2445 (aplūkots 2004.gada 10. martā).

557 Уголовное право. Часть общая. Часть особенная. Учебник. Под. Ред Л.Д. Гаухмана, Л.М. Колодкина,С.В. Максимова. Москва: Юриспрудения. 1999б с.658;

manipulācijas.[558] Līdzīgu viedokli izsaka arī V. Liholaja, šo pašu apzīmējumu attiecinot tikai uz datora vīrusu[559]. Kā minēts iepriekš, tad ne katra kaitējumu radīt spējīga programma var tikt atzīta par šī nodarījuma aizlieguma objektu. Šo problēmu ir akcentējuši arī Krievijas tiesību zinātnieki, piemēram, S. Pašins un A. Voļevodzs, norāda, ka nav pasaulē uzrakstīta instrukcija, kas dod iespēju nepārprotami pateikt, vai tā vai cita programma var tikt atzīta par minētā nodarījuma aizlieguma objektu. Programmu kaitīgumu vai derīgumu nosaka nevis pēc spējas iznīcināt, bloķēt, modificēt, kopēt informāciju **(tās ir pilnīgi tipiskas absolūti legālu programmu funkcijas**), bet gan saistībā ar to, vai programmas darbības piedāvā: 1) īpašniekam informāciju par programmas raksturu; 2) to piekrišanas saņemšanu, lai programma realizētu savas funkcijas. Ja netiek ievērots viens no šiem nosacījumiem, tad programma uzskatāma par kaitīgu.[560] Autors pilnīgi piekrīt šādam viedoklim.

Tāpēc Tieslietu ministrijas speciālisti, kas sagatavoja attiecīgos grozījumus Krimināllikumā, vienojās, ka panta darbība ir jāattiecina gan uz jebkuru programmu, gan arī citu ierīci, ko personas var izmantot ar mērķi nelikumīgi traucēt citai personai piederošu ADAS darbību, jo, kā pareizi norāda A. Pašins, tad nav sodāma kaitīgu programmu izmantošana personīgos nolūkos, piem., lai iznīcinātu sev sistēmā piederošu informāciju.[561] To, ka tiesību speciālistu vidū Latvijā nebija īstas skaidrības, ko uzskatīt par kaitīgu ierīci, apliecināja arī Iekšlietu ministrijas speciālisti, kas savā atzinumā norādīja, ka no Krimināllikuma 244. panta pirmās daļas projektā nepieciešams svītrot vārdu "neatļauta kaitīgu ierīču lietošana", norādot, ka tādā veidā tiek paredzēta situācija, ka kaitīgā ierīce var tikt izmantota

---

[558] Коментарый к уголовному кодексу Росийской федерации. Издание 3-е измененное и дополненное. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва: издательская группа Инфра · М- Норма, 2000., с. 704;

[559] Turpat, Krastiņš U. Liholaja V, Niedre A., 231.lpp.

[560] Коментарый к уголовному кодексу Росийской федерации. Издание 3-е измененное и дополненное. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва: издательская группа Инфра · М- Норма, 2000., с. 704

[561] Ibid, Коментарый к уголовному кодексу Росийской федерации. с. 704;

arī likumīgi.[562] Tas nozīmē, ka jāveic liels darbs krimināltiesību speciālistu izglītošanā.

Piemērs. Sīkdatne (cookies) tiek ievadīta lietotāja datorā, lai atvieglotu darbu ar mājas lapām. Sīkdatņu ievadīšanu ADAS atļauj arī speciālās interneta pārlūkprogrammas Explorer un Netscape. Sīkdatne var tikt izmantota arī, lai iegūtu datus par lietotāja atrašanās vietu. Taču šie skripti, sīkdatnes var tikt arī izmantoti ļaunprātīgos nolūkos, piemēram, lai iegūtu lietotāja paroli un citu ADAS drošības līdzekļu informāciju. Ar šāda skripta palīdzību nepiederošas personas var piekļūt sistēmā aizsargātas informācijas apgabaliem un izmantot to savām vajadzībām, sīkdatne var tikt apzināti inficēta ar citu kaitīgu pašreplicējošu programmu.[563]

Ja likumdevējs izpildītu Latvijas Iekšlietu ministrijas speciālistu prasību, tad Latvijā būtu jāaizliedz ne tikai sīkdatņu, bet arī citu skriptu lietošanu. Globālā tīmekļa kontekstā skripts ir programma, kas atrodas kādā tīmekļa serverī un apstrādā no pārlūkprogrammas saņemtos pieprasījumus. Tas ir pilnīgi neiespējami.

Savukārt cits piemērs liecina, ka ir arī speciāli izveidotas programmas, kuru mērķis ir vērsts tikai uz sistēmas datu un darbības traucēšanu.

Piemērs. 2004.gada 20. februārī tika atklāta kaitīga programma W32.Mydoom.F@mm. Antivīrusu programmatūras firmas *Symantec* speciālisti norāda, ka šī programma spēj: 1) masveidā izplatīties pa elektronisko pastu un atver lūkas (*back doors*) TCP protokolā, kura uzdevums ir pārbaudīt datu nosūtīšanas pareizību no klienta uz serveri[564], dodot pieeju pieslēgvietai 1080; 2) var patvaļīgi ielādēt sistēmā izpildprogrammas; 3) ja tas atrodas sistēmā no 17.-22. mēneša datumam, tad tas var no šīs sistēmas izveidot pret www.microsoft.com pakalpojumatteices uzbrukumu; 4) izveido speciāli atstātu ceļu izstrādājamajā programmā vai sistēmā, lai tajā varētu iekļūt, apejot drošības vadīklas, un tas dod iespēju uzbrucējam savienoties ar datoru un gūt ar šī datora lietotāja tiesībām piekļuvi serverim vai tīkla resursiem.[565]

Kā redzams, tad starp sīkdatni vai skriptu un datortārpu Mydoom, ir liela atšķirība, jo Mydoom ir veidots kā polimorfa kaitīga ierīce ar nolūku nodarīt pēc iespējas lielāku kaitējumu sistēmu resursiem un tam nav sociāli derīga mērķa. Taču Krimināllikuma 244. pantu paredz attiecināt ne tikai uz kaitējumu nesošām datorprogrammām, bet arī uz skriptiem un citiem instrumentiem, ko personas var izmantot, lai ietekmētu informācijas sistēmu drošību, piemēram, pakešu okšķerēšanu[566], dažādu skanēšanas programmu, maršrutētāju veidošanu piekļuves

---

562 Latvijas Republikas Iekšļietu ministrija "Par likumprojektu "Grozījumi Krimināllikumā"VSS-208) 24.02.2004 Nr.1/31-494

563 CERT ® Coordination center. Frequently asked questions about malicious web scripts redirected by web sites// http://www.cert.org/tech_tips/malicious_code_FAQ.html (aplūkots 2004.gada 10. martā).

564 Introduction to TCP/IP// http://www.yale.edu/pclt/COMM/TCPIP.HTM (aplūkots 2004.gada 10. martā).

565 W32.Mydoom.F@mm // http://www.sarc.com/avcenter/venc/data/w32.mydoom.f@mm.html (aplūkots 2004.gada 10. martā).

566 Programma vai ierīce, kas pārrauga datu pārvietošanos datoru tīklā. Okšķeri var izmantot divējādi: normālai tīkla pārvaldības funkciju izpildei un nesankcionētai informācijas izguvei no datoru tīkla. Nesankcionēti okšķeri var radīt

nodrošināšanai u.c. Tomēr nevar izslēgt, ka jebkura no šīm ierīcēm, kaut arī tās mērķis ir ietekmēt datus, tomēr var tikt izmantota arī sociāli derīgam mērķim.

Tāpēc bija ļoti svarīgi Krimināllikuma 244. panta dispozīcijā iekļaut vārdu, ka atbildība par šādu ierīču izgatavošanu un izplatīšanu iestājas tikai tad, ja tā ir veikta **neatļauti**. Ja mēs paredzētu atbildību par jebkuru šādas ierīces, kas var traucēt sistēmas resursu normālu darbību un apdraudēt to integritāti izgatavošanu vai izplatīšanu, tad Latvijā patiesi varētu rasties stāvoklis, ka ikvienu personu, kas pārbauda sistēmas drošību un šīm nolūkam izveido šādu ierīci, varētu saukt pie krimināLatbildības. Šāds stāvoklis būtu iespējams arī tāpēc, ka Krimināllikuma 244. panta 1. daļā paredzētais nodarījums ir formāls un tā izdarīšana uzskatāma par pabeigtu ar kaitējumu radīt varošas ierīces izgatavošanu, realizēšanu, izplatīšanu, glabāšanu vai citādi padarot to par izmantojamu. No iepriekšteiktā var secināt, ka pilnīgi pamatoti ES Komisijas priekšlikumā ietvarlēmumam par izbrukumiem informācijas sistēmām izvirzīta prasība paredzēt gadījumus, kad šādas darbības attaisnojamas.

Jāatzīst, ka kaitīgu ierīču radīšana un izplatīšana nav tikai ASV vai Kanādas problēma vai citu attīstītāko valstu problēma, jo to radītāji ir no dažādām valstīm, piemēram, 1986. gadā vīrusu "Brain" izstrādāja Pakistānas pilsoņi, 1986. gadā vīrusu "Vir dem" izstrādāja vācu programmētājs, R. Burgers, 1988. gadā vīrusu „Jerusalem" izstrādāja Jeruzales universitātes speciālisti, 1989. gadā vairāki vīrusi tika izstrādāti Krievijā, 1990. gadā Bulgārijā tika atklāta vīrusu izgatavošanas darbnīca[567], un, protams, nevar nepieminēt 2000. gadā Filipīnās izgudroto un izplatīto "I love you"[568] Šo sarakstu varētu turpināt, jo nav salīdzināmas programmas, kas tika radītas XX gadsimta 70.-80. gados, ar tiem kaitīgajiem rīkiem, kuru ietekmi mēs izjūtam šodien. Tomēr jāatzīst, ka par kaitīgām ierīcēm nosauktie vīrusi, datortārpi un citas ierīces pēc savas sākotnējās nozīmes nebija radītas ar mērķi apdraudēt citu personu informācijas sistēmas. To radīšana bija

---

nopietnus draudus datoru tīkla drošībai, jo tos grūti atklāt un tie var tikt ievietoti jebkurā tīkla vietā. http://www.termini.lv/index.php?term=sniffer&lang=EN&terms=sniffing (aplūkots 2004.gada 23. martā).

567 The history of computer viruses// http://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml (aplūkots 2004.gada 10. martā).

568 Short history of computer viruses and attacks by Brian Krebs// http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26?start=15&per=18 (aplūkots 2004.gada 10. martā).

saistīta ar sabiedriski derīgu mērķi, tas ir, kontrolēt, pilnveidot informācijas sistēmu drošību, atklāt kļūdas datorprogramās u.c. Pašreplicējošās programmas ir kļuvušas par nopietnu draudu visām pasaules datorsistēmām.

Piemērs. 2004.gada 26. janvārī datorspeciālisti atklāja, ka internetā izplatīta jauna kaitīga programma Mydoom. Pirmajās 36 stundās tā izsūtīja pa visu pasauli 100 miljonus inficētu vēstuļu un tas aizņēma apmēram vienu ceturto daļu no visu pasaules e- pasta sūtījumu skaita. Iepriekšējais rekords bija vīruss Sobig, kas sūtīja katru 17. vēstuli un inficēja 500 000 datoru.[569]

Vienīgi Makintoša tipa datorsistēmām līdz šim bijusi iespēja izvairīties no nopietniem apdraudējumiem, kaut gan pēdējā laikā arī šo sistēmu traucēšanai ir izstrādātas speciālas ierīces. Vīrusu mutācija, straujā IT attīstība un šo ierīču daudzfunkcionālais raksturs Kibernoziegumu konvencijas izstrādes gaitā bija cēlonis, kādēļ eksperti atteicās no idejas saistīt Konvencijas 6. pantu tikai ar datorvīrusiem. Ekspertu viedoklis bija, ka visas pasaulē līdz šim izmantotās kaitīgās programmas un speciāli veidotās ierīces ir jāapvieno ar *sui generis* kopīgu vārdu „ierīces". Ar ierīci saprot jebkuru datorprogrammu vai rīku, kas izgatavota ar mērķi ietekmēt sistēmas resursu darbību. Līdz ar to par nozieguma rīku atzīstama jebkura ierīce, kas var ietekmēt automatizētās datu apstrādes sistēmu resursus.

*Objektīvā puse*

Salīdzinājumā ar Krimināllikuma 244. panta redakciju (līdz 1.06.2005), pašreizējā panta saturā ir veiktas divas būtiskas izmaiņas: 1) ir ievērojami paplašināts to ierīču loks, par kuru izgatavošanu, glabāšanu, izplatīšanu un citādākās pieejamības nodrošināšanu var piemērot Krimināllikuma 244. pantā paredzēto sodu. To attiecina uz jebkuru ierīci (datorprogrammu vai līdzekli), kas tiek izgatavots un izmantots nolūkā veikt kādu no krimināllikumā paredzētajiem noziedzīgiem nodarījumiem. Taču panta redakcijā apzināti nav ietverts neviens ierīces, ne programmas nosaukums, tādejādi neierobežojot to skaitu;

2) atbildības pamats ir nevis jebkuras ierīces, kas var nodarīt kaitējumu sistēmas resursiem, izgatavošana, izplatīšana, izmantošana vai padarīšana par pieejamu citādā veidā, bet tikai tādi gadījumi, kad iepriekšminētās darbības veiktas ar nolūku izdarīt kaitējumu citai personai piederošai ADAS. Līdz ar to vienlaicīgi tiek

---

[569] Risk management solutions: Response to Cyber Threats and cyberterrorism.// http://www.insurancejournal.com/magazines/west/2004/02/23/features/37008.htm (aplūkots 2004.gada 22. martā).

nostiprināta arī tiesiskā garantija, ka krimināltatbildība netiek piemērota personām, kas pārbauda informācijas sistēmu drošību vai veic citu likumīgu darbību, izmantojot šādas ierīces.

Izstrādājot Kibernoziegumu konvencijas 6. pantu „ierīču ļaunrātīga izmantošana", eksperti triju gadu laikā vairākkārt mainīja tā saturu. Sākotnēji bija paredzēts atbildību noteikt par kaitīgu līdzekļu, kas nodrošina nelikumīgu piekļuvi informācijas sistēmām, nelikumīgu izgatavošanu, izplatīšanu, ieskaitot arī tādus rīkus kā hakeru izmantotus instrumentus, vīrusus, paroļu un pieejas kodu ļaunprātīgu izmantošanu, norādot, ka šāda rakstura darbības apdraud sistēmā esošo datu integritāti un konfidencialitāti.[570] Piemēram, Konvencijas projektā Nr. 21 6. pants paredzēja kriminalizēt tīšas nelikumīgas darbības, kas saistītas ar ierīču, to skaitā datorprogrammu, kas veidotas vai speciāli pielāgotas ar mērķi veikt Konvencijas 2-5 pantā paredzētos noziegumus. Par šādām ierīcēm atzina paroles, pieejas kodus vai līdzīga rakstura datus, ar kuru palīdzību iespējams piekļūt datorsistēmai.[571] Komiteja saņēma ļoti daudz kritisku piezīmju tieši par 6. panta redakciju. Viens no būtiskākiem iebildumiem bija tāds, ka eksperti nebija pietiekami skaidri pateikuši, ka nevar sodīt par šādu ierīču izmantošanu derīga sociāla mērķa sasniegšanai. M. Kenedijs (*M. Kennedy*) rakstīja, ka Konvencijas autori ir uzrakstījuši šo normu prezumējot, ka jebkura persona, kas glabās šādu ierīci, to darīs nolūkā veikt kibernoziegumus.[572]

Turcijas IPS kompānijas *Super-online* padomnieks Akdenizs rakstīja, ka arī nelikumīga ierīce var tikt izmantota likumīgiem mērķiem. Viņš norādīja vairākus piemērus, kad, lai pārbaudītu sistēmas drošības stāvokli, tika speciāli izveidota programma, kuras mērķis, atklājot IS vājās vietas, piekļūt tai un diagnosticēt tās drošības stāvokli. Viņš norādīja: Konvencijā nepārprotami jāparedz, ka atbildība var iestāties tikai tad, ja nelikumīgā ierīce tiek izmantota Konvencijas 2. - 5. pantā minēto noziegumu izdarīšanai, lai nevienam nerastos šaubas, ka atbildība var iestāties par likumīgu šādu programmu lietošanu. Akdenizs uzskata, ka, nosakot atbildību par šādas ierīces izgatavošanu, var ievērojami apgrūtināt darbu pie jaunu IS drošības instrumentu radīšanas, gan pie konkrēto problēmu zinātniskās izpētes.[573]

---

[570] Substantive criminal law. Contribution by Mr. M. Möhrenschlager. Committee of Experts on crime in Cyberspace. PC-CY (97) 50 , p. 8.

[571] Draft Convention on Cyber- crime. PC-CY (2000) draft Nr. 21., p. 5.

[572] In search of balance between police power and privacy in the Cybercrime treaty. by D.C. Kennedy // The Richmond Journal of law and technology Vol. IX. Issue 1., fall 2002, p. 14

[573] Commments received to draft Convention on Cyber- crime from 13.November 2000 to 6. December 2000. Misc.3 Pc-CY Plen 10 ,10. December 2000,p. 22.

Jāatzīst, ka Akdenica kunga bažas ir pamatotas. Šādi komentāri un kritika EP tika saņemta no vairākām ietekmīgām starptautiskām organizācijām. Tāpēc eksperti būtiski mainīja šī panta saturu, un beidzot Konvencijā[574] 6. pants „Ierīču ļaunprātīga izmantošana" (*Misuse of devices*) tika izteikts šādā redakcijā:

1. Dalībvalstīm ir jāveic tādi juridiski un citi pasākumi, kas nepieciešami, lai nacionālo valstu likumos paredzētu krimināltiesību par **šādām tīšām un nelikumīgām darbībām**:
(a) izgatavošana, pārdošana, sagādāšana lietošanai (procurement for use), izplatīšana vai par citādu pieejamības radīšanu:
1) ierīces, tajā skaitā datorprogrammas, kas domātas vai pielāgotas galvenokārt ar mērķi izdarīt vienu no noziegumiem, kas paredzēti Konvencijas 2.- 5. pantā (nelikumīgu piekļūšanu, nelikumīgu noklausīšanos/pārtveršanu, datu traucēšanu, sistēmas traucēšanu);
2) datora paroles, pieejas kodus vai līdzīgus datus, ar kuriem ir iespējams piekļūt datorsistēmai pilnībā vai tās daļai ar mērķi, ka tie ir izmantojami, lai izdarītu 2 .-5. pantā paredzētos noziegumus.
(b); (a) punkta 1. vai 2.p. paredzēto ierīču glabāšana ar mērķi tās izmantot, lai izdarītu 2. - 5. pantā paredzētos noziegumus. Dalībvalstis krimināltiesību par glabāšanu var noteikt, ja glabāšanā atrodas vairākas šādas ierīces.
2. Šis pants neparedz krimināltiesību par darbībām, ja 1.punktā paredzētās produkcijas pārdošana, sagādāšana, imports, izplatīšana vai pieejamības radīšana citādā veidā nav paredzēta Konvencijas 2. - 5. pantā, bet tiek izmantota datorsistēmu aizsardzības pārbaudei.
3. Dalībvalstis var rezervēt tiesības nepiemērot krimināltiesību par 1.punktā paredzētām darbībām ar nosacījumu, ja tas neskar 1.(a) (2) apakšpunktā minēto elementu tirdzniecību, izplatīšanu vai citāda veida pieejamības nodrošināšanu.

Eksperti, Konvencijas 6. pantā redakciju, izvirzīja sekojošus nosacījumus, saskaņā ar kuriem var iestāties krimināltiesību par ļaunprātīgu ierīču lietošanu:

1. *Atbildība par izgatavošanu* (*production*). Izgatavošana ir darbības veids, kā gala rezultātā rodas datu, komandu vai tehnisku ierīču objektīvs kopums, kas paredzēts datorsistēmas vai datortīklu resursu ietekmēšanai ar mērķi izdarīt Konvencijas 2. - 5. pantā paredzētos noziedzīgos nodarījumus (patvaļīgu piekļūšanu, nelikumīgu pieslēgšanos, datu vai sistēmas darbības traucējumus). Par izgatavošanu atzīst arī programmatūras vai ierīces pielāgošanu tādiem mērķiem. ASV jau kopš 1983. gada par noziegumu atzīst kaitīgo programmu izgatavošanu, tā, par šādu nodarījumu tika notiesāts Moriss T. [575]. Interesanti ir tas, ka Moriss T. bija gatavs palaist arī internetā programmu, kas padara nekaitīgu šī tārpa darbību, taču, kā norāda D. Kenedijs[576], tad tādā gadījumā viņš būtu nodarījis vēl lielākus zaudējumus un varbūt atbildības pakāpe viņam būtu vēl smagāka. Morisa T. vaina

---

574 Convention on Cyber- crime // www.coe.int (aplūkots 2004.gada 23. martā).

575 US v Moriss. [575]

576 In search of balance between police power and privacy in the Cybercrime treaty. by D.C. Kennedy . The Richmond Journal of law and technology. Vol. IX. Issue 1., fall 2002, p. 14

bija tā, ka viņš izgatavoto ierīci bija izgatavojis ne tikai savas sistēmas drošības pārbaudei, tāpēc tāds risks nebija attaisnojams.

2. *Atbildība par izplatīšanu* (pavairošana, tirdzniecība, eksports, imports) - jebkuras darbības, kas saistītas ar kaitīgo ierīču realizēšanu. Krievijas Federācijas Elektronisko programmu un datu bāzu aizsardzības likuma 1. pantā termins „izplatīšana" ir definēts kā "datorprogrammas pieejamības radīšana jebkurā materiālā veidā, tai skaitā, ar tīklu vai jebkurā citā veidā, kā arī pārdodot, iznomājot, aizdodot, importējot."[577]

Piemērs. Kāds Vladivostokas vidusskolēns izplatīja kādā no reģionālām interneta mājas lapām informāciju, ka viņš piedāvā iegādāties kompaktdiskus ar datorvīrusu un hakeru darbībai nepieciešamo programmatūru. Cena par šādu kompaktdisku bija 100 rubļi jeb 3 dolāri. 2004. gada 27. janvārī jaunietis pārdeva disku pirmajam pircējam, kurš bija speciāli izveidotās datornoziegumu apkarošanas grupas darbinieks. Kompaktdiskā atradās 320 programmas, to skaitā vīrusi, programmatūra paroļu uzlaušanai un cita programmatūra, kas paredzēta datorsistēmu darbības traucēšanai. 2004. gada 6. februārī jaunietis milicijas darbiniekam pārdeva vēl trīs diskus un tika aizturēts, un viņam izvirzīta apsūdzība pēc Krievijas KK 273. panta.[578]

Šis ir tipisks kaitīgo programmu izplatīšanas piemērs. Izmeklēšanā jaunietis atzina, ka visas CD esošās programmas viņš ielādējis no interneta un kompaktdiskā arī glabājis tās hipersaites, kas nodrošina piekļuvi šādiem hakeru instrumentiem. Izplatīšana ir arī ierīces, kas speciāli radītas vai pielāgotas 2. - 5. pantā paredzēto noziegumu izdarīšanai, sagādāšana lietošanai (*procurement for use*), un EM norādīts, ka izplatīšana ir aktīva darbība, nosūtot konkrēto ierīci citiem lietotājiem.[579] Izplatīšana var būt arī tad, ja persona ievada kaitīgo programmu publiskā datu pārraides tīklā, piem., internetā, nevēršot to uz konkrētu mērķi, jo ierīce pati veic savu destruktīvo darbību atbilstoši iekodētajam uzdevumam.

Piemērs. 2002. gadā pasaulē tika izplatīts vīruss ar nosaukumu "*homepage*", kurš atver lietotājam pieeju uz x - atzīmētām mājas lapām, kas satur pornogrāfiju. Vīruss tiek ievadīts datorā ar e - pasta pielikumu caur *Microsoft Outlook Express* pasta saņemšanas programmu, izmantojot *Outlook Express* adresu grāmatiņu, šis datorvīruss radīja nopietnus darbības traucējumus 7000 Zviedrijas tiesu administrācijas tīklam pievienotajiem datoriem.[580]

Par izplatīšanu ir atzīstams arī gadījums, kad kaitīgo programmu nosūta konkrētai personai, lai nelikumīgi ietekmētu tās sistēmas resursus.

---

[577] Панфилова Е. И., Попов Ф. Н. Компютерные преступления Санкт- Петербург, 1998., с. 31.

[578] How much do computer virus cost? By D. Kramarenko. http://www.crime-research.org/news/09.03.2004/124 (aplūkots 2004.gada 10. martā).

[579] Sk.Draft RM EXPC-CY (2001) 1 rev, 16 p.

[580] Sk.Porn virus affects Swedish court's e- mail system http://www.anova.com/news/story/sm_288908.html?menu (aplūkots 2001.gada 10. martā).

**Piemērs**. Beļģijas tiesa kādu 25 gadus vecu vīrieti sodīja ar naudas sodu 1500Ls par to, ka viņš, tīši atriebjoties kādai sievietei par interneta "tērzēšanas istabā" izteikto atraidījumu, nosūtīja tās datoram vīrusu, kas sabojāja šīs sievietes datorsistēmas informācijas resursus.[581]

3. Pieejamības nodrošināšana citā veidā (*otherwise making available*) nozīmē ievietot konkrēto ierīci *on - line* resursā, lai to varētu izmantot citi lietotāji. Par pieejamības nodrošināšanu Konvencijas izpratnē ir atzīstama arī hipersaišu izveidošana vai kompilācija, kas piedāvā iespēju izmantot šādas ierīces.[582]

Saskaņā ar Civillikuma 1968. pantu glabājuma līgumu var noslēgt par kustamu lietu, līdz ar to nekur juridiski nav analizēts jautājums, ko uzskatīt par glabāšanu datorsistēmā. Varētu pieņemt, ka atbilstoši tam, ka datorsistēmas resursi ir kustama manta, tad arī informācija, kas tiek glabāta kopā ar sistēmu ir pielīdzināma kustamai mantai. Daudz neskaidrāks jautājums ir par hipersaites glabāšanu. Kā zināms, hipersaite ir simbolu rinda, kas labvēlīgos apstākļos dod iespēju piekļūt *on - line* izvietotiem informācijas resursiem. Hipersaites mēs varam atrast interneta meklētājos, piemēram, *Alta Vista, Yahoo, Lycos, Google* u. c. Ja persona speciāli ievietojusi saites, kas dod pieeju iepriekš minētajām ierīcēm (datorprogrammām, kodiem u.c.), tad viņai ir konkrēti nolūki, proti, padarīt šādu informāciju citiem pieejamu. Vladivostokas skolēns savāca visu nepieciešamo informāciju, kas nodrošina pieeju kaitīgām programmām internetā, un glabāja šo informāciju kompaktdiskā. Tādā veidā viņš ikvienai personai, kas iegādājas šo disku, deva iespēju piekļūt šiem resursiem. Dotajā piemērā hipersaites glabātājs apzinās, kāda rakstura informāciju viņš piedāvā, līdz ar to viņu var saukt pie atbildības par šādas ierīces piedāvājumu. EM ir īpaši uzsvērts, ka atbildība šajā gadījumā ir jāsaista ar nodomu izmantot šīs ierīces Konvencijas 2. - 5. pantā paredzēto noziegumu izdarīšanai. Izveidojot šo noziedzīgā nodarījuma sastāvu ar attiecīgo pazīmi, nepieciešams noteikt nosacījumu, piemēram, ka glabāšana būtu sodāma tad, ja personas ADAS atrastos, piemēram, 3 hipersaites.

Autors uzskata, ka atbildība jāparedz par tīšu šāda informācijas avota izmantošanu, ja ir iegūti nepārprotami pierādījumi, ka kāda no šīm hipersaitēm atver pieeju informācijas avotam, kas atklāti piedāvā iespēju izmantot Konvencijas

---

581 Chatroom reject fined for sending virus to woman Annova http://www.ananova.com/news/story/sm_308078.html?menu (aplūkots 2004.gada 10. martā).

582 Cybercrime Convention Explanatory report. CM (2001) 144.addendum, para 71-78

6. panta 1. p. aprakstītās ierīces ar mērķi ietekmēt datorsistēmu resursus, un persona caur šo hipersaiti ir piekļuvusi šiem informācijas resursiem un ievadījusi atbilstīgo informāciju savā datorsistēmā. Tad personas darbībās būs saskatāmas Konvencijas 6. p. paredzētā nozieguma –nelikumīgās ierīces pieejamības nodrošināšanas (*procurement)* pazīmes.

Jautājums par hipersaites glabāšanu kā iespējamo krimināatbildības pamatu ir apskatīts arī citos topošās Konvencijas pantos. Eksperti 6. pantā iekļāva principu, ka dalībvalstis, ratificējot Konvenciju, var piemērot izņēmumus, proti, noteikt atbildību par vairāku hipersaišu, kodu un citu nelikumīgo ierīču glabāšanu. Autors uzskata, ka Latvijai šīs tiesības būtu jāizmanto. Krimināllikuma grozījumos ir jāparedz tādi nosacījumi, kas atbilst iepriekšminēto starptautisko normatīvo aktu prasībām un tai pat laikā dod arī garantijas, ka pie atbildības par pieejamības nodrošināšanu citā veidā netiks sauktas personas par formāliem pārkāpumiem.

Tāpēc, izstrādājot Krimināllikuma 244. panta jauno redakciju tika ievēroti šādi principi:

1. Aizliegtā darbība formulēta neatkarīgi no ierīču, kas speciāli var tikt piemērotas datu un sistēmu traucēšanai, izgatavošanas metodes un tehnoloģijas.

2. Atbildība paredzēta tikai par speciāli izgatavotu vai pielāgotu ierīces izgatavošanu, izplatīšanu, pavairošanu vai citā veidā padarītu pieejamu, ja tās mērķis ir ietekmēt sistēmas datu drošību. Ja šāda ierīce izgatavota un glabāta ar mērķi veikt darbību, kas saistīta ar sociāli derīga mērķa sasniegšanu, tad šādas ierīces nevar tikt uzskatītas par minētā panta aizlieguma priekšmetu.

3. Krimināli sodāma ir šādu ierīču izmantošana nolūkā veikt jebkuru Krimināllikumā paredzētu noziedzīgu nodarījumu. Kaut gan Kibernoziegumu konvencija attiecina šo aizliegumu tikai uz Konvencijā ietvertiem noziedzīgiem nodarījumiem pret informācijas sistēmu drošību, tas ir Krimināllikuma 144., 241., 243., 244. pants. Prakse pierāda, ka šādas kaitīgas ierīces izmanto, veicot krāpšanu, terorismu, izspiešanu, goda un cieņas aizskaršanu, autortiesību un blakustiesību pārkāpšanu, bērnu pornogrāfijas izplatīšanu u.c. noziedzīgas darbības. Tāpēc nav jēgas pantā norādīt, ka sodāmas ir tikai tādas kaitīgas ierīces izmantošana, ja tā ir saistīta ar noziedzīgiem nodarījumiem pret informācijas sistēmu drošību. Šāda

pieeja nav arī pretrunā ar Konvencijas prasībām, jo šis dokuments izvirza minimālās prasības, kas dalībvalstīm jāievēro, bet neaizliedz paplašināt vai noteikt citas prasības un aizliegumus šo nodarījumu kriminalizācijas procesā.

Sekas. Krimināllikuma 244. panta 1. daļa ir formāls noziedzīgs nodarījums, kur seku iestāšanas moments sakrīt ar aizliegto darbību, jo kā pamatoti norāda Čirilo, tad izplatot vīrusu, uzbrucējs nekad negaida uzbrukuma beigas.[583] Savukārt minētā panta 2. daļa satur nosacījumu, ka atbildība iestājas tikai tad, ja iestājušās smagas sekas, kas saistītas gan ar lielu mantisko zaudējumu nodarīšanu vai iestājusies cilvēka nāve vai citāds smags kaitējums ar likumu aizsargātām interesēm un tiesībām, līdz ar to tas ir materiāls noziedzīgs nodarījums. Obligāts priekšnoteikums ir tas, lai būtiskais kaitējums būtu tiešā cēloniskā sakarā ar vainīgās personas darbību –kaitējumu radošu programmu apzinātu aprites organizēšanu vai veikšanu. Izmeklējot šāda rakstura krimināllietas, procesa virzītājam ir pienākums noteikt cēlonisko sakarību, ka tieši no tās programmas vai programmatiskā līdzekļa, ko sistēmā, datorā vai ir internetā ievadījusi vainīgā persona, ir radušās likumā paredzētās sekas.

### 6.5. Informācijas sistēmu drošības noteikumu pārkāpšana. KL 245. pants

*Nodarījuma tiesiskais pamats*

Profesore V. Liholaja uzskata, ka ar šo noziedzīgo nodarījumu ir apdraudētas informācijas sistēmu drošības intereses.[584] Vispirms, lai noteiktu, vai ir pārkāptas kādas intereses, ir nepieciešams noteikt to tiesisko pamatu, uz kura pamata šāds krimināltiesisks regulējums noteikts. Nenoliedzami, ja runā par noteikumu pārkāpšanu, tad jāatsaucas uz konkrētiem noteikumiem, kuri ir vispārobligāti visām personām, uz kurām tie attiecas.

2002. gada 2. maijā tika pieņemts Valsts informācijas sistēmu likums, kas stājās spēkā ar 2002. gada 5. jūniju. Minētā likuma Pārejas noteikumu 3.4. punkts noteic:

*"Līdz attiecīgo Ministru kabineta noteikumu spēkā stāšanās dienai, bet ne ilgāk kā sešus mēnešus no šā likuma spēkā stāšanās dienas, ir spēkā šādi Ministru*

---

583 Chirillo John Hack attacks encyclopedia. A complete history of hacks, cracks, phreaks and spies over time. New-York-Willy Computer Publishing. John Willey & Sons Inc., 2001., p.300

584 Krastiņš U., Liholaja V., Niedre A. Krimināllikuma Zinātniski- praktiskais komentārs. (3) Sevišķā daļa. U. Krastiņa redakcijā. Rīga: AFS", Rīga, 2003, 232.lpp.

*kabineta noteikumi, ciktāl tie nav pretrunā ar šo likumu 3.p. 2000. gada 21. marta noteikumi nr. 106 "Informācijas sistēmu drošības noteikumi".*

*Šo noteikumu 4.p. noteic: Ministru kabinets sešu mēnešu laikā no šā likuma spēkā stāšanās dienas izdod šā likuma 4. panta otrajā daļā minētos noteikumus par: valsts informācijas sistēmu tehnisko prasību ievērošanu; 3) valsts informācijas sistēmu drošības prasībām.*

Tādējādi kopš 2002. gada 1. novembra Noteikumi Nr. 106 „Informācijas sistēmu drošības noteikumi" nav spēkā. Tika izstrādāti un iesniegti MK divi noteikumu projekti: 1) MK noteikumi „Personas datu apstrādes sistēmu aizsardzības obligātās tehniskās un organizatoriskās prasības"; un 2) "Valsts informācijas sistēmu drošības noteikumi".

Autors un darba grupas locekle Latvijas Bankas informācijas sistēmu drošības vadītāja I. Murāne vērsās ar vēstuli valdībā, kur norādīja uz nepieļaujamām tendencēm, izstrādājot MK Noteikumus „Personas datu apstrādes sistēmu obligātās un tehniskās organizatoriskās prasības", jo noteikumu izstrādātāji pretēji starptautiskai datu aizsardzības praksei bija paredzējuši būtisku valsts tiesību iejaukties jebkuras fiziskas personu datu apstrādes sistēmas darbībā. Ar 2003. gada 22. maija Ministru Prezidenta rīkojumu Nr. 234 tika izveidota darba grupa „Par Ministru kabineta noteikumu projektu par personas datu apstrādes sistēmu aizsardzības obligātajām tehniskajām un organizatoriskajām prasībām, par valsts informācijas sistēmu drošību, par valsts informācijas sistēmu tehnisko prasību ievērošanu un par valsts informācijas sistēmu reģistrāciju saskaņošanu". Darba grupa vienojās nevirzīt saskaņošanai Ministru kabineta noteikumu „Personas datu apstrādes sistēmu aizsardzības obligātās tehniskās un organizatoriskās prasības" projektu, un Datu valsts inspekcija to atsauca. Tāpēc šobrīd vienīgais sagatavotais noteikumu projekts ir Valsts informācijas sistēmu drošības noteikumi. Tas attieksies tikai uz tām informācijas sistēmām, kas izpildīs nepieciešamās organizatoriskās un tehniskās prasības un tiks iekļautas valsts informācijas sistēmu reģistrā. Patlaban nav precīzi zināms, cik sistēmu šie noteikumi aptvers, bet galvenokārt likuma un noteikumu mērķis ir regulēt to sistēmu, kas apstrādā valstij kritisko informāciju, organizatorisko vadību, risku pārvaldību, krīzes vadību un citus organizatoriskus kritērijus, respektīvi, šīm sistēmam ir jāaptver A un B grupas

sistēmas. A. grupas sistēmu sarakstu apstiprina MK, un šī informācija ir slepena. Tas ir pilnīgi saprotami, jo pie valsts informācijas sistēmām pieder visi centrālie reģistri, aizsardzības iestāžu, policijas, prokuratūras, banku un citu valsts pastāvēšanai vitāli svarīgu sferu iestāžu informācijas sistēmas. Visas šīs sistēmas pieder valsts vai pašvaldību iestādēm un institūcijām, un to pārziņi ir arī juridiskas personas. Tāpēc nenoliedzami, visi šo sistēmu administratori tiks atzīti par amatpersonām saskaņā ar Krimināllikuma 316. pantu, jo viņi pastāvīgi vai uz laiku pildīs valsts vai pašvaldību dienesta pienākumus un to darbība būs saistīta ar iespēju rīkoties ar valsts vai pašvaldību mantu, tas ir, automatizēto datu apstrādes sistēmu resursiem. Patlaban, līdz 2005. gada 15. septembrim, noteikumi nav pieņemti, bet atrodas pēdējā sagatavošanas stadijā.

Šobrīd Latvijā nav tādu informācijas sistēmu drošības noteikumu, kādi bija paredzēti MK Noteikumos Nr. 106. Tāpēc autors uzskata, ka Krimināllikuma 245. pants nav piemērojams. Atteikšanās no vispārobligātiem noteikumiem bija absolūti pašsaprotama, jo, kā uzskata speciālisti, tad neatkarīgi no tā, cik stingri ir informācijas drošības noteikumi, apdraudējuma iespēja pastāv vienmēr. Teorētiski, protams, var saglabāt minētā panta sastāvu, attiecinot to tikai uz valsts informācijas sistēmām.

Persona, kas atrodas valsts vai pašvaldību institūciju dienestā un atbild par informācijas sistēmu drošību, ir amatpersona. Gadījumā, ja tā nolaidīgi pilda savus pienākumus vai pārkāpj savas pilnvaras un nodara būtisku kaitējumu, to var saukt pie atbildības pēc Krimināllikuma 317., 318., 319 panta, atkarībā no nodarījuma rakstura. Ja Krimināllikuma 245. pantā paredzētais nodarījums ir kriminālpārkāpums, tad XXIV sadaļā iekļautie iepriekšminētie nodarījumi paredz daudz smagākas sankcijas. Šādos apstākļos autors uzskata, ka KL 245. pantu ieteicams no Krimināllikuma izslēgt.

## Anotācija

*Promocijas darbā ir veikta noziedzīgu nodarījumu pret informācijas sistēmu* drošību (KL 241- 245. pants) (kibernoziegumu) teorētisko problēmu izpēte. Disertācijā ir pētīti šādas vispārīgas krimināltiesību teorijas pamatnostādnes: 1) noziedzīga nodarījuma jēdziens, tā attīstība, un dota kibernozieguma definīcija. Disertācijā dots pamatojums, kāpēc nepieciešams kibernoziegumiem veltīt īpašu pētījumu, jo tas saistīts ar ir vispārējo tendenci uz tiesību un tehnoloģiju konverģences attīstību dažādās tiesību jomās, to skaitā arī krimināltiesībās; 2) noziedzīga nodarījuma sastāva (*corpus delicti*) elementu analīze. Par noziedzīgo objektu atzīstams personas tiesisko interešu apdraudējums. Disertācijā īpaša uzmanība pievērsta teorijai par nozieguma objektu vertikālo klasifikāciju, atzīstot, ka pašreiz Krimināllikuma XX nodaļā paredzētais grupas objekts – vispārējā drošība - ir atzīstams par vispārīgo objektu, bet par šo nodarījumu grupas objektu ir atzīstama informācijas sistēmu drošība (ISD), kas disertācijā aplūkota kā savrupa apakšsistēma, kas sastāv no savstarpēji integrētiem elementiem (integritātes, pieejamības un konfidencialitātes). Izteikts priekšlikums izdarīt grozījumus Krimināllikumā un noziedzīgos nodarījumus pret informācijas sistēmu drošību iekļaut atsevišķā nodaļā ar nosaukumu „Noziedzīgi nodarījumi pret automatizētas datu apstrādes sistēmu drošību". Par minētās grupas tiešo apdraudējuma objektu atzīstama kāda no informācijas sistēmu drošības pazīmēm, piemēram, 241. pantā pieejamība, 242. pantā konfidencialitāte, 243. pantā integritāte, 244. pantā un 245. pantā tiešais apdraudējuma objekts ir visu ISD elementu kopums. No objektīvās puses noziedzīgos nodarījumus pret ISD var izdarīt tikai ar darbību. Disertācijā dota plaša to darbību analīze, kas var tikt izmantoti kibernoziegumu veikšanai, īpaši liela uzmanība pievērsta jēdziena „patvaļīga piekļuve" juridiskai analīzei, to raksturojošām pazīmēm un izdarīts secinājums, ka darbību var atzīt par patvaļīgu piekļuvi tikai tad, ja sistēmas īpašnieks vai tiesiskais valdītājs ir noteicis kārtību, kā likumīgie lietotāji var piekļūt un izmantot sistēmas resursus. Ja šāda kārtība sistēmā nav noteikta, tad nav arī patvaļīgas piekļuves sastāva. Pētāmā noziedzīgo nodarījumu grupa, izņemot KL 244. panta 1.dalu, ir pieskaitāma pie materiāliem noziedzīgiem nodarījumiem, kur sekas ir obligāts atbildības priekšnosacījums,

tāpēc disertācijā analizēts jēdziens „būtisks kaitējums" un izteikts viedoklis, ka, lai izvērtētu būtiska kaitējuma materiālo saturu saistībā ar kibernoziegumiem, ieteicams veikt labojumus Likumā „Par Krimināllikuma spēkā stāšanās laiku un kārtību" 23. pantā, izstrādājot speciālu pielikumu būtiskā kaitējuma apmēra noteikšanai saistībā ar kibernoziegumiem. No subjektīvās puses šos nodarījumus var izdarīt tikai ar tīšu darbību, kas ietver sevī gan *dolus directus*, gan arī *dolus eventualis*. Disertācijā ir analizēts KL 245. panta sastāvs un izteikts viedoklis, ka šo pantu lietderīgi no Krimināllikuma izslēgt, jo tā saglabāšanai nav ne juridiskas, ne praktiskas nozīmes. Disertācijai nav tikai teorētiska, bet arī praktiska nozīme, jo, pamatojoties uz teorētiskās izpētes rezultātiem, ir izteikti vairāki praktiski ierosinājumi. Nolūkā saskaņot Krimināllikuma normas atbilstoši Eiropas Padomes Kibernoziegumu Konvencijas un ES Padomes ietvarlēmuma par uzbrukumiem informācijas autors izstrādāja likumprojektu „Par grozījumiem Krimināllikumā", kur ievērojami uzlabota spēkā esošā KL 241. panta redakcija, ierosināts izslēgt 242. pantu, izstrādāta pilnīgi jauna 243. panta „datu un sistēmu darbības traucēšana" redakcija, kurā pēc būtības ietverti divi noziedzīgu nodarījumu sastāvi - sistēmā esošo datu traucēšana un sistēmas resursu darbības traucēšana, izmantojot pakalpojumatteices uzbrukumus. 2005.gada 28. aprīlī Saeima šos grozījumus pieņēma. Promocijas darba nobeigumā pievienots aizstāvēšanai izvirzīto tēžu saraksts.

**Resume**

This Doctoral Paper provides a study of the theoretical problems related to crimes against security of information systems (Articles 241 – 245 of the Criminal Law) (cybercrimes). The following general basic approaches of the theory of criminal law are analysed in the Thesis: 1) the concept of crime, its development and also the definition of cybercrime are presented. The Thesis justifies the need to devote a special study to cybercrimes as this is related to the general tendency towards development of convergence of law and technologies in different fields of law, including criminal law; 2) analysis of the elements of *corpus delicti*. Threat to the legal interests of a person should be recognised as the criminal object. In the Thesis special attention focuses on the theory of vertical classification of objects of crime, recognising that the group object as at present provided for in Section XX of the Criminal Law – general security - should be declared as a general object and the security of information systems should be declared the group object of these crimes. The thesis views it as a separate sub-system consisting of mutually integrated elements (integrity, availability, and confidentiality). A proposal is expressed to amend the Criminal Law and to include crimes against the security of information systems in a separate section under the heading "Crimes against the security of automated data processing systems". The direct object of threat in the referred groups - for example, accessibility in Article 241, confidentiality in Article 242, integrity in Article 243, direct object of threat in Articles 244 and 245 - is the totality of all the security elements of an information system. On the objective side, crimes against the security of information systems can be committed only by action. The Thesis presents an extensive analysis of acts that may be used for committing cybercrimes, with special attention focused on legal analysis of the concept "arbitrary access" and its characterising features. The conclusion is drawn that an act may be declared arbitrary access only of the owner or legal possessor of the system has stipulated the procedure according to which rightful users can access and use the system resources. If there is no such procedure established in the system, then there is no *corpus delicti* of arbitrary access. The group of the crimes analysed, except Part 1 of Article 244 of Criminal Law, should refer to material

crimes the consequence of which is a mandatory precondition of liability; therefore the concept of material damage is analysed in the Thesis and the opinion is expressed that for the purpose of assessing the contents of material damage in relation to cybercrimes it is recommendable to amend Article 23 of the Law "On the procedure for entering into force of the Criminal Law" by elaborating a special appendix to determine the extent of material damage in relation to cybercrimes. On the subjective side, these crimes can be committed only by means of intentional acts comprising both *dolus directus* and *dolus eventualis*. The content of Article 245 of the Criminal Law is analysed in the Thesis and the view is expressed that it is necessary to exclude this Article from the Criminal Law because maintaining it achieves no legal or practical effect. The thesis is not only of theoretical, but also practical importance because based upon the results of the theoretical research several practical proposals have been already incorporated in text of to the Criminal Law for the purpose of harmonising the norms of the Criminal Law with the requirements of the Council of Europe Convention on Cybercrimes and the EU Council Framework Decision on attacks against information systems, considerably improving the wording of Article 241- 245 of the currently valid Criminal Law. The list of theses proposed for defending is attached at the end of the Doctoral Paper.

**Aizstāvībai izvirzītās tēzes**

Disertācijā pētītā tēma dod iespēju izvirzīt aizstāvībai šādas tēzes:

1. Kibernoziegumu jēdziens- jebkura nelikumīga, krimināli sodāma darbība, kurā automatizētās datu apstrādes sistēmas (datori, skeneri, drukas iekārtas, datorprogrammas un komunikācijas līdzekļi, elektroniskie tīkli u.c.) izmantotas kā noziedzīgā nodarījuma priekšmets vai noziedzīgā nodarījuma rīks ar mērķi ietekmēt automatizēto datu apstrādes sistēmu tehniskos vai informācijas resursus vai arī kā medijs nelikumīgas informācijas aprites procesā.

2. Formulējot kibernoziegumus pret automatizēto datu apstrādes sistēmu drošību, nepieciešams ievērot tehnoloģiskās neitralitātes principu. Pantu dispozīcijas ir jāformulē tā, lai to piemērošana nebūtu atkarīga no informācijas tehnoloģiju attīstības progresa.

3. Krimināllikuma XX nodaļā „Noziedzīgi nodarījumi pret vispārējo drošību un sabiedrisko kārtību" ietvertais grupas objekts „vispārējā drošība" nevar tikt atzīts par grupas objektu, jo to termins „vispārīgs" norāda, ka saistībā ar šo apzīmējumu drošība var tikt apskatīta tikai kā sistēma, bet tas nozīmē, ka atbilstoši objektu klasifikācijai pa vertikāli tā var tikt atzīta tikai par vispārīgo noziedzīgo nodarījumu objektu, t.i., visu to tiesisko interešu, ko aizsargā Krimināllikums, neatņemama sastāvdaļu.

4. Informācijas sistēmu drošība krimināltiesību izpratnē ir stāvoklis-galarezultāts, kas sasniegts, nodrošinot sistēmas resursu (informācijas un tehnisko) integritāti, pieejamību un konfidencialitāti, lai aizsargātu sistēmu pret citu personu radītajiem apdraudējumiem. Līdz ar to par grupas objektu atzīstams personas tiesisko interešu uz sistēmas resursu (informācijas un tehnisko) integritāti, pieejamību un konfidencialitāti apdraudējums.

5. Pētītā noziedzīgo nodarījumu grupa ir apveltīta ar visām grupas objektam nepieciešamajām vispārīgajām un speciālajām pazīmēm, kas dod pamatu, lai šo nodarījumu grupu izdalītu atsevišķā Krimināllikuma nodaļā ar nosaukumu „Noziedzīgi nodarījumi pret automatizēto datu apstrādes sistēmu drošību".

6. Krimināllikuma 241.- 244. pantā ietvertajiem noziedzīgajiem nodarījumiem pret informācijas sistēmu drošību nav vienādas tiešās apdraudētās intereses, jo katrs no šiem apdraudējumiem ir vērsts pret kādu no sistēmas elementiem. Krimināllikuma 241.pantā ietvertais nodarījums ir vērsts pret personu tiesisko interesi noteikt sistēmas resursu pieejamības kārtību; Krimināllikuma 243. pantā ietvertais nodarījums- pret personu tiesisko interesi uz sistēmas resursu integritāti. Tikai Krimināllikuma 244.panta nodarījumā atzīts, ka tiešā apdraudētā interese ir personas tiesiskā interese uz sistēmas resursu integritāti, pieejamību un konfidencialitāti.

7. Par noziedzīgo nodarījumu apdraudējuma priekšmetu atzīstami automatizētas datu apstrādes sistēmu tehniskie un informācijas resursi, tas ir, jebkuras ierīces vai ierīču grupas, kas savienojumā ar elektronisko pārraides tīklu nodrošina datu apstrādes procesu jebkurā tā stadijā. Tādējādi par noziedzīga nodarījuma priekšmetu atzīstams jebkurš mākslīgi radīts fakts (artifakts), mantiska, nemantiska, taustāma, netaustāma vienība, tai skaitā arī virtuālā realitāte, kurai piemīt divas pazīmes: 1) tai ir jābūt cilvēka radītai vērtībai; 2) tai ir jābūt identificējamai.

8. Noziedzīgi nodarījumi pret informācijas sistēmu drošību (kibernoziegumi) var tikt veikti tikai ar aktīvu darbību. Bezdarbība neveido šo nodarījumu sastāvu.

9. Krimināllikuma 241.- 244. panta dispozīcijā ir izmantoti dažādi tehniski termini, piemēram, „kopēšana", „piekļūšana", „modificēšana" u.c. Disertācijā izdarītais pētījums dod pamatu secinājumam, ka nereti šo terminu tehniskais saturs atšķiras no to juridiskās nozīmes, jo termins kā darbības apzīmējums juridiskā izpratnē izmantojams tikai tad, ja tas rada noteiktas tiesiskas sekas.

10. Noziedzīgā nodarījuma – „patvaļīga piekļūšana datorsistēmai", dispozīcija (241.pants) nesatur tiesiskās apdraudētās intereses materiālā satura raksturojumu. Piekļuve no tehniskā redzes viedokļa ir darbība, kas ietvert sevī divus elementus: 1)identifikāciju; 2) autentifikāciju. Lai personu sauktu pie atbildības par patvaļīgu piekļuvi, ir nepieciešams arī trešais elements, proti, personas, kurai pieder sistēma, subjektīvās gribas izpausme, ka viņa izdarīto piekļuvi atzīst par patvaļīgu.

11. Noziedzīgais nodarījums– „patvaļīga piekļūšana datorsistēmai" ir jānošķir no citiem noziedzīgiem nodarījumiem, piemēram, zādzības, kas saistīta ar iekļūšanu

glabātavā (175.panta 3.daļa), nelikumīgas informācijas resursu pārtveršanas (144. pants), noziedzīgiem nodarījumiem, kas saistīti ar automatizēto datu apstrādes sistēmu izmantošanu ar likumu aizliegtas informācijas apritei, piemēram, bērnu pornogrāfija (166. pants), rasu naida, genocīda un ksenofobiju saturošas informācijas izplatīšanu vai propagandu un publiski pieejamu mājas lapu sabojāšanu (231. pants).

12. Saucot personu pie kriminālatbildības par noziedzīgiem nodarījumiem pret informācijas sistēmu drošību, jāņem vērā arī tādi atbildību izslēdzoši apstākļi, ko neparedz Krimināllikums, bet kas par tādiem saistībā ar noziedzīgiem nodarījumiem pret sistēmu drošību atzīti ar Eiropas Savienības normatīvajiem aktiem, t.sk. lietotāju tiesības lietot savu datu aizsardzībai šifrēšanu, reversās inženierijas izmantošanu pārvaldnieku un kontrolieru darbības sistēmā, gan pilnvarotu sistēmas darbinieku, gan ārpussistēmas pilnvarotu personu speciāli veiktas sistēmu drošības pārbaudes, leģitīmo zinātnisko pētniecību.

13. Kriminālprocesa likuma 7. pantā ir ieteicams izdarīt labojumu, nosakot, ka krimināllietas noziedzīgos nodarījumos pret informācijas sistēmu drošību, izņemot gadījumus, kad apdraudējuma objekts ir valsts informācijas sistēma, ir ierosināmas tikai pēc cietušā sūdzības.

14. Visi KL 241.- 244. pantā ietvertie nodarījumi, izņemot Krimināllikuma 244.panta 1.daļā paredzēto, ir atzīstami par materiāliem noziedzīgu nodarījumu sastāviem, un tāpēc tiem obligāts atbildības nosacījums ir seku iestāšanās. Krimināllikuma 242.- 245. pants kā atbildības nosacījumu paredz būtisku kaitējumu, kas sastāv no sociālā un materiālā elementa.

15. Lai noteiktu sociālā elementa saturu noziedzīgos nodarījumos pret informācijas sistēmu drošību, ierosinu: piemērojot proporcionalitātes principu, Nacionālās drošības koncepcijā iekļaut punktu, kas visas valstī esošās automatizētās datu apstrādes sistēmas grupētu pēc sociālā nozīmīguma un ar to saistītā apdraudējuma riska pakāpes. Šim nolūkam iesaku izmantot sistēmu četru līmeņu klasifikāciju, apzīmējot to ar lielajiem burtiem A – attiecas uz visaugstākā riska apdraudējuma sistēmām, kas apstrādā vai uztur valsts drošībai kritisku informāciju (pamatā darbības saistītas ar valsts noslēpumu saturošu informāciju) ; B – augsta

riska apdraudējuma sistēmām, kas apkalpo centrālo valsts varas aparātu un uztur integrētos reģistrus, bankas, energoresursu apgādi u.c. C- vidēja riska apdraudējuma sistēmas,, kas apkalpo informācijas apgabalus, kas satur lietotājam un citam personām svarīgu informāciju, piemēram, sistēmas, kas sniedz maksas e-pakalpojumus, D- zema riska apdraudējuma sistēmas. Par tādām būtu ieteicams atzīt sistēmas, kas nesniedz maksas pakalpojumus un neveic personai sensitīvu datu apstrādi vai neuztur informāciju, kas nepieciešama valsts vai pašvaldības darbībai.

16. Lai noteiktu seku materiālā elementa saturu, ierosinu zaudējumus aprēķināt pēc šādas metodes: 1) zaudējumi, kas radušies automātiskās datu apstrādes sistēmas dīkstāves dēļ; 2) izdevumi, kas saistīti ar bojātās informācijas atjaunošanu vai aizstāšanu vai jaunu programmatisko resursu uzstādīšanu; 3) izdevumi, kas saistīti ar lietotāju piekļuves tiesību korekciju. No šiem izdevumiem atskaitāmi sistēmas amortizācijas izdevumi.

17. Nosakot materiālā elementa saturu, izņemot gadījumus, kad iestājušās smagas sekas, jāievēro „puvušā koka" princips, proti, gadījumos, kad persona sistēmas uzturēšanai izmanto nelikumīgi iegūtu programmatūru, to nevar atzīt par cietušo krimināltiesību izpratnē.

18. Izmantojot iepriekšminēto iedalījumu, sagatavot grozījumus Likumā „Par Krimināllikuma spēkā stāšanās laiku un kārtību 23. pantā" un izstrādāt speciālu pielikumu būtiskā kaitējuma satura noteikšanai saistībā ar kibernoziegumiem, īpaši pievēršot uzmanību sociālā elementa nozīmei, skaidrojot jēdzienu „un citas ar likumu aizsargātās intereses un tiesības" atbilstoši iepriekš ieteiktajam automatizēto datu apstrādes sistēmu iedalījumam valstī.

19. Noziedzīgos nodarījumos pret informācijas sistēmu drošību subjektīvā puse var izpausties tikai kā tīša darbība, kas ietver sevī gan tiešu (*dolus directus*), gan arī netiešu (*dolus eventualis*) nodomu.

20. Nepieciešams izvērtēt Krimināllikuma 245. panta lietderību divu apstākļu dēļ: 1) valstī nepastāv visām informācijas sistēmām obligāti informācijas sistēmu drošības noteikumi, līdz ar to nav tiesiskā pamata- blanketās normas, par kuras pārkāpšanu var iestāties atbildība; 2) šāda atbildība, izņemot Krievijas Federāciju un citas NVS valstis, pasaulē netiek atbalstīta.

21. Veiktais pētījums dod pamatu secināt, ja persona, kas ir atbildīga par informācijas sistēmu drošību, apzināti nepilda savus pienākumus, kā rezultātā sistēmas īpašniekam tiek nodarīts būtisks kaitējums, tad pret viņu var tikt piemēroti citi atbildības veidi. Savukārt, ja pantā paredzētās sekas nodarītas valsts informācijas sistēmās, tad šādu personu var saukt pie atbildības saskaņā ar Krimināllikuma 319. pantu „Valsts amatpersonas bezdarbība", jo saskaņā ar Krimināllikumu 316. panta 1.daļu jebkurš valsts informācijas sistēmas administrators ir vienlaikus arī valsts amatpersona.

22. Ievērojot straujo informācijas tehnoloģiju progresu, kas dod iespēju automatizēto datu apstrādes procesu izmantot tradicionālo noziedzīgo nodarījumu sagatavošanā un veikšanā, tādējādi pastiprinot šādā veidā izdarīto nodarījumu kaitīgumu, ierosinu papildināt Krimināllikuma 48. panta "Atbildību pastiprinošie apstākļi" 1. daļu ar 14. punktu un izteikt to šādā redakcijā- noziedzīgais nodarījums izdarīts, izmantojot automatizētās datu apstrādes sistēmas.

**Pielikums Nr. 1**

**Projekts grozījumi likumā „Par Krimināllikuma spēkā stāšanās laiku un kārtību"**

Pamatojoties uz 23. panta 3.daļu, papildināt likumu ar pielikumu šādā redakcijā:

Pielikums.

*„Kritēriji, pēc kuriem nosakāms citas ar likumu aizsargātas intereses vai ievērojams apdraudējums, nodarījumos pret automatizēto datu apstrādes sistēmu drošību".*

1. Ar likumu aizsargātās intereses un tiesības automatizēto datu apstrādes sistēmu drošības jomā ir apdraudētas:

1) ja nodarījums vērts pret A vai B grupas informācijas sistēmu.

2) ja nodarījums vērts pret C grupas sistēmu un apdraudējuma rezultātā traucēta sistēmas resursu darbība vairāk par 30 minūtēm;

3) ja nodarījums vērsts pret D grupas sistēmu un apdraudējuma rezultātā traucēta sistēmas resursu darbība ilgāk par vienu stundu.

2. Ievērojamus mantiskos zaudējumus nodarījumos, kas saistīti ar automatizēto datu apstrādes sistēmu, noteic ņemot vērā zemāk minētos izdevumus:

1) zaudējumus, kas saistīti ar automatizētās datu apstrādes sistēmas dīkstāvi;

2) izdevumus, kas saistīti ar bojātās informācijas atjaunošanu vai tās aizstāšanu;

3) izdevumi, kas saistīti ar jaunu programmatisko resursu, kas paredzēti sistēmas drošības atjaunošanai, uzstādīšanu;

4) izdevumi, kas saistīti ar sistēmas lietotāju piekļuves tiesību korekciju.

3. Ja persona izmanto sistēmas uzturēšanai nelicenzētus programmatiskos resursus, tad neatkarīgi no zaudējumu apmēra, izņemot, gadījumus, kad iestājas šī likuma 24. pantā paredzētās sekas, ievērojams mantisks zaudējums šī likuma 23. panta izpratnē, neiestājas.

**Pielikums Nr. 2**

**Projekts: "Par grozījumiem valsts nacionālās drošības koncepcijā"**

Papildināt Koncepcijas 1.2. punktu ar sekojošu rindkopu:

Lai panāktu elektroniskās vides drošību, visas valstī esošās automatizētās datu apstrādes sistēmas iedalāmas atbilstoši apdraudējuma pakāpei četrās grupās: A) sistēmas ar visaugstākā riska apdraudējuma pakāpi, kas nodrošina valsts drošībai svarīgu informācijas apriti, kuru apdraudējuma gadījumā var tik būtiski ietekmēta valsts drošība. Šo sistēmu sarakstu apstiprina Ministru kabinets; B) sistēmas ar augstu riska apdraudējuma pakāpi, kas nodrošina valstij un sabiedrībai svarīgu funkciju izpildi un kas apstrādā sensitīvus personu datusun kas ir reģisttrētas valsts informācijas sistēmu reģistrā; C) sistēmas ar ierobežotu apdraudējuma pakāpi, kas nodrošina informācijas apriti komercdarbības veikšanai; D) sistēmas ar zema riska apdraudējuma pakāpi, kas tiek izmantotas sistēmas īpašnieku vai pilnvaroto personu personīgo vajadzību apmierināšanai.

**Izmantotās literatūras un juridisko aktu saraksts**

Literatūra un monogrāfijas

1. Таганцев Н.С. Курсь Русского уголовного права. Часть общая книга 1-я. Учение о преступлении. Санкт-Перербургь,1874.

2. Таганцев Н.С. Руское уголовное право. Лекции. Часть общая. В.2т.Москва [b.i.],1894.

3. Анализ о преступлении исследование. Исследование П.П.Пусторослева Москва: Университетская типография, 1892.

4. Sodu likums ar komentāriem. Otrais izd. P. Minca un J. Lauva red. Rīga, 1938., Valsts tipogrāfijas izdevums.

5. Docents Lejiņš Pēteris Krimināltiesības- Rīga: [b.i] 1940.

6. Sinaiskis V. Civiltiesības I. –Rīga: A/S "Valters un Rapa",1935.

7. Mincs P. Krimināltiesību kurss. Vispārējā daļa. Otrs pārstrādātais un papildinātais izdevums. Rīga: Autora izdevums, 1934.

8. Profesors Krugļevskis A. "Princips "nulla poena sine lege" un tā nozīme krimināltiesībās. Rīga: [b.i.] 1937.

9. Кудрявцев В.Н. Обьективная сторона преступления. Москва: Госюриздат, 1960.

10. Пионтковский А.А. Учение о преступлеплении по советскому уголовному праву. Москва: Юридическая литература, 1961.

11. Курс Советского уголовного права. ч. Общая т.1. Ленинград: изд-во Ленинградского университета,1968.

12. Курс Советского Уголовного права в шести томах, том. II. Общая часть под. ред.Пионтковсковского А.А. Москва: Наука, 1970.

13. Советское Уголовное право. Общая часть. Москва: Юридическая литература, 1977.

14. Уголовное право. История юридической науки. Под. ред. В.Н. Кудрявцева Москва: Изд. Наука, 1978.

15. Глистин В.К. Проблема уголовно- правовой охраны общественных отношений. Ленинград: издательство Ленинградского университета, 1979.

16. Коржанский Н.И. Обьект преступления и предмет уголовно правовой охраны. Москва. [b.i.] 1980.

17. Советское уголовное право. Общая ч. Москва: изд. Московского университета, 1981.

18. Schjolberg Stein Computers and penal legislation. A study of the legal politics of a new technology Universitetsforlaget, Oslo, 1983.

19. Parker D. Fighting Computer crime,[ b.i.] 1983

20. Прохоров В.С. Преступление и ответственность.Ленинград: изд.-во Ленинградского университета.,1984.

21. Eisenshitz T.S.Information transfer Policy isues of control and access. London, Library Association publishing,1984.

22. Марцев А. И. Преступление: сущность и содержание. Омск: МВД СССР Омская высшая шлола милиции, 1986.

23. Кудрявцев В.Н. Закон, поведение, ответственность. Москва:[b.i] 1986

24. Computer related crimes by Dr. Gulshan Rai, R. K. Dubash, Dr. A.K. Chakravarti Government of India dep. of Electronics New Deli.; OECD - Computer-Related Crime, Analysis of Legal Policy ,Paris, 1986.

25. Information security in Nordic Countries. Nordiske Seminar–og Arbeijds rapporter 1993

26. Уголовное право. Общая часть. Учебник. Под. ред. Б.В. Эдравомыслова, Москва: МГУ, 1996.

27. Наумов А.В. Уголовное право. Общая часть: Курс лекций. Москва: БЕК,1996.

28. Online law The spa's legal guide to doing business on the Internet. Th. J. Smedinghoff, ed. The software publishers Association, 1996.

29. Новое уголовное право России. Учебное пособие. Особенная часть. Под ред. Н.Ф.Кузнецовой. Москва: Зеркало ТЕИС, 1996.

30. Учебник уголовного права. Общая часть. Под ред. И.Н. Кудрявцева и А.В. Наумова. Москва: издательство Спарк, 1996.

31. Словарь по уголовному праву. Под ред. А.В. Наумова. Москва: Издательство -БЕК, 1997.

32. The Criminal law of Japan The General part by Shigemitsu Dando, translated by B. J. George, Rothman & Co, Littleton, Colorado 80127, 1997.

33. Копилов В.А. Информационное право. Москва: Юристь, 1997.

34. Bitāns A. Civiltiesiskā atbildība un tās veidi.- Rīga: AGB, 1997.

35. Уголовное право. Общая часть. Учебник для вузов., Москва: ИНФРА· М- НОРМА, 1997.

36. Krastiņš U. Mācība par nozieguma sastāvu. Rīga: Zvaigzne ABC, 1997.

37. Уголовное право. Общая часть. Под редакцией. З.А.Казаченко и А. Незнамова. Москва: Инфра· М-Норма, 1997.

38. Уголовное право. Общая часть. Учебник для вузов. Москва: Инфра ·М-Норма, 1997.

39. Krimināllikums Prof Dr. hab.jur. U.Krastiņa un Dr. iur. A. Niedres komentāri. Rīga- TNA, 1998

40. Banku Informācijas tehnoloģijas drošības noteikumu rokasgrāmata. Latvijas banka, 1998.

41. Флетчер Д., Наумов А.В. Основные концепциии современного уголовного права. Москва: Юристь,1998.

42. Criminal law in Denmark by Lars Bo Langsted, Van Greve, Peter Garde. Kluwer Law International. The Hague-London- Boston, 1998.

43. Legal aspects of computer- related crime in the Information Society – Comcrime- study - prepared for the European Commission by prof. Dr. Ulrich Sieber University of Wurzburg, Version 1.0 of 1st Jjanuary 1998.

44. Law of International on-line business A. Global perspective general editor Christian Campbel Sweet& Maxwell chapter 8 Finland by Pekka Raatikainen, Ahola& Sokka. - Helsinki Finland, London, 1998.

45. Панфилова Е. И., Попов Ф. Н. Компютерные преступления. Санкт-Петербург: [ b.i.] 1998.

46. Cybercrime & Secyrity. Compiled & edited by Alan E. Brill, Fletcher N. Baldwin, Jr. Robert J. Munro. II. Infrastructure protection & management solutions. Booklet II.6 Protection and defence of intrution by Dorothy.

Denning D. Georgetown university, March 5 1996. issued September 1998. Oceana publications, Inc., Dobbs Ferry, Ny., II.6-1

47. Grabovsky P.N. Smith R. Crime in the digital age. Controling telecommunications and cyberspace illegalities. –Transaction publishers/ The federation press, 1998

48. User identification and authentification a brief introduction February 1998 by Mark Bide and Trevor Hing. Book industry Communication & Edit EUR

49. Minimum Provisions for the investigation of computer based offences by David E. Thompson and Desmond R. Berwick © 1998 National Police Research Unit.

50. Курс Уголовного права. Общая часть. Том 1: Учение о преступлении. Под редакцией. Н.Ф. Кузнецовой и И.М. Тяжковой.Москва: Зеркало,1999.

51. Уголовное право. Под. ред. Гаухмана, Юриспруденция, Москва, 1999.

52. Krastiņš U., Liholaja V., Niedre A. Krimināltiesības. Rīga: TNA, 1999.

53. Krastiņš U., V. Liholaja, A. Niedre Krimināllikuma komentāri.1. grāmata. Vispārīgā daļa. Rīga- AFS, 1999.

54. Grewlich Klaus W. Governance in "cyberspace" access and public interest in global communications. Kluwer law international 1999.

55. Real law@ virtual space regulation in cyberspace. ed. by Susan J. Drucker, Garry Gumpert, Hampton press Inc.1999.

56. Росссийское уголовное право. Общая ч. Учебник. Под редакцией М.П. Журавлева. 1999. Москва: издательство "Щит-М" 1999.

57. Уголовное право Росиии. Учебник для вузов. В 2- х томах. Т.1. Общая часть. Под редакцией А.И. Игнатова и Ю. А. Красикова. Москва-Норма- Инфра· М, 1999.

58. Ахметин Х. М., Петухов А. А. Современное уголовное законодательство КНР. Уголовный кодекс КНР, Москва: Издательский дом. "Муравей", 2000.

59. The implementation of the Corpus Juris in the member States. Vol. 1. Prof. M. Delmas- Marthy and prof. J.A.E. Vervaele. Antwerpen-Groningen-Oxford- Insersentia, 2000.

60. A Handbook of criminal law terms by Bryan A. Garner. St. Paul, Minnesota –West group, 2000.

61. Гаврилов О.А. Курс правовой информатики. Учебник для вузов.- Москва: Норма-Инфра·М, 2000.

62. Judins A.Krimināl atbildības izslēdzamības apstākļi. Rīga: TNA, 2000.

63. Krastiņš U. Noziedzīgs nodarījums. – Rīga: TNA, 2000.

64. Law's future(s) British legal developments in the 21st Century edited by David Hayton. Oxford-Portland Oregon – Hart publishing, 2000.

65. Simester A.P., G.R. Sullivan Criminal law theory and doctrine. Hart publishing, Oxford- Portland Oregon, 2000.

66. Соколов А.В. Шпионские стучки. Новое и лутшее- Полигон, Санкт-Петербург , 2000.

67. [b.a.] High technology crime in California. Annual report on high technology crime in California. Prepared by High tech crime advisory committee, 2000.

68. [b.a.]Anarchy cookbook version 2000, [b.i.]

69. Clarkson C.M.V. Understanding criminal law Third ed., London, Sweet& Maxwell, 2000.

70. Chirillo John Hack attacks encyclopedia. A complete history of hacks, cracks, phreaks and spies over time. New-York-Willy Computer Publishing. John Willey & Sons Inc., 2001.

71. Gelbstein E.,Kamal A. Information insecurity. A survival guide to the uncharted territories of cyber- threats and cyber security. New-York- United Nation ICT task force and UNITAR , 2002.

72. Gragovsky P., Smith R., Dempsey R. Electronic theft Unlawful Acquisition in cyberspace.- Cambridge University press, 2001.

73. Кудрявцев В.Н. Общая теория класификациии преступлений. Москва: Res cottidiana. Юристь, 2001.

74. Егоров В.С. Понятие состава преступления в уголовном праве. Уч.пособие. М.,Московский психолого социальный институт, 2001.

75. Новоселов Г.П. Учение об обьекте преступлениюю Методологические аспекты. Москва: Норма, 2001.

76. Уголовное право. Общая часть. Пособые для подготовки к экзамену. 2-е издание Москва: Юрайт, 2001.

77.Курс Уголовного права. Том 4, Особенная часть. Под редакцией. Г.Н. Борзенкова и В.С. Комисарова, Москва, Зеркало-М, 2002.

78. Волеводз А. Г. Противодействие компютерным преступлениям. Правовые основы международного сотрудничества. Москва: Юрлитинформ, 2002.

79. Hack attacks revealed. A complete reference for Unix, Windows and Linux with custom security toolkit. Second edition John Chirillo. Indianopolis-Willey publishing, 2002.

80. Смирнова Н.Н. Уголовное право. Учебное пособые. Санкт-Петербург: издательство Мыхайлова, 2002

81. Леонов Д.Г., Лукацкий А.В., Медведовский И.Д., Семянов Б.В. Атака из Интернет. Аспекты защиты. Москва: Соломон-Р, 2002

82. Informācijas un komunikāciju tiesības Ķiņa U. redakcijā II. sēj., Trešā grāmata. Rīga: Turība, 2002.

83. Towards a universal order of cyberspace: managing threats from cybercrime to cyberwar. Report& recommendations.[b.i] 2002.

84. Mission Critical Security Planner. Creating Custumised strategies by Eric Greenberg. Indianpoliss-Wiley publishing Inc. 2003.

85. Wayne R. LaFave Criminal law Fourth edition Hornbook Series Student edition. Thomson West., 2003.

86. Liholaja V. Krimināllatbildība Spānijā un Latvijā. Rīga: Latvijas Vēstnesis, 2003.

87. Krastiņš U., Liholaja V. Niedre A. Krimināllikuma zinātniski- praktiskais komentārs (1) Vispārīgā daļa. U. Krastiņa redakcijā. Rīga- AFS, 2003

88. Krastiņš U., Liholaja V., Niedre A. Krimināllikuma zinātniski- praktiskais komentārs 3. sevišķā daļa U. Krastiņa redakcijā., Rīga : AFS, 2003.

89. Уголовное право зарубежных стран. Общая часть. Под редакцией Проф. И.Д. Козочкина. Москва: Омега Л, 2003

90. Kuznetsova N.F Selected works. Saint Petersburg: Yuridichesky Center Press, 2003.

91. Miķelsons U. Informācijas tehnoloģiju noziegumu izmeklēšanas īpatnības. Rīga: Turība, 2003.

92. Identity theft law & filings answers by Robert Morgester, Deputy attorney General, [b.i] 2003.

93. Орехов В.В. Необходимая оборона и иные обстоятельства, изключающие реступность деяния.Санкт-петербург- Юридический центр Пресс, 2003

94. Ветров Н.И. Уголовное право. Общая часть. Москва: Юнити, 2003.

95. Handbook of legislative procedures of computer and network misuse in EU countries. Study for the European Commission Directorate-General Information society (2002) Rand Europe. © ECSC-EC-EAEC, Brussels-Luxembourg 2003.

96. Kacman. A.Computer crimes Disertation to come forward as candidate of legal sciences. Authors summary. Tbilisi: State University of Tbilisi: 2004.

97. Smith Russel G.; Grabosky Peter; Urbas Gregor Cybercriminals on Trial. Cambridge University Press, 2004.

98. Ashworth Andrew Principles of Criminal law. Third edition. Oxford University Press,[b.g.].

99. Introduction to Criminal Justice fifth edition by J.J. Senna, L. J. Siegel St. Paul-New York- Los Angeles- Sanfrancisco –West publishing company [b.g.].

100. Essays in Criminal law Nils Jareborg Iustus Förlag. Juridiska Förennigen i Uppsala, [b.g.].

101. Computer related crimes by Dr. Gulshan Rai, R. K. Dubash, Dr. A.K. Chakravarti Government of India dep. of Electronics New Deli[ b.i][b.g.]

102. Crimes related to computer networks-Some legal aspects by Hans G. Nilson[b.g][b.i].

103. Fundamentals of criminal law. Second edition. Paul. H. Robinson. Little, Brown and company. Boston- new- York- Toronto- London,[b.g]

104. International response to cybercrimes Ch.2. by Tonya L. Putnam, David D. Eliot Huver Press,[b.g]

105. KPFSR Kriminālkodeks. Komentārs I. T. Goļakova red.- Rīga: Grāmatu apgāds, 1946.

106. Коментарый к Уголовному кодексу РСФСР, под. ред. Ю.Д. Северина. Москва: Юридическая литература,1980.

107. Коментарый к Уголовному кодексу РСФСР ,под. ред. Ю.Д. Северина. Москва: Юридическая литература,1984.

108. Коментарый к уголовному кодексу Росийской федерации. Издание 3-е измененное и дополненное. Под. ред. Генерального прокурора Российской Федерации Ю.И. Скуратова и Председателя Верховного суда Российской Федерации В.М. Лебедева. Москва- издательская группа Инфра · М- Норма, 2000.

110. Čerfase L. Latīņu valodas spārnotie teicieni.- Rīga, Zinātne, 1992.

111. Filozofijas atlants attēli un teksti. Rīga: Zvaigzne ABC, 1999.

Periodikā publicētie zinātniskie raksti

1. Лейст И. Понятие ответсвенности в теории права,// Вестник Московского Университета 1/1994 с. 11 Право с.2

2. Sieber U. Computer crime and Criminal information law. New trends in the international risk and information society. Updated and extended version of an article in the German language published in Computer und Recht (CR) 1995

3. Catherine Therese Clarke. From criminet to cyber perp: towards an inclusive approach to oicing. The involving criminal means rea on the Internet. Oregon law review, Spring., 1996.

4. The cyberspace revolution David G. Post Keynote Address, Computer Policy & Law Conference, Cornell University, July 9. 1997.

5. Why police don't care about computer crime. 10 Harv. J.L.&Tech. 465.(Summer 1997) by Marc D. Goodman

6. Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 Texas law review 553 (1998).

7. Ķinis U. Tiesības informācijas sabiedrībā. Latvija un Eiropas Savienība Nr. 18. 2000.gada decembris,36.-43.lpp.

8. Brenner Susan "Is there such a thing as a virtual crime?" California Criminal Law Review Volume 4: June 2001.

9. Ķinis U. Kibernoziegumi un krimināļprocess. Latvijas Vēstnesis, 2001.gada 20. un 28.februāris.

10. Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law Susan W Brenner. University of Dayton School of Law. E Law - Murdoch university Electronic Journal of Law. Volume 8 Number 2 (June 2001).

11. Cyber Attacks during the war on terrorism: Predictive analysis. Institute for security technology studies at Dartmouth college, September 2001.

12. Susan W. Brenner, State Cybercrime Legislation in the United States of America: A Survey, 7 RICH. J.L. & TECH. 28 (Winter 2001).

13. Cybercrime investigation and prosecution: The role of the penal and procedural law by S. W. Brenner// E-law – Murdoch University Electronic journal of law.Vol. 8 Nr.2 (June 2001)// http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html (aplūkots 2004.gada 22. martā).

14. Brennere V.S. Kibernoziegumi un tradicionālie noziedzīgie nodarījumi: juridisko problēmu analīze, Likums un tiesības, 2002, 4.sēj.,nr.9 (37).

15. The legislative response to the evalution of computer viruses by: Mark R. Collombel .The Richmond journal of law and technology. Vol. VIII, Issue 3, Spring 2002.

16. Acceptable use. Whose responsibility is it? By Patti Lawrence// SANS Institute 2002.

17. In search of balance between police power and privacy in the Cybercrime treaty. by D.C. Kennedy // The Richmond Journal of law and technology Vol. IX. Issue 1., fall 2002.

18. The law and economics of reverse engineering by Pamela Samuelson and Susanne Scotchmer// Yale Law Journal May 2002

19. Substantive criminal law Wayne R.La Fave Part.2 General principles Chapter 5. Mental states. Westlaw 2003.

20. Hopkins Sh.L. Cybercrime convention: A positive beginning to a long road ahead. Journal of High technology law. 2003.

21. Substantive Criminal Law Wayne R. LaFave Part 1. Introduction; Sources And Limitations Chapter 1. Introduction And General Considerations. Westlaw 2003.

22. Cybercrime Convention: A Positive beginning to a long road ahead. Shannon L. Hopkins//Journal of high technology law, 2003.

23. Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes by Orin S. Kerr. // New york University law review . Vol. 78 (2003) Nr. 5 November

24. The US response to criminal exploitations of the Internet and other new technologies presentation by Michael A. Sussman. Money Laundering and Cybercrime: The EU Response to Criminal exploitation of new technologies. Academy of European law. Trier, Germany 20-22. february 2003.

25. Belardo John and Savage Stefan Denial of service attacks: real vulnerabilities and practical solutions. San Diego-Department of Computer science and engineering University of California,[b.g.] p. 4

26. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy by Dorothy E. Denning Georgetown University http://www.nautilus.org/info-policy/workshop/papers/denning.html (aplūkots 2004.gada 7. februārī).

Internetā publicēti palīgmateriāli

1. Eiropas Padomes informācijas biroja mājas lapa. http://www.coecidriga.lv/tulkojumi/R(87)18.htm (aplūkots 2005.gada 24.aprīlī).

2. The Code of Hamurapi. The Avalon Project at Yale Law School. www.yale.edu/lawweb/avalon/medieval/hamcode.htm (aplūkots 2005.gada 30. aprīlī).

3. The legal framework - unauthorised access to computer systems, Penal legislation in 37 countries (last updata March 15 1999 by Stein Scjolberg http://www.mossbyrett.of.no/info/legal.html (aplūkots 2005.gada 23. martā).

4. Cybercrime law. A global survey of computercrime legislation. http://www.cybercrimelaw.net/index.html (aplūkots 2005.gada 6. maijā).

5. The electric law library's legal lexicon on crime. http://www.lectlaw.com/def/c330.htm; [b.a.]

6. Criminal law in England and Wales http://www.luiss.it/erasmuslaw/uk/Ingh8.html#p1 (aplūkots 2005.gada 11.aprīlī).

7. Connecticut General Assembly http://search.cga.state.ct.us/ (aplūkots 2005.gada 14. martā).

8. State computer crime statutes citations http://www.crime-research.org/library/State.pdf (aplūkots 2005.gada 23. martā).

9. Computer crime by R. B. Standler http://www.rbs2.com/ccrime.htm#anchor111111 (aplūkots 2005.gada 22. martā).

10. Virus information library. http://vil.nai.com/vil/content/v_98229.htm (aplūkots 2005.gada 22. martā ).

11. Responsibility for computer crimes provided by CIS and Baltic countries' criminal law. Computer crime research center. http: www.crime-research.org/eng/library/Criminal_Codes.html (aplūkots 2005.gada 22. martā).

12. Голубев А. Компютерная преступность – угроза национальной безопасности. Cybercrime research centra mājas lapa http://www.crime-research.ru/library/interv2.html (Aplūkots 2005.gada 21. novembrī).

13. Голубев В.Типология преступлений в сфере использования ЭВМ http://www.crime-research.ru/library/Golubev1203.html (aplūkots 2005.gada 20.aprīlī)

14. Slot Machine Justice for Melissa Author by Mark Rash http://www.securityfocus.com/columnists/81 (aplūkots 2005.gada 12. martā).

15. International review of criminal policy-United nations manual on the prevention and control of computer- related crime http://www.uncjin.org/Documents/EighthCongress.html#congress (aplūkots 2005.gada 21.aprīlī).

16. CERT mājas lapa http://www.cert.org/tech_tips/CIH_FAQ.html (aplūkots 2005.gada 7. aprīlī).

17. CERT coordination Center. Denial of service attacks// http://www.cert.org/tech_tips/denial_of_service.html (aplūkots 2005.gada 22. aprīlī).

18. CERT ® Coordination center. Frequently asked questions about malicious web scripts redirected by web sites http://www.cert.org/tech_tips/malicious_code_FAQ.html (aplūkots 2005.gada 10. aprīlī).

19. Risk management solutions: Response to cyber threats and cyberterrorism. http://www.insurancejournal.com/magazines/west/2004/02/23/features/37008.htm (aplūkots 2005.gada 23.aprīlī).

20. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Chapter Report, 05/22/96, GAO/AIMD–96–84), sk. http://www.access.gpo.gov/cgi–bin/useftp.cgi?IPaddress=wais.access.gpo.gov&filename=ai96084.txt&directory=/diskb/wais/data/gao (aplūkots 2005.gada 29. aprīlī).

21. USA Federal Communication Commission Compliance& Information bureau Interferrence handbook. http://www.fcc.gov/cib/Publications/tvibook.html (aplūkots 2005.gada 12. aprīlī).

22. The largest bank of Estonia under hacker attack by Dmitri Kramarenko http://www.crime-research.org/news/17.03.2004/137 (aplūkots 2005.gada 22. aprīlī).

23. Distributed denial of service attacks by P. Robichaux http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/ddosatku.asp (aplūkots 2004.gada 22.martā).

24. General viruses issues http://macsupport.miningco.com/compute/macsupport/msub4.htm; (aplūkots 2005.gada 10. aprīlī).

25. Investigation tool: Knowledge. Computer crime The U.N. Manual adapted by Editor Micheal J. O'Brien http://www.mobrien.com/computer_crime.shtml#extent (aplūkots 2005.gada 20.februārī).

26. A short history of computer viruses and attacks by Brian Krebs http://www.securityfocus.com/news/2445 (aplūkots 2005.gada 31.martā).

27. The history of computer viruses http://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml (aplūkots 2005.gada 31. martā).

28. How much does computer virus cost? By D. Kramarenko http://www.crime-research.org/news/09.03.2004/124 (aplūkots 2005.gada 10. aprīlī).

29. Chatroom reject fined for sending virus to woman Annova http://www.ananova.com/news/story/sm_308078.html?menu (aplūkots 2005.gada 10. aprīlī).

30. U.S. House Committee Passes Anti-Spam Bill by Dave Murhy. http://dgl.com/itinfo/2000/it000323.html (aplūkots 2005.gada 12. aprīlī).

31. 2004 Carnegie Mellon University. http://www.cert.org/stats/#incidents (aplūkots 2005.gada 10. aprīlī)

32.W32.Mydoom.F@mm http://www.sarc.com/avcenter/venc/data/w32.mydoom.f@mm.html (aplūkots 2005.gada 10. aprīlī).

33. Introduction to TCP/IP. http://www.yale.edu/pclt/COMM/TCPIP.HTM (aplūkots 2005.gada 10. aprīlī).

34. Federal Standard Glosary of Telecommunication Terms http://www.its.bldrdoc.gov/fs-1037/dir-032/_4740.htm (aplūkots 2005.gada 23. aprīlī).

35. High tech dictionary http://www.computeruser.com/resources/dictionary/definition.html?lookup=8250 (aplūkots 2005.gada 28. aprīlī).

36. American heritage. Dictionary of English language: Forth edition 2000 http://www.bartleby.com/61/54/D0035400.html; (aplūkots 2005.gada 10. janvārī).

37. WikipediA The free Encyclopedya http://en.wikipedia.org/wiki/Interference (aplūkots 2005.gada 22. martā).

38. Webster dictionary http://www.m-w.com/cgi-bin/dictionary (aplūkots 2005.gada 23. martā).

39. Telecoms glosary of telecommunication terms http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm (aplūkots 2005.gada 23. aprīlī).

40. Cambridge advanced learner's dictionary http://dictionary.cambridge.org/define.asp?key=71111&dict=CALD&desc=secure (aplūkots 2005.gada 21. janvārī).

41. The Wordsmyth English Dictionary-Thesaurus http://www.wordsmyth.net/live/home.php?script=search&matchent=security&matchtype=exact (aplūkots 2005.gada 20. martā).

42. DEFCON http://www.defcon.org (aplūkots 2005. gada 23. martā).

43. Lielā terminu vārdnīca. http://www.termini.lv (aplūkots 2005.gada 12. aprīlī).

44. Computer crime statutes state by state http://www.onlinesecurity.com/links/links683.php (aplūkots 2004.gada 14. martā).

45. Understanding incident response http://www.fedcirc.gov/library/documents/understanding.html (aplūkots 2004.gada 22. martā).

46. Polimorhic virus. http://www.fcs.uga.edu/~mhazen/projects/re95/polymorph.html (aplūkots 2004.gada 22. martā).

47. Remarks of Deputy Attorney General Eric H. Holder, Jr. High-Tech Crime Summit January 12, 2000 http://www.usdoj-crm/mis/mdf (apskatīts 2003.gada 24. maijā).

48. The Internet Encyclopedia of phylosophy. Category. http://www.utm.edu/research/iep/c/category.htm (aplūkots 2003.gada 19. oktobrī).

49. Computer crime by R. B. Standler http://www.rbs2.com/ccrime.htm#anchor111111 (aplūkots 2002.gada 22. martā).

50. When economic crime becomes organized: the role of information technologies.A case study. http://www.transcrime.unitnt.it (aplūkots 2001.gada 21. janvārī).

52. When economic crime becomes organized: the role of information technologies.A case study // http://www.transcrime.unitnt.it (Aplūkots 2001.gada 21. janvārī).

53. FBI Investigates Web Domains Suspicious Names Registered before Attack.
http://abcnews.go.com/sections/scitech/TechTV/techtv_domains010921.html (aplūkots 2001.gada 25.septembrī).

54. Recombinant Culture: crime in the digital network by Curtis E.A. Karnow Landels, Ripley & Diamond Defcon II Las Vegas July 1994 http://www.cpsr.org/cpsr/privacy/crime/karnow.html (aplūkots 2000.gada 21. oktobrī).

55. U.S. networks run big risk of cyber–strikes, experts assert. http://www.siliconvalley.com/docs/news/depth/cyber100101.htm# (aplūkots 2001.gada 25.septembrī).

56. Porn virus affects Swedish court's e- mail system. http://www.anova.com/news/story/sm_288908.html?menu (aplūkots 2001.gada 10. martā).

56. Rules in the Virtual Society by Mark Gould http://aranea.law.bris.ac.uk/VirSoc/ (aplūkots 2000.gada 10. oktobrī).

57. Cyber-crime and legal problems of Internet usage by Golubev Vladimir http://www.networkremotemonitor.com/articles/cyber/cyber.html (aplūkots 2000.gada 2. jūnijā).

Prakses materiāli

1. US Supreme Court. Miller v California 413 U.S. 15. (1973) http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=413&invol=15 (aplūkots 2005.gada 21. aprīlī).

2. United States v Moriss http://www.law.uoregon.edu/faculty/kaoki/site/secure/cases/unauthorized/us_v_morris.php (aplūkots 2005.gada 23. martā).

3. Judgement in US v Robert Tappan Morris// http://www.rbs2.com/morris.htm (aplūkots 2005.gada 23. martā).

4. United states of America v Ali Saleh Kahlan Al-Marri.

http://news.findlaw.com/hdocs/docs/almarri/usalmarri61803dmol.pdf (aplūkots 2005.gada 14.martā).

5. EF Cultural travel BV, ET AL. v Zefer Corporation and Explorica, INC., ET AL// http://business.cch.com/computer/1020/EFCultural.pdf (aplūkots 2005.gada 11. martā).

6. Testimony United States Senate Committee on the judiciary. Executive business meeting. Report on the investigation into improper access to the Senate Judiciary Committee's computer system. March 4. 2004// http://news.findlaw.com/hdocs/docs/senate/pickle30404rpt1.html (aplūkots 2005.gada 22. martā).

7. LR IeM VP GKrPP Ekonomikas policijas pārvaldes krimināllietas Nr. 11810014003 materiāli.

8. 2003.gada 25. novembra Spriedums A.G. apsūdzībā pēc Krimināllikuma 116. panta un 175.panta 2.daļas.Kuldīgas rajona tiesas Krimināllieta Nr. 1250011203 KL19-246/03

9. Spriedums Vidzemes apgabaltiesas krimināllietā Nr. 1180007903/K-05-44/04 S.C. apsūdzībā pēc Krimināllikuma 177. panta 3.daļas un 241. panta 2.daļas.

10. OECD Guidelines for the security of Information systems 26 November 1992 Explanatory Memorandum to Accompany the Guidelines for the Security of Information Systems http://www.oecd.org/dsti/sti/it/secur/prod/e secur (aplūkots 2005.gada 21. janvārī).

11. Commission of the European Communities. Proposal for a Council framework decision on combating serious attacks against information systems. eEirope 2002 http://cryptome.org/eu-antihack.htm (aplūkots 2005.gada 22. martā).

12. 2003 CSI/FBI Computer Crime and Security Survey

13. 2003 Australian Computer crime and security survey.

14. Routine external and internal "hacking", An important par of information assurance. Mary Washington College, MBUS 511, Security Essentials by Benjamin Herman GSEC Practical Assignment - Version 1.2b © SANS Institute 2003

15. Dayton Cybercrime Seminar 2004. Spring http://lawschool.westlaw.com (aplūkots 2004.gada 25. martā).

16. 2004 CSI/FBI Computer crime and security survay

17. OECD Guidlines for the security of information systems and networks. Towards a culture of security 2002

17. Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)) 11. July 2001

18. Cybercrime Convention Explanatory report. CM (2001) 144.addendum

20. Computer crime in Poland: three years' expierence in enforcing the law. Contribution by Andrzej Adamski Conf CY (2001) Nat 1

21. Comentary on articles of the Convention PC-CY (2000)14- Draft EM REV.3, p. Committee of experts on crime in cyberspace (PC-CY) Summary report of the 7th Plenary meeting. Restricted PC- CY (2000)11

22. Conference on cybercrime. Budapest 22. November 2001. National report Japan. Conf CY (2001) Nat.1

23. ConfCy (2001) Exp.Mem. Explanatory Report to the Convention on Cybercrime

24. UN Tenth United nations Congress on the Prevention of crime and the Treatment of Offenders Vienna 10-17 Aprill 2000. Crimes related to computer network. background paper for the workshop on crimes related to the computer network A/Conf.187/10

25. Information management: Legal and security issues by Andrzej Adamski. Presentation of Polish delegation to UN X Congress on crime prevention Vienna 2000

26. Commments received to draft Convention on Cyber- crime from 13.November 2000 to 6. December 2000. Misc.3 Pc- CY Plen 10 ,10. December 2000

27. [b.a.]High technology crime in California. Annual report on high technology crime in California. Prepared by High tech crime advisory committee, 2000

28. Eurostat R&D and Innovation Statistics- Eight EEA Working Party Meeting Luxembourg, 22nd-25th November 1999 Doc Eurostat/A/4/REDIS/99/10

29. Permanent Council of Organisation of American States.responses received to the questionnaire prepared at the first meeting of government experts on cyber crime. GE/REMJA/doc.47/99, 5 October 1999

30. The University of Dayton School of law. Cybercrimes. Cybercrimes model state computer crimes code. Fall. 1999.

31. Some trends of cybercrime under Latvian substantial laws, by Kinis U. PC-CY (97) 17

32. M. Mohrenschlager "Substantive criminal law" PC- CY ( 97) 50

33. PC-CY (97) 40 Computer- related investigations:serch and seizure. Options paper by Donald K. Piragoff and Larisa L. Easson Canada, September 1997

34. Bundesamt für Sicherheit in der Informationstechnik IT-Grundshutzhandbuch 1997 BSI 7252 CD

35. Recommendation Nr. (95)13 of criminal procedurial law cennected with information technology. P. Csonka Council of Europe Activities related to information technology, Data protection and computer crime 5 (1996) Information & Communication technology law

36. OECD - Computer-Related Crime, Analysis of Legal Policy , Paris, 1986

37. Autora personīgā e- pasta sarakste ar Dr. Sc.Comp. J. Borzovu "teorētisks jautājums".

38. "Some question of criminal law theory" by S. Brenner. Autora privātā elektroniskā pasta sarakste.

39. Some trends of cybercrime under Latvian Substantial law by Uldis Ķinis PC-CY (97)17

Starptautiskie tiesību akti

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or "spam" COM (2004) 28 final

2. ConfCT(2001) Exp.Mem. Explanatory report to the Convention on cybercrime. Strasbourg 12 November 2001

3. Convention on cybercrime (ETS. No 185) Explanatory report// http://conventions.coe.int/Treaty/EN/cadreprincipal.htm (aplūkots 2005.gada 21. aprīlī).

4. Proposal of Council framework decision on attacks against information systems. Explanatory memorandum. Brussels COM (2002) 173 Final 19.04.2002 2002/0086 (CNS)

5. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach. COM/2001/0298 final http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=52001DC0298&model=guichett (aplūkots 2005.gada 21. janvārī).

6. Recommendation No R (89)9 on computer related crime report prepared by proffessor Henrik W.K. Kaspersen Computer/law Institute Amsterdam February 1997 CDPC (97)5; PC-CY (97(5 p.91

7. Council Resolution of 17 January 1995 on the lawful interception of telecommunications Official Journal C 329, 04/11/1996 P. 0001 – 0006 http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31996G1104&model=guichett (aplūkots 2005.gada 23. martā).

8. Recommendation Nr. (95)13 of criminal procedurial law cennected with information technology. P. Csonka Council of Europe Activities related to information technology, Data protection and computer crime 5 (1996) Information & Communication technology law

9. OECD Guidelines for the security of Information systems 26 November 1992 Explanatory Memorandum to Accompany the Guidelines for the Security of Information Systems

10. Directive 91/250 of May 1991 on the legal protection on computer programs// OJ L 122 , 17/05/1991 P. 0042 - 0046

11. Council of Europe Legal affairs Computer related crime pefased by August Bequai, European by European Committee on Crime Problems, Strasbour 1990. Recommendation No (89)9 on computer related crime and final report of the European Committee on Crime Problems

Citi dokumenti

1. Уголовный Кодекс Австрии. Перевод с немецкого Серебренниковой А.В. Москва: МАКС Пресс, 2001

2.Уголовный Кодекс Республики Беларусь. Минск: Тессей, 2001

3. Уголовный Кодекс Республики Болгария. Минск: Тессей, 2000

4. Уголовный Кодекс Грузии. Научный редактор З.К. Бигвана, Санкт-Петербург, Юридический центр пресс, 2002

5. Уголовный Кодекс Голландии, Научный редактор Б.В.Волженин. Перевод с английского И.М. Мироновой. Санкт-Петербург: Юридический центр пресс, 2001

6. Уголовный Кодекс Франции, Под редакцией Л.В. Головко, Н.Е. Криловой. Перевод с французского Н. Е. Криловой. Санкт-Петербург: Юридический центр пресс, 2002

7. Уголовный Кодекс Республики Казахстан. Санкт-Петербург: Юридический центр пресс, 2001

8. Уголовный Кодекс Китайской Народной Республики. Санкт-Петербург: Юридический центр пресс, 2001

9. Уголовный Кодекс Испании. Под редакцией Н.Ф. Кузнецовой и Ф.М. Решетникова. Москва: Зеркало, 1998

10. Уголовный Кодекс Киргизской Республики. Санкт-Петербург: Юридический центр пресс, 2002

11. Уголовный Кодекс Республики Казахстан. Санкт-Петербург: Юридический центр пресс, 2001

12. Уголовный Кодекс Республики Молдова. Санкт-Петербург: Юридический центр пресс, 2003

13. Уголовный Кодекс Республики Польша. Минск: Тессей, 1998

14. Уголовный Кодекс Российской Федерации. Полный сборник кодексов Российской Федерации. Москва: Айст, 1999

15. Уголовный Кодекс Швеции. Перевод С.С. Беляева. Москва: МГУ, 2000

16. Уголовный Кодекс Швейцарии. Москва: Зеркало, 2000

17. Уголовный Кодекс Японии. Санкт-Петербург: Юридический центр пресс, 2002

18. Уголовный Кодекс Республики Таджикистан. Санкт-Петербург: Юридический центр пресс, 2001

19. Criminal code (Strafgezetzbuch StGB) http:// www.juscomp.org/gla/statutes/StGB.htm (aplūkots 2004.gada 22. martā).

20. Codici e Leggi per l'udienza penale 2004. M.Chiavario,D.Manzione,T.Padovani, edizione Zanichelli 2004

21. Penal Code of Estonia// htpp://www.crime-research.org/eng/library/Criminal_Codes.hml (aplūkots 2004.gada 22. martā).

22. Федеральный закон " Об информации, информатизации и защите информации" от 25 января 1995г.[b.i]

23. Criminal code of Republic of Lithuania [b.i] 2002

24. Закон о Безопасности. Ведомости Сьезда Народных Депутатов Российской Федерации. 1992. Nr. 15

25. Israel Computers Law of 1995 [b.i]

26. Portugal Criminal Information law of August 17 1991[b.i.]

27. Venecuela Special Statute against computer related crimes[ b.g.][b.i.].

28. UK Computer misuse Act [b.i], 1990

29. UK Terrorism Act 2000// http:// www.hmso.gov.uk/acts/acts2000/00011--b.html#1(aplūkots.2005.gada 12. janvārī).

30. Proposal of Council framework decision on attacks against information systems. Explanatory memorandum. Brussels COM (2002) 173 Final 19.04.2002 2002/0086 (CNS

Latvijas tiesību akti

1. Latvijas Satversme. Rīga: TNA, 1998.

2. Krimināllikums. Likums par krimināllikuma spēkā stāšanās un piemērošanas kārtību. Rīga: TNA, 2003.