LATVIJAS UNIVERSITĀTE
JURIDISKĀ FAKULTĀTE
Krimināltiesisko zinātņu katedra

Bakalaura darbs

Noziedzīgu nodarījumu Informācijas sistēmu drošības jomā krimināltiesiskie un kriminoloģiskie aspekti

Saņemts
_____ katedra
2010.g. ___._____

_____
Sekretāra(-es) paraksts

Nepilna laika klātienes nodaļas
7. semestra studente
Ingrīda Irguļska
ii 05006

Zinātniskais vadītājs
Dr. iur., docents Andrejs Vilks

Rīga, 2010

Satura rādītājs

Bakalaura darbā lietotie apzīmējumi

- ETS – (EN - *European Treaty Series*) Eiropas līgumu sērija. Konvencijas un līgumi, kas parakstīti laika posmā no 1949. gada līdz 2003. gadam, tikuši publicēti ETS.
- EN – angļu valodā
- RUS – krievu valodā
- IS – informācijas sistēma
- VISR – Valsts informācijas sistēmu reģistrs
- IP – (EN - *Internet Protocol*) Interneta protokols
- IMEI – (EN - *International Mobile Equipment Identity*) Starptautiskais mobilā aprīkojuma identifikators, kas unikāls katrai ražotajai ierīcei
- MAC – (EN - *Media Access Control*) Unikāls identifikators, kas tiek piešķirts katrai tehniskā aprīkojuma vienībai
- KL – Krimināllikums
- LAPK – Latvijas administratīvo pārkāpumu kodekss
- MP3 – patentēts digitālās audio kodēšanas formāts
- RGPP – Rīgas galvenā policijas pārvalde
- VP – Valsts policija
- VID – Valsts ieņēmumu dienests
- LATAFIS – Automatizētā daktiloskopiskās identifikācijas sistēma
- ITIL – Informācijas tehnoloģiju pakalpojumu vadības sistēmu standarts
- ANO – Apvienoto Nāciju Organizācija
- LVS ISO/IEC 17799:2002 – Latvijas standarts "Informācijas tehnoloģija. Prakses kodekss informācijas drošības pārvaldībai"
- ISO – (EN - *International Organization for Standartization*) – Starptautiskā standartizācijas organizācija
- NASA – (EN - *National Aeronautics and Space Administration*) – Nacionālā aeronautikas un kosmosa administrācija
- LETA – Nacionālā ziņu aģentūra
- RAPLM – Reģionālās attīstības un pašvaldības lietu ministrijas
- ESM – elektroniskā skaitļojamā mašīna

- CERT – (DDIRV) Datoru drošības incidentu reaģēšanas vienība
- GB – Gigabaits

Ievads

Bakalaura darba tēma ir "Noziedzīgu nodarījumu Informācijas sistēmu drošības jomā krimināltiesiskie un kriminoloģiskie aspekti". Aplūkojamo noziedzīgo nodarījumu grupa nav pietiekami izpētīta. Tā ir saistīta ar noziedzīgiem nodarījumiem datorvidē jeb tā sauktajiem kibernoziegumiem vai datornoziegumiem, kuri spriežot pēc pētījumu un apkopojumu rezultātiem, kā arī dažādu rakstu publikācijām masu saziņas līdzekļos un kriminālās statistikas datiem ir aktuāli šodien un savu aktualitāti nezaudēs arī turpmāk. Informācijas tehnoloģijas strauji attīstās un tās tiek pielietotas dažādās dzīves nozarēs, līdz ar ko bieži vien ir problēmas ne tikai izprast attiecīgo terminoloģiju vai darbības principus, bet arī ar to ieguvumu aizsargāšanu, ko var sniegt informācijas tehnoloģijas. Datortīklus un elektronisko informāciju var izmantot arī noziedzīgu nodarījumu izdarīšanai. Pierādījumus, kas saistīti ar šādiem noziedzīgiem nodarījumiem, var uzglabāt un nodot izmantojot internetu. Informācijas tehnoloģiju devums, ko tās var sniegt un sniedz var tikt izmantots arī ļaunprātīgiem mērķiem un nodarīt lielu kaitējumu neskatoties uz to radīšanas ideju. Plašā datorsistēmu integrācija mūsdienu modernajā sabiedrībā padara tās par kiberapdraudējuma objektiem.

Bakalaura darba **hipotēze**: noziedzīgi nodarījumi informācijas sistēmu drošības jomā ir saistīti ar to, ka informācijas tehnoloģijas attīstās daudz intensīvāk, salīdzinot ar to drošību nodrošinošo krimināltiesisko regulējumu.

Bakalaura darba **mērķis** ir izpētīt mūsdienu informācijas tehnoloģiju daļas – informācijas sistēmu drošības sasaisti ar pastāvošajām krimināltiesībām un izpētīt, kādi kriminogēnie procesi ietekmē šo sasaisti.

Lai sasniegtu izvirzīto mērķi, tika izvirzīti sekojoši **uzdevumi**:

1) izpētīt jēdzienu "Informācijas sistēmas un to drošība", apzināt tā saturu;
2) izpētīt spēkā esošos tiesību aktus informācijas sistēmu drošības jomā Latvijas Republikā;

3) noskaidrot noziedzīgu nodarījumu informācijas sistēmu drošības jomā kriminoloģiskos aspektus;
4) apzināt esošos prevencijas līdzekļus un pasākumus noziedzīgu nodarījumu informācijas sistēmu drošības jomā novēršanai;
5) izpētīt ārvalstu tendences un metodes informācijas sistēmu drošības aizsardzības jomā.

Bakalaura darba izstrādes procesā izmantotas šādas **pētnieciskās metodes**:

1) kriminālās statistikas un dokumentu analīzes metode;
2) aptaujas metode veicot iedzīvotāju anketēšanu un intervējot ekspertus;
3) publikāciju masu saziņas līdzekļos izpēte, kontentanalīzes metode, par noziedzīgu nodarījumu informācijas sistēmu drošības jomā gadījumiem Latvijā un ārvalstīs, kā arī tādiem gadījumiem, kuros ir un varētu būt iesaistīti Latvijas iedzīvotāji, 2010. gada laikā.

Bakalaura darbā izstrādes procesā tika veikta arī iedzīvotāju anketēšana (sk. Pielikumu Nr. 1 un Nr. 2), lai noskaidrotu iedzīvotāju vispārējo izpratni par kibernoziegumiem un to, cik lielu daļu no tās veido noziedzīgi nodarījumi informācijas sistēmu drošības jomā.

Bakalaura darba autore tikās un intervēja Latvijas Universitātes Matemātikas un Informātikas institūta Tīkla risinājumu daļas vadītāja vietnieci Katrīnu Sataki un sazinājās ar Valsts policijas Galvenās Kriminālpolicijas pārvaldes 4. nodaļas priekšnieku Aleksandru Buko, kurš sniedza atbildes uz jautājumiem par informācijas sistēmu drošību (sk. Pielikumu Nr. 3 un Nr. 4).

1. Informācijas sistēmas, to drošības un to apdraudējuma jēdziens un būtība

Noziedzīgi nodarījumi informācijas sistēmu drošības jomā ir tikai neliela daļa no vispārējās kibernoziegumu jeb datornoziegumu grupas. Tādēļ autores ieskatā ir lietderīgi izskaidrot atšķirību starp datornoziegumiem vispārējā izpratnē un noziedzīgiem nodarījumiem informācijas sistēmu drošības jomā.

Ar tādiem vārdiem, kā „*kibernoziegums*" vai „*datornoziegums*" jāsaprot jebkura krimināla aktivitāte izmantojot datorus un internetu. [1] Šī aktivitāte ietver dažādas darbības sākot ar nelegālu mūzikas failu lejupielādi visbeidzot ar daudzu miljonu dolāru zādzību no banku kontiem. Kibernoziegumi ietver arī nemonetārus nodarījumus, kā piemēram, ļaunprātīgu programmu radīšana un izplatīšana vai konfidenciālas informācijas izplatīšana internetā.

Pasaules likumdošanā ir problēmas ar kibernoziegumu definēšanu. Jo tas skaitās diezgan jauns noziegumu paveids.

Eiropas Padome 2001. gadā ir izstrādājusi Konvenciju par kibernoziegumiem (*ETS 185*), kura Latvijā ir stājusies spēkā 2007. gada 1. jūnijā. Minētā konvencija ir vienīgais saistošais šāda veida instruments, kas kalpo par vadlīniju izstrādājot dalībvalstu nacionālo likumdošanu pret Kibernoziegumiem. Konvenciju papildina Protokols par Ksenofobiju un Rasismu, kas izdarīts ar datorsistēmu palīdzību (*ETS 189*).

Šajā konvencijā ir izveidots šāds kibernoziegumu iedalījums[2]:

Noziegumu grupa	Nozieguma veids
Noziedzīgi nodarījumi, kas vērsti pret datorsistēmu un datu konfidencialitāti, integritāti un pieejamību	Patvaļīga piekļūšana, patvaļīga pārtveršana, datu traucēšana, sistēmas traucēšana, ierīces ļaunprātīga izmantošana.
Ar datoru saistītie noziedzīgie nodarījumi	Ar datoru saistīta viltošana, krāpšana
Ar saturu saistītie noziedzīgie nodarījumi	Nodarījumi saistīti ar bērnu pornogrāfiju
Ar autortiesību un blakus tiesību pārkāpumiem saistītie noziedzīgie nodarījumi	

1. tabula: Konvencijas par kibernoziegumiem kibernoziegumu sadalījums

[1] Cybercrime. http://www.techterms.com/definition/cybercrime [aplūkots 2010. gada 22. septembrī]
[2] Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [aplūkots 2010. gada 22. septembrī]

Noziedzīgi nodarījumi, kas apdraud informācijas sistēmu drošību saskaņā ar minēto Konvenciju pieder pie noziegumu grupas – Noziedzīgi nodarījumi, kas vērsti pret datorsistēmu un datu konfidencialitāti, integritāti un pieejamību.

Latvijas Universitātes Datorikas fakultātes Bakalaura darba "Kibernoziegumi" autors Vitālijs Drivinieks iedala kibernoziegumus divās grupās pēc datora lomas noziedzīgu nodarījumu izdarīšanā "dators – kā rīks" un "dators kā - mērķis" [3].

Noziedzīgi nodarījumi informācijas sistēmu drošības jomā pieder pie grupas "dators kā mērķis", kuru pamatā ir tieši informatīvo sistēmu, datoru vai citu informāciju apstrādājošo ierīču darba pārtraukšana, aizkavēšana vai darbības veida izmainīšana, kā arī nelegāla piekļūšana aizsargātiem resursiem.

Lai izprastu, kas ir noziedzīgu nodarījumu informācijas sistēmu drošības jomā objekts, nepieciešams izpētīt terminu "informācijas sistēmas" un tām piedēvētās īpašības.

Konvencijas par kibernoziegumiem 1. pantā ir sniegti definējumi šādiem jēdzieniem:

1) "datorsistēma" - jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču grupa, no kuras viena vai vairākas ierīces saskaņā ar programmu veic automātisku datu apstrādi,
2) "dati" - jebkuri fakti, informācija vai koncepcija, kas paredzēta apstrādāšanai datorsistēmā piemērotā formā, tai skaitā programma, kas piemērota, lai liktu datorsistēmai veikt šādu funkciju,
3) "pakalpojuma sniedzējs" - jebkura juridiska vai fiziska persona, kas nodrošina savu pakalpojumu lietotājiem iespēju sazināties ar datorsistēmas palīdzību; jebkura cita persona, kas pārstrādā vai uzkrāj datus šādu komunikācijas pakalpojumu vai šādu pakalpojumu izmantotāju vārdā,
4) "datu plūsma" - jebkuri uz komunikāciju attiecināmi dati, kas radīti ar datorsistēmas palīdzību, kas veido daļu no komunikācijas ķēdes, norādot komunikācijas izcelsmi, saņēmēju, virzienu, laiku, datumu, apjomu, ilgumu vai pakalpojuma veidu.

Šī pati konvencija datorsistēmām un datiem piešķir trīs īpašības - "pazīmes, bez kuru konstatēšanas nevar būt ne runas par noziedzīgu nodarījumu pret informācijas sistēmu drošību." [4]

[3] Drivinieks V. Kibernoziegumi. Bakalaura darbs. Rīga: Latvijas Universitāte, 2009., 32.lpp.
[4] Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007., 110.lpp.

1) **Konfidencialitāte** - [EN – *confidentiality*; RUS - *конфиденциальность*] - datus raksturojoša īpašība, kas norāda to datu apjomu, kāds nav pieejams vai nav atklāts nepilnvarotiem indivīdiem, procesiem vai citām vienībām;
2) **Integritāte** – [EN – *integrity*; RUS - *целостность*] - datora atmiņā uzglabāto datu pilnīguma un korektuma saglabāšana pēc to modificēšanas;
3) **Pieejamība** [EN – *data accessibility*; RUS - *доступность данных*] - programmas vai lietotāja potenciālā spēja lasīt datus atkarībā no pieprasījuma valodas un paroles zināšanas.[5]

No augstāk minētā izriet, ka informācijas sistēmu drošība ir tāds informācijas sistēmas stāvoklis, kad darbojoties informācijas sistēmai tās konfidencialitāte, integritāte un pieejamība netiek traucētas, kas izriet arī no Informācijas tehnoloģiju drošības likuma projekta 3. panta 2. daļas. Konvencijā par kibernoziegumiem norādīti noziedzīgu nodarījumu veidi, kas vēršoties tieši pret minētajām datorsistēmām un datiem piedēvētajām īpašībām apdraud informācijas sistēmu tehniskos un informācijas resursus. Tie ir:

1) patvaļīga piekļūšana;
2) patvaļīga pārtveršana;
3) datu traucēšana;
4) sistēmas traucēšana;
5) ierīces ļaunprātīga izmantošana.

Ievērojot to, ka šī konvencija ir saistoša arī Latvijai, konvencijā paredzētie noziedzīgo nodarījumu veidi ir paredzēti arī Krimināllikumā, kas ir viens no konvencijas priekšnosacījumiem – lai Eiropas Savienības dalībvalstis likumdošanas procesā iestrādā mehānismus, kas aizsargā arī to pašu objektu, ko aizsargā konvencija. Krimināllikums aizsargā „automatizētas datu apstrādes sistēmas tehniskos un informācijas resursus", kas tiek aplūkots dotā bakalaura darba kontekstā.

Pārējie Konvencijā par kibernoziegumiem minētie noziedzīgie nodarījumi nepieder pie datu vai datorsistēmu drošību apdraudošajiem noziedzīgajiem nodarījumiem, jo to apdraudējuma objekts ir cits un šādi noziedzīgie nodarījumi pieder pie ar datoru saistītajiem ("dators - kā rīks") noziedzīgajiem nodarījumiem, ar saturu saistītajiem noziedzīgajiem nodarījumiem, ar autortiesību un blakustiesību pārkāpšanu saistītajiem noziedzīgajiem nodarījumiem.

[5] Terminoloģijas portāls. http://termini.letonika.lv/ [aplūkots 2010. gada 19. oktobrī]

Valsts informācijas sistēmu likums sniedz definējumu jēdzienam – valsts informācijas sistēma: strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta valsts funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana (informācijas aprite). Bez tam dotajā likumā informācijas sistēmas tiek iedalītas vairākās grupās:

1) Integrētā valsts IS – loģiska valsts IS apvienība, kuras ietvaros vienotā informācijas laukā tiek uzturēti atsevišķu valsts IS dati.
2) Centralizētā valsts IS – valsts IS lietotājs lieto centralizēti, izmantojot valsts IS savietotāju,
3) Kritiskā valsts IS – šīs sistēmas drošības apdraudējuma gadījumā valsts un sabiedrības drošības funkciju izpildei nepieciešamās informācijas aprite var tikt pakļauta riskam.

Ministru kabineta noteikumu Nr. 765 "Valsts informācijas sistēmu vispārējās drošības prasības" 2.7. punktā ir sniegts likumdevēja piedāvātais valsts IS drošības apdraudējuma definējums, kas atbilst pēc būtības vispārīgi arī pārējo – ne valsts IS, apdraudējuma definīcijai – "ar nodomu (tīši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas var izraisīt sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama".

MK instrukcijas Nr.20 "Valsts pārvaldes funkciju izpildi apdraudošu kiberuzbrukumu noteikšanas instrukcijas" izpratnē kibernoziegums ir patvaļīga (bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības) piekļūšana automatizētai datu apstrādes sistēmai vai tās daļai, ja tas saistīts ar datu apstrādes sistēmas aizsardzības līdzekļu pārvarēšanu; automatizētā datu apstrādes sistēmā esošās informācijas patvaļīga grozīšana, bojāšana, iznīcināšana, pasliktināšana vai aizklāšana (pieejamības ierobežošana) vai apzināti nepatiesas informācijas ievadīšana automatizētā datu apstrādes sistēmā; apzināta ierīces (arī datorprogrammas) izmantošana, kura paredzēta patvaļīgai automatizētas datu apstrādes sistēmas resursu ietekmēšanai.

Kaitējums iedarbojoties uz valsts IS konfidencialitāti, integritāti, pieejamību var tikt nodarīts jebkurai juridiskai un / vai fiziskai personai, kura normatīvajos aktos noteiktā kārtībā sniedz ziņas par sevi. Saskaņā ar Valsts informācijas sistēmu likuma 13. pantu, valsts IS ir reģistrējamas Valsts informācijas sistēmu reģistrā (VISR). VISR nodrošina iespēju jebkuram

interesentam vienkopus iegūt informāciju par valsts informācijas sistēmām. VISR pārzinis ir Reģionālās attīstības un pašvaldību lietu ministrija.[6]

Ikdienā, ja pastāv Informācijas sistēma, pastāv arī risks tās, tajās esošo datu un to veidojošo fizisko un loģisko elementu apdraudējumam. Informācijas sistēmas nav viendabīgas un ir veidotas dažādu funkciju izpildei, dati tiek grupēti vairākās kategorijās un katrai informācijas sistēmā esošai datu kategorijai ir dažādas pakāpes risks tikt apdraudētai.

Latvija, ievērojot tai saistošu konvenciju, starptautisko līgumu un protokolu prasības, normatīvajos aktos, kas regulē informācijas sistēmu drošību, ir paredzējusi ne tikai dažādus noziedzīgo nodarījumu veidus (KL 241.-245.p.), kas apdraud informācijas sistēmu drošību, bet izstrādājusi dažādus mehānismus Ministru kabineta noteikumu veidā (arī jaunā Informācijas tehnoloģiju drošības likuma, kas stāsies spēkā 2011. gadā), kas varētu to pareizas un ilglaicīgas piemērošanas rezultātā samazināt reālo iespējamo noziedzīgu nodarījumu informācijas sistēmu drošības jomā notikumu skaitu.

[6] Valsts informācijas sistēmu reģistrs. http://www.visr.eps.gov.lv/visr/ [aplūkots 2010. gada 23. septembrī]

2. Noziedzīgu nodarījumu informācijas sistēmu drošības jomā veidi un to krimināltiesiskais raksturojums

Jirgens Storbeks (bijušais Eiropola direktors, pilnvaras no 1999. līdz 2004. gadam) Internetu ir nodēvējis par "*jaunu dzīves sfēru un jaunu noziedzības skatuvi*"[7].

U. Ķinis norādījis, ka lai definētu kibernoziegumus, ir „*nepieciešams konstatēt, vai kibernoziegums ir jauna veida noziedzīgs nodarījums, vai tam piemīt tradicionālam nodarījumam raksturīgas pazīmes*"[8]. Šo apgalvojumu var attiecināt arī uz noziedzīgiem nodarījumiem informācijas sistēmu drošības jomā.

Sniedzot atbildi uz šo problēmjautājumu, U. Ķinis ir sniedzis atbildi, ka kibernoziegumi nav principiāli jauna veida noziedzīgi nodarījumi, tiem piemīt visas tradicionālam noziedzīgam nodarījumam nepieciešamās pazīmes (prettiesiskums un soda piedraudējums), tomēr ir arī atšķirības no klasiska noziedzīga nodarījuma jēdziena:

1) par kibernoziegumu var atzīt tikai personas tīšu darbību, izslēdzot atbildību par bezdarbību un nodarījumu aiz neuzmanības;
2) darbībai jābūt saistītai ar informācijas apriti kibertelpā;
3) šīs darbības var izdarīt izmantojot vai ietekmējot informācijas sistēmu resursus;
4) šie nodarījumi izdarīti attālināti – tieši, fiziski, neiedarbojoties uz IS resursiem.[9]

Izpētot Krimināllikumu noziedzīgiem nodarījumiem informācijas sistēmu drošības jomā nav paredzēta īpaša vieta vai nodaļa, tomēr tie ir ietverti Krimināllikuma XX nodaļā, kuras nosaukums ir „Noziedzīgi nodarījumi pret vispārējo drošību un sabiedrisko kārtību." Tādi noziedzīgi nodarījumi, kas apdraud informācijas sistēmu drošību Krimināllikumā atrodas starp ugunsdrošības noteikumu pārkāpšanu (240. pants) un ātri uzliesmojošu vielu un priekšmetu, kā arī kodīgu vielu neatļautu pārsūtīšanu (246. pants). Tātad, pavisam pieci Krimināllikuma panti. Krimināllikuma 242. pants ticis izslēgts ar 28.04.2005. likumu, kas stājas spēkā 01.06.2005.

Noziedzīgu nodarījumu informācijas sistēmu drošības jomā grupas objekts ir informācijas sistēmu drošība. Zemāk aplūkoto Krimināllikuma pantu Subjekts ir fiziska un pieskaitāma

[7] Information Insecurity. http://www.un.int/kamal/information_insecurity/Information_Insecurity_Second_Edition_PDF.pdf [aplūkots 2010. gada 21. oktobrī]
[8] Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007., 46.lpp.
[9] Turpat, 57.lpp.

persona, kura uz noziedzīgā nodarījuma izdarīšanas brīdi ir sasniegusi 14 gadu vecumu. Izņēmums ir KL 245. panta subjekts – speciālais subjekts.

2.1. Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai

Krimināllikuma 241. panta 1. daļa sniedz definējumu patvaļīgas piekļūšanas automatizētai datu apstrādes sistēmai noziedzīga nodarījuma sastāvam - patvaļīga (bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības) piekļūšana automatizētai datu apstrādes sistēmai vai tās daļai, ja tas saistīts ar datu apstrādes sistēmas aizsardzības līdzekļu pārvarēšanu un ja ar to radīts būtisks kaitējums. Dota panta noziedzīgā nodarījuma sastāvs ir materiāls, jo panta dispozīcijā ir norādītas kaitīgās sekas – radīts būtisks kaitējums. Pirmkārt, sistēmai jāpastāv aizsardzībai, jo, ja sistēma nebūs nodrošināta ar attiecīgiem aizsardzības līdzekļiem, analizējamā noziedzīgā nodarījuma sastāvs neveidosies.[10] Otra obligāta objektīvās puses pazīme ir – būtisks kaitējums, tāpēc jākonstatē, ka patvaļīgas piekļūšanas automatizētai datu apstrādes sistēmai rezultātā ir nodarīts ievērojams mantiskais kaitējums un apdraudētas vēl citas ar likumu aizsargātas intereses, vai arī, ka šāds interešu apdraudējums ir būtisks.[11] Zaudējumu izteiksmē šajā panta daļā minētā noziedzīgā nodarījuma izraisītais materiālais kaitējums pārsniedz piecu Latvijas Republikā noteikto minimālo mēnešalgu kopsummu. Krimināllikuma 241. panta 1. daļā paredzētais noziedzīgais nodarījums saskaņā ar Krimināllikuma 7. panta 3. daļu ir mazāk smags noziegums. Izplatītākie informācijas sistēmu pārvarēšanas līdzekļi ir[12]:

- programmas vājo vietu jeb programmas koda izmantošana;
- sociālās inženierijas – psiholoģiskas metodes informācijas iegūšanai no cilvēkiem vai metodes, kas nav saistītas ar loģisko informācijas sistēmu pārvarēšanu;
- paroļu vārdnīcu un piekļuves kodu izmantošana.

Krimināllikuma 241. panta 2. daļā paredzētais noziedzīgais nodarījums arī ir mazāk smags noziegums, bet šeit objektīvās puses pazīmes bez Krimināllikuma 241. panta 1. daļā minētajām ir mantkārīgs nolūks un smagas sekas, kas veido noziedzīgā nodarījuma materiālu (pēc kaitīguma smaguma pakāpes) un kvalificētu (pēc nodarījuma sastāva konstrukcijas īpatnībām) sastāvu. Šī noziedzīgā nodarījuma smagas sekas saskaņā ar likumu "Par

[10] Krastiņš U, Liholaja V., Niedre A. Krimināltiesības sevišķā daļa. Trešais papildinātais izdevums. Rīga: Tiesu namu aģentūra, 2009., 574.lpp.
[11] Turpat
[12] Drivinieks V. Kibernoziegumi. Bakalaura darbs. Rīga: Latvijas Universitāte, 2009., 37.lpp.

krimināllikuma spēkā stāšanās laiku un kārtību" būs mantiskais zaudējums lielā apmērā – tiks konstatēta zaudējuma summa, kas sasniedz vismaz piecdesmit Latvijas Republikā noteikto minimālo mēnešalgu kopsummu vai smags kaitējums ar likumu aizsargātām interesēm un tiesībām.

Kā piemēru, aplūkosim Latvijas Republikas Augstākās tiesas Senāta Krimināllietu departamenta 2006. gada 18. janvāra lēmumu lietā SKK – 01- 0007/06, no kura izriet, ka ar Rīgas pilsētas Centra rajona tiesas 2004. gada 8. marta spriedumu Nikolajs. K. un Ruslans B. atzīti par vainīgiem pēc Krimināllikuma 241. panta 2. daļas un katrs sodīti ar brīvības atņemšanu uz 6 (sešiem) mēnešiem. Bet spriedums tika atcelts pilnībā un kriminālprocess izbeigts noziedzīgā nodarījuma sastāva trūkuma dēļ sakarā ar to, ka pēc grozījumiem Krimināllikumā, darbības, kuras abi izdarīja neveidoja noziedzīgā nodarījuma sastāvu, jo netika konstatēts liels kaitējuma apmērs un mantkārīgs nolūks, turklāt saskaņā ar pārejas noteikumiem, pret personām bija jāpiemēro tā panta versija, kura bija labvēlīgāka apsūdzētajiem.

Darbības bija šādas: viņi bija patvaļīgi piekļuvuši automatizētai datorsistēmai, tādā veidā nepiederīgai personai radot iespēju iepazīties ar sistēmā ievietoto informāciju un tās darbību, saistītu ar datortehnikas programmatūras aizsardzības līdzekļu pārvarēšanu. Senāta Krimināllietu departaments atzina, ka neviena no iepriekš norādītajām obligātajām noziedzīgā nodarījuma sastāva pazīmēm abiem apsūdzētajiem netika konstatētas un inkriminētas.[13]

Krimināllikuma 241. panta 3. daļā paredzētais noziedzīgais nodarījums saskaņā ar Krimināllikuma 7. panta 4. daļu ir smags noziegums. Bet šeit objektīvās puses pazīmes bez Krimināllikuma 241. panta 1. daļā minētajām ir, ja Krimināllikuma 241. panta 1. daļā paredzētās darbības tiek vērstas pret valsts informācijas sistēmām. KL 241. panta 3. daļas noziedzīgā nodarījuma sastāvs ir materiāls. Šajā pantā paredzētā noziedzīgā nodarījuma noziedzīgā darbība ir vēršanās pret sistēmas īpašnieka vai viņa pilnvarotās personas noteikto kārtību likumīgam lietotājam vai ISD pazīmi – pieejamību.[14] Attiecīgi, šajā pantā paredzētā noziedzīgā nodarījuma objekts ir personas tiesību apdraudējums realizēt sev vēlamās pieejamības tiesības uz sistēmā esošiem resursiem.[15]

Krimināls odāmas nav tādas personas mērķtiecīgi veiktas darbības, kuras nerada būtisku kaitējumu, tas ir, likumdevējs šādai darbībai nav piešķīris augstu kriminalizācijas pakāpi,

[13] Latvijas Republikas Augstākās tiesas Senāta Krimināllietu departamenta 2006. gada 18. janvāra lēmums lietā SKK – 01- 0007/06.
[14] Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007., 204.lpp.
[15] Turpat – 205.lpp.

iespējams, dēļ tā, ka Internets pats par sevi ir nedrošs. U. Ķinis pauž viedokli: "*pati par sevi piekļūšana valsts informācijas sistēmām, pārvarot sistēmu aizsardzību, jau automātiski būtu atzīstama par būtisku kaitējumu*."[16]

Latvijas administratīvo pārkāpumu kodeksa 204^7. pantā paredzēta atbildība par pārkāpumu – nelikumīgām darbībām ar fiziskās personas datiem - tas ir, par jebkurām nelikumīgām darbībām ar fiziskās personas datiem, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu, izpaušanu, bloķēšanu vai dzēšanu. Tomēr uzņēmumu privātā informācija vienalga tiek apdraudēta, jo tā nav pienācīgi aizsargāta ar derīgām aizsargājošām tiesību normām gadījumos, kad tiek realizēta nelikumīga piekļuve uzņēmumu informācijas sistēmām un nav radīts ar to būtisks kaitējums.

Izpētot masu informācijas līdzekļus, kā piemēru, aplūkojamā Krimināllikuma panta ilustrācijai var minēt rakstu par hakeru darbībām Amerikā, kuri "uzlaužot sakaru operatora interneta vietni nolaupījuši vairāku personu elektroniskās adreses".[17] K. Sataki norāda, ka ir nekorekti lietot terminu "nolaupījuši" aprakstot nodarījuma objektīvo pusi, jo nolaupīšana ir zādzība un laupīšana. Proti, pirmajā gadījumā – svešas kustamas mantas slepena vai atklāta nolaupīšana, bet otrajā gadījumā – svešas kustamas mantas nolaupīšana, ja tā saistīta ar vardarbību vai vardarbības piedraudējumu. Dotajā piemērā nav tikusi konstatēta vardarbība vai vardarbības piedraudējums. Tātad, paliek tikai zādzība. Tomēr, nozagt var tikai kustamu mantu. Tātad – ķermenisku lietu. K. Sataki norāda, ka uz elektroniskajām adresēm mēs šādu apzīmējumu nevaram attiecināt. KL 177^1.pants lieto jēdzienu „svešas mantas vai tiesību uz šādu mantu, vai citu mantisku labumu iegūšana" pie kā būtu arī jāpieturas.[18]

Ja mēs rakstā minētās darbības pārceltu Latvijas vidē. Varētu konstatēt, ka izpildās KL 241.p. 1.d. paredzētā objektīvās puses pazīme – tika apieti konkrētās vietnes aizsardzības līdzekļi – tā tika "uzlauzta" un tikuši iegūti tās saturošie dati – svešam uzņēmumam piederošā bezķermeniska lieta – elektroniskās adreses. Protams, rakstā nav minēts, tas, cik liels kaitējums nodarīts. Turklāt, vēl no minētā raksta izriet, ka noziedzīgais nodarījums izdarīts organizētas grupas sastāvā "Pircēju datus nolaupīja grupējuma ar nosaukumu «*Goatse Security*» biedri.".

[16] Turpat – 233.lpp.
[17] Hakeri nozaguši augsti stāvošu "iPad" īpašnieku elektroniskās adreses.
http://www.apollo.lv/portal/news/articles/205775 [aplūkots 2010. gada 11. jūnijā]
[18] Intervija ar LU MII Tīkla risinājumu daļas vadītāja vietnieci K. Sataki 2010. gada 29. oktobrī.

Analizējot Latvijas *Neo* darbības, viņa darbībās ir saskatāmas tādas objektīvās puses darbības – kā VID EDS datu bāzes lejupielādēšana un valsts struktūru algu publiskošana sociālajā interneta vietnē *Twitter*. Risinot jautājumu, vai Neo jeb Ilmārs Poikāns ir saucams pie atbildības pēc Krimināllikuma 241. panta, ir jākonstatē, vai VID EDS pieder pie kritisko valsts IS kategorijas un papildus vai nodarītā kaitējuma apmērs sastāda tādu kaitējuma apjomu, par kuru personu var saukt pie atbildības. A. Buko uzskata, ka VID EDS piemīt kritiskas valsts IS pazīmes, kā arī, ka izmeklēšanai jāpamato būtiska kaitējuma esamība.[19]

Noziedzīgā nodarījuma subjekts ir fiziska un pieskaitāma persona, kas uz noziedzīgā nodarījuma izdarīšanas brīdi ir sasniegusi četrpadsmit gadu vecumu.

No subjektīvās puses dotajā pantā minēto noziedzīgo nodarījumu var izdarīt tikai ar nodomu – tiešu vai netiešu. Nevar netīšam apiet aizsargātu informācijas sistēmu vai veikt manipulācijas ar tajā esošiem aizsargātiem datiem radot ievērojamu mantisku kaitējumu.

2.2. Automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju

Krimināllikuma 243. panta 1. daļa sniedz definējumu automatizētas datu apstrādes sistēmas darbības traucēšanas noziedzīga nodarījuma sastāvam – automatizētā datu apstrādes sistēmā esošās informācijas neatļautu grozīšanu, bojāšanu, iznīcināšanu, pasliktināšanu vai aizklāšanu vai apzināti nepatiesas informācijas ievadīšanu automatizētā datu apstrādes sistēmā, ja ar to tiek bojāta vai iznīcināta aizsardzības sistēma vai radīts būtisks kaitējums. Krimināllikuma 243. panta 1. daļā paredzētais noziedzīgais nodarījums ir mazāk smags noziegums. Noziedzīgā nodarījuma sastāvs ir materiāls, jo paredz būtiska kaitējuma nodarīšanu. No objektīvās puses neatļautās darbības šajā daļā:

- grozīšana – izmaiņu izdarīšana, aizstājot kādu sistēmas elementu ar citu vai vairākiem citiem elementiem;
- bojāšana – darbība, kuras rezultātā, informācija daļēji zaudē savu sākotnējo kvalitāti, bet ir iespēja to atjaunot;
- iznīcināšana – iedarbība uz informāciju, kuras rezultātā tā vairs nav atjaunojama,
- pasliktināšana – iedarbība uz informāciju, kuras rezultātā tiek sabojāta tās struktūra, neciešot saturiskajam apjomam;

[19] Bakalaura darba Pielikums Nr.4

- aizklāšana – jebkura darbība, kas beidz pieeju sistēmai vai nu tāpēc, ka tie ir nodzēsti un fiziski vairs nepastāv, vai arī tie padarīti nepieejami un ekspluatācijai nederīgi;
- ievadīšana – apzināti nepatiesas informācijas ievadīšana, tās pievienošana, vai pārpludināšana ar datiem.[20]

Turklāt nepieciešams papildus konstatēt aizsardzības sistēmas bojājuma vai iznīcināšanas faktu vai būtiska kaitējuma faktu.

Krimināllikuma 243. panta 2. daļā paredzētais noziedzīgais nodarījums ir mazāk smags noziegums ar materiālu noziedzīgā nodarījuma sastāvu, no objektīvās puses neatļautās darbības ir papildinātas ar: pārnešanu, izdzēšanu, izmainīšanu. Un tiek prasīta zaudējumu konstatēšana lielos apmēros - nozieguma priekšmeta kopējā vērtība nodarījuma izdarīšanas brīdī nav mazāka par piecdesmit Latvijas Republikā noteikto minimālo mēnešalgu kopsummu.

Krimināllikuma 243. panta 3. daļā paredzētais noziedzīgais nodarījums ir smags noziegums ar materiālu noziedzīgā nodarījuma sastāvu, paredzēta atbildība, ja Krimināllikuma 243. panta 1. vai 2. daļā minētās darbības ir izdarījusi organizēta grupa, vai arī, ja tās izdarītas mantkārīgos nolūkos, vai tās izraisījušas smagas sekas.

Krimināllikuma 243. panta 4. daļā paredzētais noziedzīgais nodarījums ir smags noziegums ar materiālu noziedzīgā nodarījuma sastāvu, un paredz atbildību, ja Krimināllikuma 243. panta 1. vai 2. daļā minētās darbības ir vērstas pret valsts informācijas sistēmām.

Pie šāda veida nodarījuma varētu pieskaitīt arī "drazu pasta" sūtīšanu. Ar šādām "drazu pasta" tehnoloģijām var tikt palaistas ne tikai dažādas kaitīgās programmas, kas nosūta tā sūtītājam konkrētā datora lietotāja datus, bet arī šāda veida "pasts" pārpludina elektroniskās pasta sistēmas atmiņu, nemaz nerunājot par patērēto laiku parastai šādu vēstuļu dzēšanai. Tomēr saukt pie atbildības "drazu pasta" sūtītājus varētu būt praktiski neiespējams process, jo bieži vien "drazu pasta" darbībā ir iesaistīti ļoti daudzi robottīkli, nevis personas, un sākotnējo avotu atrast ir neiespējami. Vēl pie šajā pantā paredzētajiem nodarījumiem var pieskaitīt pakalpojuma atteices uzbrukumus, kad vienam un tam pašam serverim tiek nosūtīti vairāki pieprasījumi ar to savienoties, līdz tas nespēj vairs tikt galā ar šiem pieprasījumiem un "uzkarās".

Izpētot masu informācijas līdzekļus, kā piemēru, aplūkojamā Krimināllikuma panta ilustrācijai var minēt rakstu par kiberuzbrukumu ziņu aģentūrai LETA 2010. gada 30. septembrī

[20] Krastiņš U, Liholaja V., Niedre A. Krimināltiesības sevišķā daļa. Trešais papildinātais izdevums. Rīga: Tiesu namu aģentūra, 2009., 576.-577.lpp.

izmantojot pakalpojumu bloķēšanas metodi, kad vienlaicīgi sūtot no daudziem datoriem tieši uzbrukuma mērķa datoram daudzus pieprasījumus savienoties ar to, tika uz laiku paralizēta LETA`s IS darbība.[21]

Noziedzīgā nodarījuma subjekts ir fiziska un pieskaitāma persona, kas uz noziedzīgā nodarījuma izdarīšanas brīdi ir sasniegusi četrpadsmit gadu vecumu.

No subjektīvās puses dotajā pantā minēto noziedzīgo nodarījumu var izdarīt tikai ar nodomu – tiešu vai netiešu.

2.3. Nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm

Krimināllikuma 244. panta 1. daļa paredz tādu noziedzīga nodarījuma sastāva veidu kā nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm – tādas ierīces (arī datorprogrammas) neatļauta izgatavošana, pielāgošana, izmantošana, realizēšana, izplatīšana vai glabāšana, kura paredzēta automatizētas datu apstrādes sistēmas resursu ietekmēšanai nolūkā izdarīt noziedzīgu nodarījumu. Šajā panta daļā paredzētais noziedzīgais nodarījums ir mazāk smags noziegums. Šajā panta daļā paredzētais noziedzīgā nodarījuma sastāvs ir nošķelts, jo tajā ietvertas pazīmes, kas raksturo gatavošanos noziedzīgā nodarījuma izdarīšanai, kas vērsta uz to, lai iestātos vēlamās kaitīgās sekas, bet šīs sekas nav iekļautas konkrētā noziedzīgā nodarījuma sastāvā. Tiek paredzēta ierīces izgatavošana vai datorprogrammas uzrakstīšana, lai ar to pēc tam izdarītu citu noziedzīgu nodarījumu.

Šī panta otrā daļa paredz atbildību, ja šī paša panta pirmajā daļā minētās darbības izraisījušas smagas sekas un šajā daļā paredzētais noziedzīgais nodarījums ir smags noziegums. Šajā panta daļā paredzētā noziedzīgā nodarījuma sastāvs ir kvalificēts un materiāls, jo ir nepieciešama smagu seku konstatēšana.

Pie šī veida noziedzīgajiem nodarījumiem var pieskaitīt tādas darbības kā ļaunprātīgas programmatūras (*malware, malicious software*), datorvīrusu, kas ir ļaunprātīgas programmatūras paveids, rakstīšana un izplatīšana. Ļaunprātīga programmatūra ir speciāli radītas datorprogrammas nolūkā ietekmēt datorsistēmas un informācijas sistēmas, un radīt kaitējumu to īpašniekiem un / vai lietotājiem.

[21] Pirms vēlēšanām aģentūra LETA pārvar kiberuzbrukumu. http://www.apollo.lv/portal/news/articles/216089 [aplūkots 2010. gada 01. oktobrī]

Izpētot masu informācijas līdzekļus, kā piemēru, aplūkojamā Krimināllikuma panta ilustrācijai var minēt desmit „internetzagļu" no bijušajām PSRS valstīm sešu miljonu sterliņa mārciņu nozagšanas faktu no Lielbritānijas bankām. Noziedznieki izmantojuši datorvīrusus, ar kuru palīdzību inficējuši tūkstošiem datoru Lielbritānijā. Šī programma darbojās ļaujot noziedzniekiem piekļūt kredītiestādes parolēm, kas ļāva piekļūt banku rēķiniem lietojot internetu.[22]

Kā arī kā piemēru var minēt hakeru darbības, kuri piekļūstot tādām vietnēm kā *www.youtube.com* ievieš tajās kaitīgās programmas, un nezinoši lietotāji, kuri domā, ka, lai noskatītos attiecīgo viedo materiālu, tiem jāielādē kāda pazīstama programma, patiesībā ielādē kaitīgu programmatūru, kas ne tikai piekļūst attiecīgās personas datiem, bet arī dažos gadījumos sagrauj attiecīgo informācijas sistēmu. Eksperti konstatējuši, ka krāpnieciskie materiāli šajā vietnē augšupielādēti arī no Latvijas datoriem[23] Līdzīgi, jābūt uzmanīgiem arī sociālā tīkla "*Facebook*" lietotājiem, jo līdzīga situācija bija arī šī sociālā tīkla vietnē, kur lietotājam tika piedāvāta iespēja par brīvu ielādēt speciālu mediju programmu, kas ļauj noskatīties lietotājam vēlamo video, bet tiklīdz lietotājs piekrīt instalēt šo programmu, viņš ieinstalē kaitīgo programmatūru, kas var radīt negatīvas sekas lietotāja datiem, to datu aizsardzībai un arī neretu lietotāja datorsistēmai.[24]

Noziedzīgā nodarījuma subjekts ir fiziska un pieskaitāma persona, kas uz noziedzīgā nodarījuma izdarīšanas brīdi ir sasniegusi četrpadsmit gadu vecumu.

No subjektīvās puses dotajā pantā minēto noziedzīgo nodarījumu var izdarīt tikai ar nodomu – tiešu vai netiešu.

2.4. Datu, programmatūras un iekārtu iegūšana, izgatavošana, izmainīšana, glabāšana un izplatīšana nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām

Lai saprastu, kāds noziedzīgā nodarījuma sastāvs paredzēts Krimināllikuma 244^1. pantā, nepieciešams saprast, terminu – *elektronisko sakaru tīklu galiekārtas*. Elektronisko sakaru likums sniedz šādu skaidrojumu: galiekārtas - iekārtas (piemēram, tālruņa aparāti, faksi, modemi, datu

[22] Lielbritānijā par vērienīgu internetkrāpniecību apsūdzēti arī hakeri no Latvijas. http://www.apollo.lv/portal/news/articles/215980 [aplūkots 2010. gada 30. septembrī]
[23] Hakeri izgudrojuši shēmu, kā inficēt datorus caur "YouTube". http://www.apollo.lv/portal/news/articles/206049 [aplūkots 2010. gada 15. jūnijā]
[24] Noticis kārtējais uzbrukums "Facebook" lietotājiem. http://www.apollo.lv/portal/news/articles/204960 [aplūkots 2010. gada 06. martā]

pārraides iekārtas, privātās automātiskās telefonu centrāles, privātie tīkli, taksofoni), kas paredzētas tiešai vai netiešai pieslēgšanai publiskā elektronisko sakaru tīkla pieslēguma punktiem. Elektronisko sakaru tīklu galiekārtas pieder pie informācijas sistēmu veidojošiem fiziskajiem elementiem.

Krimināllikuma 244^1. pantā paredzētais noziedzīgais nodarījums - elektronisko sakaru tīklu galiekārtu identificēšanai elektronisko sakaru tīklā nepieciešamo datu izmainīšana vai par šādam nolūkam paredzētu datu iegūšana, glabāšana vai izplatīšana, kā arī par šādam nolūkam paredzētas programmatūras vai iekārtas iegūšana, izgatavošana, glabāšana vai izplatīšana bez ražotāja vai tā pilnvarotas personas piekrišanas, ja šādas darbības izdarītas mantkārīgā nolūkā vai ja tās izdarījusi personu grupa pēc iepriekšējas vienošanās, vai ja ar to radīts būtisks kaitējums – ir mazāk smags noziegums. Šajā pantā paredzētā noziedzīgā nodarījuma sastāvs atkarībā no gadījuma ir materiāls vai formāls. Noziedzīgā nodarījuma objektīvo pusi veido elektronisko sakaru tīklu galiekārtu identificēšanai elektronisko sakaru tīklā nepieciešamo datu izmainīšana bez ražotāja vai tās pilnvarotas personas piekrišanas vai šāda veida izmainīšanai paredzētu datu iegūšana / glabāšana, vai šim pašam nolūkam paredzētas programmatūras / iekārtas iegūšana, pagatavošana vai glabāšana.

Dotā panta sastāvs ir gandrīz līdzīgs Latvijas administratīvo pārkāpumu kodeksa 148^2. pantam, tikai LAPK dotā panta sastāvā netiek prasīta mantkarīga nolūka, personu grupas pēc iepriekšējas vienošanās vai būtiska kaitējuma konstatācija. Pēc aplūkojamā Krimināllikuma panta tiks kvalificēts arī tāds noziedzīgs nodarījums, ko persona izdarījusi atkāroti gada laikā, ja tā iepriekš tikusi administratīvi sodīta pēc Latvijas administratīvo pārkāpumu kodeksa 148^2. panta, kurš paredz atbildību par elektronisko sakaru tīklu galiekārtu identificēšanai elektronisko sakaru tīklā nepieciešamo datu izmainīšanu vai par šādam nolūkam paredzētu datu iegūšanu, glabāšanu vai izplatīšanu, kā arī par šādam nolūkam paredzētas programmatūras vai iekārtas iegūšanu, izgatavošanu, glabāšanu vai izplatīšanu bez ražotāja vai tā pilnvarotas personas piekrišanas.

Kā piemērus šāda veida noziedzīgai darbībai var minēt ierīces IMEI numura vai MAC adreses izmainīšanu to aizvietojot ar kādas citas galiekārtas numuru. Turklāt nav svarīgi, vai programmas un / vai ierīces ir tālāk izmantotas iedarbībai uz elektronisko sakaru galiekārtām, pietiek ar to vien, ka attiecīgās programmas un ierīces ir derīgas šādai iedarbībai. Aplūkojamā Krimināllikuma pantā minētais noziedzīgā nodarījuma sastāvs ir materiāls.

Noziedzīgā nodarījuma subjekts ir fiziska un pieskaitāma persona, kas uz noziedzīgā nodarījuma izdarīšanas brīdi ir sasniegusi četrpadsmit gadu vecumu.

No subjektīvās puses dotajā pantā minēto noziedzīgo nodarījumu var izdarīt tikai ar nodomu – tiešu vai netiešu.

2.5. Informācijas sistēmas drošības noteikumu pārkāpšana

Krimināllikuma 245. pants paredz noziedzīgu nodarījumu - informācijas sistēmas drošības noteikumu pārkāpšana. Šajā pantā paredzētā noziedzīgā nodarījuma sastāvs ir materiāls. Aplūkojamā pantā paredzētais noziedzīgais nodarījums ir kriminālpārkāpums. Atbildība par šajā pantā paredzētā noziedzīgā nodarījuma izdarīšanu iestājas, ja ir pieļauta informācijas režīma vai tās aizsardzībai izstrādātu informācijas glabāšanas un apstrādes noteikumu vai citu informācijas datorsistēmas drošības noteikumu pārkāpšana, ko izdarījusi persona, kura ir atbildīga par šo noteikumu ievērošanu, ja tas bijis par iemeslu informācijas nolaupīšanai, iznīcināšanai vai bojāšanai vai ja ar to radīts cits būtisks kaitējums. Noziedzīgā nodarījuma sastāvs ir materiāls. Aplūkojamā norma ir blanketa norma un satur norādes uz citiem normatīviem aktiem, kas paredz atbildību par šādu noteikumu pārkāpšanu, piemēram, uz Valsts informācijas sistēmu likumu vai nākotnē Informācijas tehnoloģiju drošības likumu.

Noziedzīgajam nodarījumam ir speciāls subjekts - fiziska un pieskaitāma persona, kas uz noziedzīgā nodarījuma izdarīšanas brīdi ir sasniegusi četrpadsmit gadu vecumu, un kurai ir uzticēta attiecīgās informācijas sistēmas drošība un kurai jārūpējas, lai tiktu ievēroti visi attiecīgajai informācijas sistēmai piemērojamie drošības standarti. No subjektīvās puses dotajā pantā minēto noziedzīgo nodarījumu var izdarīt tīši un aiz neuzmanības, bet attieksme pret sekām izpaudīsies noziedzīgas nevērības formā.[25] Noziedzīgās nevērības objektīvais kritērijs nozīmē, ka personai jāievēro savas profesijas, specialitātes vai nodarbošanās noteikumi, kas tiek prasīti, lai nepieļautu kaitīgo seku iestāšanos.[26]

Valsts informācijas sistēmu likums paredz Valsts IS turētāja atbildību par datu drošību un aizsardzību. Valsts IS turētājs – valsts IS pārzinis vai pilnvarota institūcija, kas uztur sistēmas funkcionalitāti un nodrošina informācijas apriti. Savukārt šis pārzinis ir tiesīgs iecelt

[25] Krastiņš U, Liholaja V., Niedre A. Krimināltiesības sevišķā daļa. Trešais papildinātais izdevums. Rīga: Tiesu namu aģentūra, 2009., 587.lpp.
[26] Krastiņš U, Liholaja V., Niedre A. Krimināltiesības vispārīgā daļa. Trešais papildinātais izdevums. Rīga: Tiesu namu aģentūra, 2008., 174.lpp.

pārvaldnieku vai vairākus pēc nepieciešamības katrai IS atsevišķi, kas ietilpst pārziņa kompetencē. Tieši atbildīgs šajā gadījumā ir Valsts IS drošības pārvaldnieks – fiziska sertificēta persona, ja tā ar savu darbību vai bezdarbību ir pieļāvusi kaitīgo seku un kaitējuma iestāšanos, tātad iespējamais šāda veida noziedzīgu nodarījumu subjekts ir arī Valsts IS drošības pārvaldnieks, lai arī Krimināllikumā nav paredzēta atbildība tieši par bezdarbību. Bet, tas nenozīmē, ka IS drošības pārzinis būs atbildīgs pilnīgi visos gadījumos, kad viņa pārvaldībā esošā IS tiks kompromitēta. Persona, kura ir atbildīga par IS drošību nesīs atbildību par šajā pantā paredzētajām darbībām, tikai tad, ja tā noignorēs potenciālos draudus IS, vai kaut kādu iemeslu dēļ neievēros attiecīgai sistēmai paredzētos nepieciešamos drošības noteikumus un tiks konstatēts, ka dēļ šo noteikumu neievērošanas IS ir kompromitēta. K. Sataki norāda, ka šādas situācijas var rasties gadījumos, kad netiek veikts nepārtraukta IS uzraudzība.[27]

Vai būtu saucams tādā gadījumā IS drošības pārvaldnieks par bezdarbību, ja tā pārvaldītā informācijas sistēma tiek kompromitēta? U. Ķinis uzskata, ka ir bīstami padarīt IS drošības pārvaldniekus par potenciālajiem noziedzniekiem, pieļaujot to darbībās neuzmanību kā vainas formu, turklāt, tas būtu arī rupjš Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas pārkāpums, jo neviena valsts pasaulē nav spējīga izstrādāt tādus IS drošības noteikumus, lai to piemērošanas gadījumā līdz minimumam samazinātu apdraudējumus visām valstī esošām IS.[28] Darba autore nepiekrīt viedoklim, ka par IS drošību atbildīgā persona nenes atbildību par to, ka tās pārziņā esošā IS tiek kompromitēta. Tas nozīmētu tikai to, ka, drošības pārzinis varētu vispār nepildīt savus pienākumus un visā tiktu vainoti tikai hakeri. Jāievēro arī cilvēciskais faktors un cilvēku vada emocijas. Protams, tas nenozīmē, ka jāieslīgst galējībās, un būtu jāizvērtē, kādu iemeslu dēļ radušās noziedzīgā nodarījuma sekas – vai informācija tikusi kompromitēta dēļ tā, ka serverī iespēris zibens vai arī dēļ tā, ka IS ielauzusies persona, kurai nebija attiecīgās pilnvaras tai piekļūt. IS drošības pārvaldnieka atbildības pakāpe būtu jāizvērtē jebkurā informācijas sistēmas apdraudējuma gadījumā, it īpaši, ja ielaušanās sistēmā notiktu vairākkārtīgi, vai nerastos jautājums par bezdarbību un informācijas sistēmas drošības noteikumu pārkāpšanu, par ko ir paredzēta krimināltatbildība. A. Buko norāda: "*šim jautājumam ir vairāki aspekti. Pirmkārt, par IT drošību iestādē atbild iestādes vadītājs vai īpaši pilnvarota persona (piemēram, drošības pārvaldnieks valsts IS gadījumā). Otrkārt, ir jānodala tās sistēmas, kurām IT drošība kā īpašs režīms ir obligāts pienākums (piemēram, Valsts IS, bankas IS), un sistēmas, kuru drošības režīmu*

[27] Intervija ar LU MII Tīklu risinājumu daļas vadītāja vietnieci K. Sataki 2010. gada 29. oktobrī.
[28] Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007., 200.lpp.

un risku analīzi nosaka pats īpašnieks (piemēram, privātajā sektorā). Treškārt, līdz informācijas tehnoloģiju drošības likuma spēkā stāšanos, par IT drošību valstiskā līmenī atbild vairākas institūcijas (politiski – Satiksmes ministrija (izriet no Elektronisko sakaru likuma); RAPLM (izriet no VIS likuma); valsts pārvaldē – Datu valsts inspekcija; noziedzīgu nodarījumu prevencijā – Valsts policija un Drošības policija)."

2010. gada 28. oktobrī Saeima 3. lasījumā izskatīja un pieņēma jaunu Informācijas tehnoloģiju drošības likumu, kurš paredzams stāsies spēkā 2011. gada 1. februārī. No likuma projekta teksta izriet, ka likums būs saistošs ne tikai valsts un pašvaldību institūcijām, bet arī komersantiem un citām privāto tiesību juridiskajām personām.

2.6. Citu tiesību normu nošķiršanas problēmas

Bez iepriekš aplūkotajiem Krimināllikuma pantiem (KL 241. – 245.p.) Krimināllikumā ir atrodami neskaitāmi panti, kas pēc sava rakstura ir līdzīgi noziedzīgiem nodarījumiem informācijas sistēmu drošības jomā, bet, kuru apdraudējuma objekts ir cits.

Piemēram, Krimināllikuma 144. pants - Korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšana. Attiecībā par šo pantu U. Ķinis vērš uzmanību, ka, lai arī šis pants pēc sava satura ir līdzīgs KL 241.p. sastāvam, galvenā atšķirība šeit ir tajā, ka KL 144.p. nodarījuma izdarīšanai, informācija tiek iegūta neatļauti pieslēdzoties vai nu telekomunikācijām vai datorsistēmai, pārtverot pārraidīto datu saturu, nevis, kā KL 241.p. – realizējot piekļuvi, izmantojot trūkumus esošajā informācijas sistēmas drošībā, atklājot piekļuves kodus vai paroles. [29]

Krimināllikuma 177.[1]p. Krāpšana automatizētā datu apstrādes sistēmā. Attiecībā uz šo pantu ir pieejams Latvijas Republikas Augstākās tiesas Senāta Krimināllietu departamenta 2006. gada 11. septembra lēmums lietā SKK – 410/2006.[30] Ar šo spriedumu tika norādīta Krimināllikuma 177.[1] panta īpašā nozīme.

Sākotnēji Ar Valmieras rajona tiesas 2005.gada 30.marta spriedumu R.G. un A.Ļ. atzīti ar vainīgiem sodīti pēc Krimināllikuma 175. panta 3.daļas ar brīvības atņemšanu uz 3 gadiem bez

[29] Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007., 144.-145..lpp.
[30] Latvijas Republikas Augstākās tiesas Senāta Krimināllietu departamenta 2006. gada 11. septembra lēmums lietā SKK – 410/2006.

mantas konfiskācijas. A.Ļ., būdams agrāk sodīts par zādzības izdarīšanu, par ko sodāmība nav dzēsta un noņemta likumā noteiktā kārtībā, atkārtoti 2004.gada 23.novembrī ap plkst.19:00 ieradās Valmierā, [..], SIA „[A]" spēļu zālē „[B]", kur, darbodamies personu grupā pēc iepriekšējas vienošanās ar R.G., nelikumīgi no glabātavas – spēļu automāta kopīgi (*viens veica nelikumīgas darbības ar spēļu automātu, bet otrs tajā laikā uzmanīja, lai citas personas neievērotu zādzības izdarīšanu*) slepeni nozaga SIA „[A]" piederošo naudu Ls 102,30. Zādzību izdarīja sekojošā veidā: izmantojot to, ka spēļu automātam Nr.18 no aizmugures var piekļūt pie elektrības izslēgšanas - ieslēgšanas slēdža, veica nelikumīgas darbības, no automāta iegūstot naudu, proti, iemetot spēļu automātā monētu, vienlaicīgi nospieda pogu „naudas izmaksa" un atslēdza automātu no elektrības padeves, kā rezultātā, rodoties spēļu automātā strāvas padeves pārtraukumam, nauda izkrita, pēc tam, atkal ieslēdzot automātu kredītpunkti, kas tika doti par vienu naudas vienību, tika saglabāti uz ekrāna un tādējādi, atkal veicot iepriekšminētās darbības, viņi atkārtoti ieguva naudu. Iepriekš minētās darbības A.Ļ. un R.G. 2004.gada 23.novembrī veica vairākkārtīgi, kopā nozogot naudu Ls 102,30 apmērā. Šādas darbības abi veica vairākkārt. Prokurors dotajā lietā piekrita U. Ķiņa viedoklim - „tiesu spriedumos aprakstītais iekļūšanas veids mantas glabātavā un naudas iegūšana neatbilst Krimināllikuma 175. panta sastāva objekta un subjektīvās puses pazīmēm. Savu apgalvojumu prokurors pamato ar to, ka Krimināllikuma 177. pants neaizliedz automatizēto ierīci atzīt par krāpšanas objektu. No subjektīvās puses šajā gadījumā, apsūdzētie ar viltu, t.i., uzdodot automatizētai sistēmai izmaksāt kredītpunktus skaidrā naudā, un automatizētai ierīcei pieņemot lēmumu izmaksāt atbilstoši kredītpunktu skaitam naudas vienību, tās izsniegšanas brīdī, iedarbojas uz automatizēto sistēmu, atslēdzot un atjaunojot tai strāvas piegādi, kā rezultātā automatizētā sistēma saglabā kredītpunktus, pēc kuras jau ir notikusi naudas izmaksa un apsūdzētie prettiesiski iegūst tiesības uz kredītpunktiem, kurus, atkārtojot izklāstītās darbības, turpina izņemt no automatizētās ierīces – spēļu automāta, skaidrā naudā. Pie izklāstītiem apstākļiem notiek nevis naudas iegūšana iekļūstot glabātavā, bet gan, izkrāpjot automatizētai iekārtai kredītpunktus, t.i., tiesības uz šo kredītpunktu izmaksu skaidrā naudā ar turpmāku šo kredītpunktu saglabāšanu automatizētā ierīcē." [31]

Tāpat nepieciešams minēt arī KL 193.[1]p. Datu, programmatūras un iekārtu iegūšana, izgatavošana, izplatīšana, izmantošana un glabāšana nelikumīgām darbībām ar finanšu instrumentiem un maksāšanas līdzekļiem, KL 288.p. Telekomunikāciju iekārtu, radio un

[31] Ķinis U. Kibernoziegumi un kriminālprocess. Jurista Vārds" 27.02.2001. 5 (198)

televīzijas raidītāju un pasta tehnoloģisko iekārtu bojāšana, KL 305.p. Personu speciālās aizsardzības noteikumu pārkāpšana; pantu esamību. KL 145.p. Nelikumīgas darbības ar fiziskās personas datiem, KL 148.p. Autortiesību un blakustiesību pārkāpšana, KL 149.p. Nelikumīgas darbības ar autortiesību un blakustiesību objektiem.

U. Ķinis norāda arī, ka svarīgi norobežot patvaļīgu piekļūšanu datu apstrādes sistēmai (KL 241.p.) no zādzības, saistītas ar iekļūšanu dzīvoklī vai citā telpā vai glabātuvē (KL 175.p. 3.d.), jo Informācijas sistēma ar visu tās resursu kopumu arī nereti tiek uzskatīta par konteineru, kur glabājas informācija.[32] Līdzīgi arī, ja persona prettiesiski iekļūst telpā, kurā atrodas datorsistēma, nodarījums tiek kvalificēts pēc KL 175. panta 3. daļas, tādējādi, KL 241.p. izpratnē patvaļīga piekļuve nenozīmē personas veiktās fiziskās darbības iekļūstot telpā, kurā atrodas datorsistēma, jo šajā pantā piekļuve tiek īstenota attālināti.[33]

Arī KL 88.p. 2.d. terorisma objektīvā puse izpaužas kā valsts teritorijā vai kontinentālajā šelfā izvietotu fizisku objektu, automatizēto datu apstrādes sistēmu, elektronisko tīklu, kā arī citu objektu, kuru mērķis ir nodrošināt valsts drošību, iznīcināšanu vai bojāšanu.[34] U. Krastiņš norāda, ka terorisms pēc savas būtības ir vairākobjektu nodarījums, kas apdraud LR valsts drošību un ekonomisko sistēmu. Tajā pat laikā apdraud cilvēku dzīvību un veselību, viņu mantu, uzņēmumu, iestāžu un organizāciju normālu darbību, vispārējo drošību un sabiedrisko kārtību.[35] KL 88.p. minētā terorisma subjektīvās puses pazīme ir nolūks iebiedēt iedzīvotājus vai piespiest valsti, tās institūcijas vai starptautiskas organizācijas izdarīt kādu darbību vai atturēties no tās, vai kaitēt valsts, tās iedzīvotāju vai starptautiskas organizācijas interesēm (terorisms). U. Ķinis norāda: „*valstīs, kur visa ekonomika, politika un sadzīve ir atkarīga no informācijas un komunikācijas tehnoloģiju darbības, noziedznieks ar tastatūras palīdzību piecu minūšu laikā var iznīcināt valsts ekonomiku un radīt īstu paniku iedzīvotājos*".[36]

Šajā apakšnodaļā aplūkoto noziedzīgo nodarījumu tiešais objekts nav informācijas sistēmu drošība, šajos gadījumos dators tiek izmantots kā rīks šo noziedzīgo nodarījumu izdarīšanai.

[32] Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007., 143.lpp.
[33] Turpat – 209.lpp.
[34] Krastiņš U, Liholaja V., Niedre A. Krimināltiesības sevišķā daļa. Trešais papildinātais izdevums. Rīga: Tiesu namu aģentūra, 2009., 47.lpp.
[35] Turpat - 46.lpp.
[36] Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007., 232.-233.lpp.

3. Noziedzīgu nodarījumu informācijas sistēmu drošības jomā kriminoloģiskie aspekti

Lai pilnīgāk izprastu noziedzīgo nodarījumu informācijas sistēmu drošības jomā pastāvošo stāvokli uz doto brīdi, nepieciešams izpētīt vispārīgo kibernoziegumu izplatības stāvokli un tendences Latvijas Republikā, jo noziedzīgie nodarījumi informācijas sistēmu drošības jomā ir vispārējo kibernoziegumu neatņemama sastāvdaļa un ir skaidrs, ka Latvija nebūt nav vadošā valsts, no kuras nāk pasaules primārais kiberapdraudējums.

3.1. Noziedzīgu nodarījumu informācijas sistēmu drošības jomā stāvokļa un izplatības raksturojums

Latvijā interneta segmenta attīstība vērojama četros virzienos – sociālo resursu jomā, e-komercijas jomā, informācijas portālu jomā un datu apmaiņas jomā. Sociālo tīklu jomas attīstība paaugstina riskus personu fizisko datu zādzības no informācijas sistēmām attīstībai. Savukārt e-komercijas resursu attīstība veicina maksāšanas līdzekļu datu zādzību/pārtveršanu attīstību no kredītiestāžu un tirdzniecības uzņēmumu informācijas sistēmām, piemēram, tās uzlaužot vai šos datus iegūstot ar ļaunprātīgu programmu palīdzību.[37]

Saskaņā ar Informācijas centra[38] rīcībā esošo 2007. gada kriminālo statistiku, 2007. gadā tikuši reģistrēti 55620 noziedzīgi nodarījumi, no kuriem pēc Krimināllikuma XX nodaļā esošās grupas objekta "Noziedzīgi nodarījumi pret vispārējo drošību un sabiedrisko kārtību", pie kura pieder arī tieši noziedzīgi nodarījumi informācijas sistēmu drošības jomā, Latvijas Republikā reģistrēti 2821 noziedzīgi nodarījumi.

Valsts policija savā 2007. gada pārskatā ir norādījusi uz vairākām kibernoziegumu tendencēm. Īpaši norādot uz to starptautisko raksturu, atzīmējot to, ka 90 % no tiem ir latenti.

Arvien izplatītāka kļūst nelikumīga autortiesību un blakustiesību objektu apmaiņa, izmantojot failu apmaiņas programmas. Minēto darbību veikšanas paņēmieni tiek nepārtraukti pilnveidoti, ar katru gadu failu apmaiņas protokoli (programmas) tiek modificēti, iegūstot jaunu veidolu un darbības principus, tādējādi, cenšoties apiet tiesību normās pieņemto nelikumīgo darbību sastāvu. Jāatzīmē, ka nelikumīga failu lejupielādēšana tiek uzskatīta par nesodāmu, tāpat

[37] Skolēns ar vienu klikšķi var pakļaut skolu kiberuzbrukumiem. http://www.apollo.lv/portal/news/articles/216479 [aplūkots 2010. gada 22. oktobrī]
[38] LR IeM Informācijas centrs. Kriminālā statistika. http://www.ic.iem.gov.lv/?q=lv/node/75 [aplūkots 2010. gada 20. oktobrī]

kā lielākajā daļā sabiedrības nav izpratnes par audio un video failu likumīgu atrašanos uz informācijas nesējiem (datoru cietie diski, zibatmiņas, atmiņas kartes, MP3 atskaņotāji). Izplatīts ir uzskats, ka nopērkot darbu, ar to var tālāk rīkoties pēc saviem ieskatiem. Jāatzīmē, ka nelikumīgu autortiesību un blakustiesību objektu izmantošanu arvien vairāk veic pusaudži un jaunieši, kuri par vieglas peļņas avotu uzskata datorprogrammu lejupielādēšanu internetā un to pārdošanu vai piedāvāšanu uzstādīt „klientu" datorsistēmās. Kopumā vērojama arī pavirša datorprogrammu lietotāju attieksme pret programmatūru, to uzstādīšanas, izmantošanas un citiem licencēšanas nosacījumiem. Ir daudz uzņēmumu, kuros tiek legāli izmantotas attiecīgās jomas bāzes programmas, taču atbalsta programmas, kuras ir daudz vienkāršākas un lētākas, vairumā gadījumu datorsistēmās atrodas nelikumīgi. 2007.gadā kopumā veiktas aptuveni 150 resoriskās pārbaudes uzņēmumu saimnieciskās darbības veikšanas vietās.

Veiktas aptuveni 40 resoriskās pārbaudes dažādās Rīgas un citu Latvijas pilsētu audiovizuālo objektu izplatīšanas vietās un publiskā izpildījuma vietās (videonomās, tirgos, veikalos, klubos, bāros), kā arī tika kontrolētas nepieciešamās atļaujas saistībā ar publisko izpildījumu. Apmēram 70% gadījumos no veiktajām pārbaudēm tika uzsākti kriminālprocesi, pārējos gadījumos tika sastādīti protokoli par administratīvo pārkāpumu. 2007.gadā šajā jomā notika aktīva sadarbība ar RGPP, citām VP teritoriālajām iestādēm, VID un Valsts darba inspekciju.[39]

Saskaņā ar Informācijas centra rīcībā esošo 2008. gada kriminālo statistiku, 2008. gadā tikuši reģistrēti 57475 noziedzīgi nodarījumi, no kuriem pēc Krimināllikuma XX nodaļā esošās grupas objekta "Noziedzīgi nodarījumi pret vispārējo drošību un sabiedrisko kārtību", pie kura pieder arī tieši noziedzīgi nodarījumi informācijas sistēmu drošības jomā, Latvijas Republikā reģistrēti 3876 noziedzīgi nodarījumi.

Savukārt Valsts policijas 2008. gada publiskajā pārskatā[40] tiek atzīmēts, ka Pieaudzis kibernoziegumu skaits. To veicina interneta lietotāju skaita pieaugums, internetā piedāvātās iespējas un šo noziegumu latentums. Lielākais pieaugums ir vērojams tādos noziedzīgo nodarījumu veidos kā krāpšana internetā, nodarījumi, pārkāpjot interneta lietotāju konfidencialitātes intereses, personas datu nolaupīšana un izmantošana (pārsvarā dati par bankas kontiem un kredītkartēm), noziedzīgi iegūtu līdzekļu legalizācija alternatīvajās maksāšanas sistēmās, komerciālā bērnu pornogrāfija, datorprogrammu aizsardzības pārvarēšana, noziegumi

[39] Valsts policijas 2007. gada pārskats. http://www.vp.gov.lv/?sadala=189 [aplūkots 2010. gada 01. oktobrī]
[40] Valsts policijas 2008. gada pārskats. http://www.vp.gov.lv/?sadala=189 [aplūkots 2010. gada 01. oktobrī]

komunikāciju sfērā u.c. Kibernoziegumi lielākoties ir starptautiska rakstura un saistīti ar organizētām grupām, kā arī tiek izdarīti mantkārīgos nolūkos. Ar interneta vispārējo pieejamību, nepārtraukto attīstību un lietotāju skaita pieaugumu, iesaistot e-pakalpojumu izmantošanā lietotājus ar virspusējām datu drošības zināšanām. Palielināsies cietušo skaits mantiska rakstura nodarījumos, kuros tiks pielietoti informācijas tehnoloģijas resursi un tīklu nepietiekamās aizsardzības dēļ tiks būtiski traucēta personu identificēšana. Kibertehnisko ekspertīžu nodaļā reģistrēto ekspertīžu skaits saskaņā ar Informācijas sistēmas LATAFIS datiem sasniedz 492 ekspertīzes, kas ir par 163 ekspertīzēm vairāk nekā 2007. gadā.

Saskaņā ar Informācijas centra rīcībā esošo 2009. gada kriminālo statistiku, 2009. gadā tikuši reģistrēti 56748 noziedzīgi nodarījumi, no kuriem pēc Krimināllikuma XX nodaļā esošās grupas objekta "Noziedzīgi nodarījumi pret vispārējo drošību un sabiedrisko kārtību", pie kura pieder arī tieši noziedzīgi nodarījumi informācijas sistēmu drošības jomā, Latvijas Republikā reģistrēti 3530 noziedzīgi nodarījumi.

Savukārt 2009. gadā, saskaņā ar Valsts policijas publicēto informāciju pieaudzis pārkāpumu skaits Intelektuālā īpašuma tiesību aizsardzības jomā. Pasliktinoties ekonomiskajai situācijai valstī, komersanti līdzekļu taupības nolūkā izvēlas lietot nelicencētas datorprogrammas, nepagarinot licenču darbības termiņu, instalējot programmas neatbilstošam datoru skaitam un dažādos citos veidos mēģinot apiet licencēšanas noteikumus un autortiesību ievērošanu. Ja iepriekšējos gados lielākā daļa nelikumīgo datorprogrammu lietotāji bija komersanti, kas saistīti ar būvniecību, tad 2009.gads iezīmē visai negatīvas tendences visa veida un profila uzņēmumos. Palielinās arī iesniegumu skaits par Latvijā radītu autortiesību un blakustiesību objektu nelikumīgu izmantošanu - datorprogrammas, datu bāzes, filmas, mūzika, literatūra u.c. Turpina samazināties audio vizuālās produkcijas ievešana no citām valstīm, tai skaitā no Krievijas. 2009. gadā salīdzinot ar 2009. gadu samazinājies Infotehnisko ekspertīžu nodaļā veikto ekspertīžu skaits no 847 veiktām ekspertīzēm uz 587 veiktām ekspertīzēm.[41] Tāpat arī pārskatā norādīts, ka 2010. gadā jau VP štats samazināts par 1678 vienībām, kas negatīvi ietekmēs VP darbību un noziedzīgu nodarījumu atklāšanas kapacitāti. Un tomēr kā viens no galvenajiem 2010. gada VP darbības virzieniem ir intelektuālā un rūpnieciskā īpašuma tiesību aizsardzības jomā, kā arī kibernoziegumu novēršanai un apkarošanai. Kā viens no administratīvā darba prioritārajiem virzieniem norādīts datortehnikas un datortīkla drošības un izmantošanas normatīvo aktu

[41] Valsts policijas 2009. gada pārskats. http://www.vp.gov.lv/?sadala=189 [aplūkots 2010. gada 04. oktobrī]

pilnveidošana, kā arī informātikas un komunikācijas tehnoloģiju apkalpošanas kārtības atbilstoši ITIL standartam ar atbilstošu sistēmu dokumentāciju – konfigurāciju datu bāzi sakārtošana, rezerves kopēšanas politiku, sistēmas atjaunošanas plāniem; e-pasta infrastruktūras drošības pilnveidošana.

Aplūkojot publiski pieejamo tiesu statistiku[42] no 2005. gada, secināms, ka visā šajā laika periodā līdz šim brīdim neviens Latvijas Republikā nav reāli notiesāts par noziedzīga nodarījuma izdarīšanu, kas apdraud informācijas sistēmu drošību. Ja neskaita bakalaura darbā iepriekš pieminēto Rīgas pilsētas Centra rajona tiesas 2004. gada 8. marta spriedumu, kas tomēr vēlāk tika atcelts pilnībā ar Latvijas Republikas Augstākās tiesas Senāta Krimināllietu departamenta 2006. gada 18. janvāra lēmumu lietā SKK – 01- 0007/06. Kriminālprocesa taisnīgs noregulējums var būt sasniegts ne tikai ar tiesas spriedumu, bet arī ar prokurora priekšrakstu par sodu vai izlīgumu.

Veicot atsevišķu pieprasījumu LR IeM Informācijas Centram izdevās iegūt sekojošu informāciju par reģistrētajiem noziedzīgajiem nodarījumiem informācijas sistēmu drošības jomā pēc Krimināllikuma 241.-245.p., laika posmā no 2007.gada līdz 2010.gada 9 mēnešiem:

KL pants	**Gads**			
	2007.g.	**2008.g.**	**2009.g.**	**2010.g. 9 mēn.**
241.p.	2	1	2	-
243.p.	1	1	2	1
244.p.	-	-	2	1
245.p.	1	-	-	-

2. tabula: uzsākto noziedzīgu nodarījumu informācijas sistēmu drošības jomā statistika

Šie dati norāda uz to, ka neskatoties uz lielajiem skaitļiem statistikas datos vērtējot noziedzīgu nodarījumu izplatību pēc Krimināllikuma XX nodaļas, tie nemaz neatspoguļo reālo noziedzīgu nodarījumu informācijas sistēmu drošības jomā izplatību. Šeit izpaužas šīs noziedzīgo nodarījumu grupas latentums, pat, ja tiek veiktas darbības, par kurām paredzēta atbildība aplūkojamos krimināllikuma pantos, cilvēki par to nemēdz ziņot, jo dažreiz šie noziedzīgie nodarījumi ir paša cietušā nepamanīti.

V. Drivinieks norāda uz neziņošanu par informācijas sistēmu apdraudējumiem kā iemeslu šo noziedzīgo nodarījumu latentumam: "*Baumas par to, ka kādas bankas datu aizsardzība tiek apieta, izdarīs bankai vairākas reizes lielākus zaudējumus, nekā nozagtā summa. Bankas klienti*

[42] Latvijas tiesu portāls. http://www.tiesas.lv/index.php?id=2044 [aplūkots 2010. gada 20. oktobrī]

vienkārši šīm bankām neticēs, it īpaši Latvijā, kur ir bankas ar sliktu datu aizsardzības reputāciju. Tāpēc šāda tipa noziegumi arī netiks atklāti, jo bankai ir izdevīgāk nomainīt tīkla administratoru un atgriezt personai nozagto naudu, nevis griezties policijā."[43] Interneta lietotāji līdz ar to ir vairāk apdraudēti internetā, jo mūsdienu digitālās noziedzības pazīme ir tieši privātu datu, identitātes un paroļu zagšana, kas paver iespējas citu noziedzīgu nodarījumu, piemēram, krāpšanas izdarīšanai. Tautā pastāv teiciens, ka zinātne virza progresu, jāteic, ka, piemēram, ļaunprātīgu programmu, to skaitā datorvīrusu, rakstīšana pati par sevi liek programmētājiem radīt jaunākus un jaunākus veidus, kā pilnveidot un attīstīt programmatūru un aizsardzības iespējas. Vēršoties pret informācijas sistēmu konfidencialitāti, integritāti un pieejamību, tās resursi var kļūt nepieejami vai darboties daudz lēnāk nekā parasti, piemēram, ielaužoties sistēmā un svešas sistēmas resursus lietojot, lai uzturētu robotu tīklu vai "aizņemoties" informācijas resursus, lai parazītiskā veidā darbinātu savu programmatūru.

3.2. Noziedzīgu nodarījumu informācijas sistēmu drošības jomā seku raksturojums

Sekas ir rezultāts, kas rodas izpildot dažādas darbības. Sekas var būt gan pozitīvas gan negatīvas. Piemēram, neuzlādējot mobilā tālruņa bateriju, sekas ir tādas, ka nebūs pieejama mobilo sakaru komunikācija, iespējams brīdī, kad tā būs ļoti nepieciešama. Runājot par kibernoziegumu, to skaitā noziedzīgu nodarījumu, kas vērsti pret informācijas sistēmu drošību, izraisītajām sekām, nepieciešams konstatēt cēloņsakarību, kādā vidē šīs sekas rodas, un novērtēt seku radītos kopejos zaudējumus, kā arī izvērtēt vai ir radīts būtisks kaitējums kādām interesēm un vai šis veiktās darbības ir atzīstamas par prettiesiskām.

Noziedzīgu nodarījumu informācijas sistēmu drošības jomā radītās sekas rodas gan virtuālajā vidē, gan reālajā pasaulē. Cilvēks, kas sēž pie datora darbojoties interneta vidē atrodas divas pasaulēs – vienā, kurā viņš guļ, elpo, uzņem barību, un datorpasaulē, kurā biti tiek pārvērsti attēlos, skaņās, sistēmās. Iedarbojoties uz bitiem, ir loģiski izsecināt, ka iespaids tiek atstāts arī uz citu personu – bērnu, programmētāju, mājsaimnieci, valsts prezidenta kanceleju, kas atrodas pie cita datora kādā citā zemeslodes vietā. Šis atstatais iespaids ir sekas.

Saskaņā ar Starptautiskās datornoziedzības komitejas datiem datornoziegumi rada nopietnu apdraudējumu jebkurai organizācijai, kuras rīcībā ir datortehnika, turklāt tai draud arī

[43] Drivinieks V. Kibernoziegumi. Bakalaura darbs. Rīga: Latvijas Universitāte, 2009., 5.lpp.

nozīmīgi materiāli zaudējumi. Saskaņā ar aprēķiniem, elektroniskās skaitļošanas sistēmas sabojāšana noziedzīga nodarījuma dēļ pat vislielākajai bankai var beigties ar bankrotu četru dienu laikā.[44]

U. Ķinis norāda, ka noziedzīgos nodarījumos pret informācijas sistēmu drošību sekas iedalāmas divās kategorijās – mantiskās sekas, kas izpaužas konkrētu zaudējumu nodarīšanā sistēmas īpašniekam vai tiesiskajam valdītājam, vai datu subjektam, šādas sekas ir paredzētas arī attiecīgajos krimināllikuma pantos; fiziskās sekas – datu apstrādes sistēmu darbības fiziska sagraušana vai darbības traucēšana. [45]

Bakalaura darba autore uzskata, ka svarīgas ir arī sociālās un kognitīvās sekas, kuras atstāj vai var atstāt noziedzīgi nodarījumi informācijas sistēmu drošības jomā tieši cietušās personas uztverē, piemēram, izmaiņas domāšanā vai turpmāka neuzticēšanās. Daudziem, no aptaujātajiem cilvēkiem, ir palikušas spilgti izteiktas negatīvas atmiņas par piedzīvotu naudas iztrūkumu no konta veicot nedrošas preces pirkumu internetā. Savukārt, uzņēmumi zaudē iegūto reputāciju un klientu uzticību.

Inovatīvu IT drošības risinājumu biznesa tīkla attīstītājs Andris Soroka norāda: „*ka jebkura datu noplūde var tikt finansiāli novērtēta. Visā pasaulē jau ir dažādas iestādes, kas veic katras datu noplūdes novērtējumu, un, ja piemēram, VID EDS datu noplūdi ir grūti novērtēt, tad ASV, Lielbritānijā, Vācijā un citur ikviens datu noplūdes fakts ir izteikts naudas vienībā.*"[46]

Latvijā šobrīd nav institūcijas, kas specializētos informācijas sistēmu drošības incidentu seku aprēķināšanā, šis uzdevums ir jāveic cietušajai pusei, kura apgalvo, ka tai ir radušies tieši vai netieši zaudējumi noziedzīga nodarījuma informācijas sistēmu drošības jomā rezultātā.

3.3. Noziedzīgu nodarījumu informācijas sistēmu jomā subjektu raksturojums

Kā norāda Eduardo Gelbšteins un Ahmads Kamals – ANO izdotā kiberdrošības ceļveža[47] autori norāda, ka informācijas sistēmu drošības apdraudējums apdraud ne tikai mieru un drošību, bet arī cilvēka darba

[44] [B.a.] Mācību grāmata. Kriminoloģija. [B.v.] Nordik, 2004., 340.lpp.
[45] Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007., 163.lpp.
[46] A. Soroka. Vai kibernoziedzība ir nopietns drauds Latvijas attīstībai. http://www.saki.lv/viedokli/462-vai-kibernoziedzba-ir-nopietns-drauds-latvijas-attstbai [aplūkots 2010. gada 09.septembrī]
[47] Information Insecurity.
http://www.un.int/kamal/information_insecurity/Information_Insecurity_Second_Edition_PDF.pdf [aplūkots 2010. gada 21. oktobrī]

augļus. Galvenais šī apdraudējuma aspekts izriet no noziedzīgās motivācijas dabas un tās izplatības. Ir virtuāli neiespējami novērot motivāciju, jo tā ir daudzpusīga, neredzama un pārsvarā neatklājama. Problēmas būtība slēpjas apstāklī, ka motivēti indivīdi ir ārkārtīgi radoši. Viņu radošums ir saskatāms pat viņu daudzslāņainajā motivācijā. Tāpēc, zagļa motivācija vienmēr būs lielāka par izmeklētāja motivāciju. Noziedznieks vienmēr ir pāris soļus priekšā izmeklētājam. Kamēr likums iedarbosies caur tā nebeidzamajiem lokiem, motivēts noziedznieks vienmēr atradīs jaunus veidus, kā uzlauzt tā bruņas. Tādējādi, kibervidē pati svarīgāka aizsardzība ir divējāda. Pirmkārt, jāsāk ar ievainojamības pareizu analīzi. Otrkārt, jānovērtē oponenta motivācija. Ievainojamība un motivācija ir divi pareizas izpratnes un reaģēšanas uz kiberapdraudējumiem un kiberuzbrukumiem stūrakmeņi. Cilvēciskais faktors ir tikpat svarīgs informācijas drošības aspekts kā tehniskie aspekti, piemēram, bieži tiek pārsūtītas konfidenciālas e-pasta adreses, darbā vecāki, kuri ņem bērnus līdzi uz darbu, ļauj tiem piekļūt iekšējam tīklam. Bieži tiek atvērti skaidri redzami aizdomīgi e-pasta sūtījumi, lai vienkārši aplūkotu to saturu. Pastāvošo situāciju vēl nedrošāku dara uzņēmumu nevēlēšanās atklāt, ka tās kļuvušas par uzlaušanas mērķi. Pat, ja noziedznieks ir identificēts un pierādījumi tiek pietiekami savākti, iztiesāto lietu procents ir neliels.

Visklasiskākā uztvere par noziedzīgu nodarījumu informācijas sistēmu jomā subjektiem ir tāda, ka tos izdara t.s. "*hakeri*", gluži kā ārzemju filmās. Nezinātāji, pat neiedomātos, ka pats pirmais datornoziegums esot izdarīts jau 1801. gadā Francijā kādā tekstilrūpnīcā, kurā darbinieki vērsās pret Džozefa Džakarda[48] (*Joseph Marie Jacquard*) izgudrojumu, steļļu mehānismu, kas ar perfokaršu palīdzību veidoja dažādus rakstus. Šī mehānisma mērķis bija atvieglot strādnieku smago roku darbu un veicināt uzņēmuma peļņu mehanizējot stelles tā, lai tās varētu saražot vairāk. Rūpnīcas strādnieki saskatīja draudus šajā attīstībā un sabojāja stelles, bet pati ideja turpināja attīstīties binārās 1 un 0 sistēmas veidā. Kur perfokartē bija caurumiņš, to apzīmētu ar 0, bet, kur nebija – ar 1. Tāpat arī elektriskās ierīcēs, kur, lai to ieslēgtu jānospiež „I", lai izslēgtu – 0. Paturot prātā, ka tehnika attīstās, arī ar vārdu „dators" vai "elektroniskā skaitļojamā mašīna"

[48] Inventor Joseph Marie Jacquard. http://www.ideafinder.com/history/inventors/jacquard.htm [aplūkots 2010. gada 22. septembrī]

nav jāsaprot tikai dators, bet piemēram arī jebkāda veida telefons, mehanizētās sistēmas, automāti, lāzerstari, jo lietojot šos mehānismus vai vēršoties pret tiem pastāv iespēja izdarīt kibernoziegumu.

Neskatoties uz tehnoloģiju attīstību un to, ka tiek radīti pamazām arī roboti, kas programmēti veikt noteiktas darbības – par to kodu būs atbildīgs tā radītājs – cilvēks.

ANO ir publicējusi kiberdraudu un kiberdrošības ceļvedi[49], kurā tiek sniegts kibernoziedznieku tipu, tātad arī noziedzīgu nodarījumu informācijas sistēmu jomā subjektu, raksturojums. Katrai šai grupai dažāda līmeņa zināšanas, dažāda motivācija izdarīt noziedzīgu nodarījumu un attiecīgi arī dažāda pieeja, vai piekļuves līmenis pie informācijas sistēmas. Noziedzīgo nodarījumu subjektus informācijas sistēmu drošības jomā, kā arī kibernoziegumu subjektus vispārīgi var iedalīt sekojošās grupās.

Ļaunprātīgie savējie (*Malicious insiders*). Personas, kuru motivāciju izdarīt noziedzīgas darbības var iedalīt divās kategorijās:

1) motivācija iegūt sev finansiālu labumu, kā arī iespējams kolēģim, vai ieplānojot dalīt šo labumu ar citiem kolēģiem. Labas izredzes palikt nenotvertam, tomēr, ja notver, tad ir grūti savākt nepieciešamos pierādījumus, lai varētu šo personu notiesāt. Šo personu plānos nav nodarīt vardarbību. Šo personu paveiktie datornoziegumi neatstāj ievērojamas nozieguma pēdas, raksturīgs darbībām liecinieku trūkums. Un ievērojot, ka šādu personu darbības var graut uzņēmuma reputāciju, par šo personu veiktajiem noziegumiem reti kad tiek ziņots.
2) Motivācija atriebties darba devējam vai kolēģiem, vai trešo pušu spiediens, vai īpašs politisks atbalsts. Šī grupa ir bīstamākā. Piederošās personas – savējie pārzin informācijas sistēmu vājās vietas un var manipulēt ar to datiem un programmatūru, ielādēt kaitīgu programmatūru un citos veidos sabotēt darba devēja informācijas sistēmas.

Ja šīs personas darbības vieta ir valsts kritiskās infrastruktūras, tad situācija izveidojas līdzīga kiberterorisma izraisītai situācijai un rada lielāko risku, jo tiek apdraudētas tieši kritiskās valsts informācijas sistēmas. Šai personu kategorijai kā ārvalstu piemēru var minēt ziņas par to, ka Moldovā saniknots datortīklu administrators iznīcinājis Moldovas sporta arhīvu jo viņš ticis

[49] Information Insecurity.
http://www.un.int/kamal/information_insecurity/Information_Insecurity_Second_Edition_PDF.pdf [aplūkots 2010. gada 30. septembrī]

atlaists no darba, turklāt šī persona no sava darba devēja netika saņēmusi algu vairāku mēnešu garumā.[50]

Skripta bērneļi (*Script kiddies*). Personas - jauni cilvēki, kam patīk datori. Parasti viesojas hakeru klubu mājas lapās, apmainoties ar gataviem rīkiem un metodēm. Šīm personām patīk izlikties par pieredzējušākām, nekā tās ir patiesībā. Piemēram, ja kādam izdevies uzlauzt mājas lapu vai informācijas sistēmu ar kādām īpašām metodēm un tas nostrādā, tad šīs personas uzzinot par šīm metodēm tās pielietojot izdara tieši to pašu. Idejiski neko jaunu viņi neizdara.

Hakeri, krekeri, un citi (*Hackers, crackers and other*). Cilvēki ar tehnisku domāšanu, tādi, kas labi izprot un raksta programmatūru, ir zinoši matemātikā. Hakeru grupas ir labi organizētas, tas apmainās ar informāciju labāk nekā drošības administratori. Ir tāda grupa ka ētiskie hakeri, kuri tikai uzlauž aizsardzību, lai vairotu zināšanas, bet, protams, nepaziņo par to sistēmu īpašniekiem. Neētisko hakeru noziegumu izdarīšanas iemeslus visbiežāk var definē šādi: „*Tikai tādēļ, ka tas tur atrodas, un es zinu kā.*" Vai „*Lai izraisītu maksimālas neērtības un kaunu*", vai „*Lai piekļūtu krāpnieciskiem datiem, kas ļautu izdarīt krāpnieciskas darbības*". Hakeri uzlauž informācijas sistēmas bez tās īpašnieka ziņas un bieži vien pielāgo datorus savām vajadzībām.

A. Buko norāda "*Entuziasti ar kreatīvām spējām. Šo grupu mēdz „stereotipiski" apzīmēt ar žargona vārdu hakeri („hacker") jeb lauzēji. Vārdu hakeris IT speciālisti sākotnēji izmantoja, apzīmējot augsti kvalificētu programmētāju, un līdz ar to šis vārds nekādi nebija attiecināts uz noziegumu izdarīšanu. Vēlāk ar šo vārdu apzīmēja kvalificētu kibernoziegumu izdarītāju (sadzīves līmenī arī joprojām), taču speciālistu vidū jau kādu laiku tas netiek izmantots noziedznieka raksturojumam, ar to apzīmē personas, kurām piemīt spējas nepārtraukti patstāvīgi pārbaudīt jaunas tehnoloģijas, paaugstināt savas zināšanas, apšaubīt aizsardzības efektivitāti kā tādu un meklēt aizsardzības pārvarēšanas iespējas. Jānorāda, ka šādas īpašības, protams, var izmantot tiesībpārkāpumu realizācijai, taču tā nav obligāta (lielākoties izņēmuma) prasība. Tāpēc šo kibernoziedznieku grupu šāda rakstura pētījumā ir vērts apzīmēt ar vārdu „lauzējs". Lauzējiem piemīt kvalificētas zināšanas IT jomā, kas atšķirībā no citiem speciālistiem neizpaužas kāda apstiprinoša sertifikāta vai diploma iegūšanā. Šīs personas aizsardzības jauninājumus vai kādas tehnoloģijas uztver kā izaicinājumu savu spēju pārbaudei un nepārtraukti cenšas atklāt kādu nepilnību, noziedzīgu motīvu dēļ.*"

[50] Saniknots datortīklu administrators iznīcinājis Moldovas sporta arhīvu. http://www.apollo.lv/portal/news/articles/218760 [aplūkots 2010. gada 28. oktobrī]

Pasaulē noziedzīgu nodarījumu informācijas sistēmu drošības jomā – hakeri jeb lauzēji iedalās melnajos un baltajos hakeros. Par "melnajiem hakeriem" tiek saukti tādi noziedzīgu nodarījumu informācijas sistēmu drošības jomā, kas nodarbojas ar kriminmāla rakstura darbībām, savukārt par "baltajiem hakeriem" tiek sauktas tādas personas, kuru nodarījumi nav atzīti par tādiem, kas nes sabiedrībai kaitējumu.

Kaitīgā koda rakstītāji (*Writers of malicious code*). Standarttermins, lai apzīmētu personas, kas savu radošo darbību vērš, uz kaitīgā koda, programmatūras rakstīšanu, lai panāktu, ka datorsistēma izpilda tā īpašniekam nevēlamas darbības. Zināmākās kaitīgā koda formas – datorvīrusi un datortārpi. Gandrīz ikviens ar pamatiemaņām programmēšanā var uzrakstīt vai modificēt kaitīgu programmatūru vai vīrusu. Un šādu programmatūru var konstatēt tikai pēc tam, kad jau ir inficēts liels skaits datoru. Jo katram kodam ir līdzīgas daļas. Ir arī citas tehnikas, piemēram, MS Office aplikācijas ar paplašinājumu *.vbs*, kas ticis izmantots vīrusam ar nosaukumu „*Melissa*"; izpildāmie faili ar paplašinājumu *.exe*, vai arī steganogrāfijas (informācijas šifrēšanas) tehnika, vīruss, kas paslēpts attēla failā, vai arī Trojas zirgi, pilnībā normāla programma, bet tajā paslēpts kaitīgais kods. Nav līdz galam skaidrs, kas motivē kaitīgā koda rakstītājus. Daļa šo personu uzskata šāda veida programmatūras rakstīšanu par praktiska rakstura joku. Citi var būt sponsorētas personas, kurām maksā par dažādu līdzekļu un rīku attīstīšanu, lai piekļūtu datorsistēmām. Ir arī cita kaitīgā koda rakstītāju kategorija, kurā ietilpst personas ar izcilām zināšanām programmēšanā, kas spēj uzrakstīt tādus kodus kā "loģiskās bumbas", "aizmugures ieejas" vai "neautorizētas piekļuves ģenerālpilnvaras", kā arī, kuri spējīgi uzprogrammēt programmas, kas ļauj veikt krāpnieciskas transakcijas. Arī šajos gadījumos kā motivācija var būt personas atriebība attiecīgās datorsistēmas īpašniekam. Kā arī darbības var būt vērstas uz attiecīgās sistēmas sabotēšanu vai finansiāla labuma gūšanu pašam kaitīgā koda rakstītājam.

Haktīvisti (*Hacktivists*). Ideoloģiski protestētāji digitālajā vidē. Haktīvistu mērķis parasti ir valdības mājas lapas, starptautiskas organizācijas, kredītiestādes. Haktīvisti apgalvo, ka tā ir civilās nepaklausības forma. Haktīvisti apgalvo, ka kibervide sniedz cilvēkiem iespēju tapt sadzirdētiem. Tomēr haktīvistu izpausmēm var būt arī pretēji mērķi sabiedrības interesēm, piemēram, haktīvisti var izplatīt arī nepatiesu informāciju vai rosināt uz vardarbību vai rasu naidu.

Bakalaura darba autore pie haktīvistiem pieskaita arī Latvijas *Neo* jeb Ilmāru Poikānu – LU MII Mākslīgā intelekta laboratorijas līdzstrādnieks. Sekojot līdzi sižetam par VID datu noplūdi masu informācijas līdzekļos ir redzams, ka *Neo* ir atpazīstams ar VID datu bāzes lejupielādēšanu un dažādu valsts struktūru amatpersonu algu saraksta publiskošanu. Turklāt I. Poikāna izplatītajos rakstos interneta vietnēs *www.draugiem.lv*, *www.twitter.com*, pārsvarā dominē raksti, kas apspriež, kritizē un norāda uz Latvijas politiskās struktūras trūkumiem. *Neo* motivācijai ir trīs stūrakmeņi, kā norāda I. Poikāns savā rakstā "Vienkārši par Neo stratēģiju": vecās sistēmas pārlāde, nākotnes valsts un sabiedrības sadarbības formas izveide, iekšējās izmaiņas iedzīvotājos un garīgā atmoda.[51] Turklāt sabiedrībā dominē *Neo* gaišais tēls, jo ekonomiskie jautājumi un materiālās vērtības Latvijas iedzīvotājiem šobrīd ir "sāpīgs jautājums". *Neo* publikācijas par ierēdņu algām norāda uz lielo atšķirību atalgojuma sistēmās. A. Soroka norāda uz Neo kā uz „*"kiberlabvēli", kurš iekustināja Latvijas IT drošības jautājumu*".[52] Arī Informācijas drošības eksperte un Latvijas Universitātes pasniedzēja – Ilze Murāne norāda, ka "*Neo gaišais tēls ir būvēts uz to, ka viņš publiskoja, cik ierēdņi saņēma prēmijās. Bet cik viņš savāca komersantu un godīgu nodokļu maksātāju datus?*"[53] Arī LU MII tīkla risinājumu daļas vadītāja vietniece K. Sataki norāda, ka likumu nevar staipīt kā ienāk prātā, sabiedrībai simpatizē, ka tiek publiskoti dati par valsts ierēdņiem, bet simpatizējošo indivīdu attieksme mainītos, ja dati, piemēram, par šī paša indivīda veselības stāvokli tiktu nopludināti tādā pašā veidā. Starp veiktās iedzīvotāju aptaujas anketām ir atrodama arī tāda anonīma anketa, kur uz jautājumu: „Kāda ir Jūsu attieksme pret „hakeriem"" ir tikusi iegūta atbilde – „*Pret hakeriem, negatīva, Neo – pozitīva*".[54]

Spiegi (*Spies*). Spiegi – industriālie un citi. Industriālā spiegošana ir saistīta ar sacīkstes principu tirgū. Un piedalīšanās tirgū rosina sacīksti dažādiem līdzekļiem un metodēm. Industriālā spiegošana ielaužoties konkurentu informācijas glabātuvēs ir pieaugoša tendence, jo ražotāji paļaujas uz informācijas tehnoloģijām un dažāda veida pētījumus, mārketinga stratēģijas datu veidā glabā savās informācijas sistēmās. Industriālā spiegošana ir apmaksāts pasākums, kas ļauj negodīgā veidā cīnīties par ietekmi ekonomiskajā tirgū. Neiztikt arī bez spiegošanas

[51] I. Poikāns. Vienkārši par Neo stratēģiju. http://213.175.75.4/hot/?rid=41090 [aplūkots 2010. gada 22. novembrī]
[52] A. Soroka. Vai kibernoziedzība ir nopietns drauds Latvijas attīstībai. http://www.saki.lv/viedokli/462-vai-kibernoziedzba-ir-nopietns-drauds-latvijas-attstbai [aplūkots 2010. gada 09.septembrī]
[53] IT eksperti: par VID datu noplūdi jāatbild valdībai. http://www.apollo.lv/portal/news/articles/208923 [aplūkots 2010. gada 20. augustā]
[54] Sk. Pielikumu Nr. 2

klasiskās izpratnes. Ne tikai valstu valdības, bet arī organizētās noziedzības grupas, kā arī teroristiskie grupējumi ir ieinteresētas izmantot personas ar ievērojamām zināšanām informāciju tehnoloģiju jomā izlūkošanas funkciju nodrošināšanai.

Organizētā noziedzība (*Organized crime*). Tehnoloģiju attīstību izmanto organizētās noziedzības grupas personiska labuma gūšanai. Galvenā motivācija ir finansiāla labuma gūšana. Informācijas sistēmu drošības jomā organizētās noziedzības dalībnieku darbība var izpausties galvenokārt ar informācijas tehnoloģiju palīdzību atvieglojot citu noziedzīgu nodarījumu veidu īstenošanu, piemēram, krāpšanu. Kā arī zogot no interneta personas identitātes datus. Kibervidē ir viegli slēpt organizētās noziedzības pēdas, kā arī vairākās valstīs nav pietiekama normatīvo aktu kopuma, kas atvieglotu cīņu ar organizēto noziedzību kibervidē, pat, ja tādi eksistē, to piemērošana ir sarežģīts process.

Kiberteroristi (*Cyber - terrorists*). Praksē nepastāv tāda stabila termina kā kiberteroristi, bet tomēr tāds termins eksistē un pēc savas būtības apzīmē personas, kuru darbība, programmēšanas iemaņas un radītā programmatūra spēj paralizēt Interneta darbību ievērojamā līmenī (valsts, reģionu), kā arī tādu organizāciju darbību, kuras ir atkarīgas no paralizētā Interneta sektora darbības. Labi organizēta kiberuzbrukuma, kas vērsts pret kritisku valsts informācijas sistēmu darbību, potenciālā ietekme varētu tikt pielīdzināta aktīvam kiberkaram.

A. Buko intervijā interneta vietnei *www.kriminal.lv* ir norādījis, ka atsevišķi vērts norādīt tādu grupu kā "**greizsirdīgās otrās puses**", jo mūsdienās ir moderni izsekot savas otrās puses ar mūsdienu tehnoloģiju palīdzību.[55]

Latvijas Universitātes fizikas un matemātikas fakultātes mājas lapā *www.fizmati.lv* ziņu sadaļā 2005. gadā parādījās raksts „Krievu hakeri – labākie pasaulē"[56] Kā arī Krievijas portāls *www.webplanet.ru*, 2004.gadā ir publicējis rakstu „Krievu hakeris jauns, bet bīstams"[57]. Vai tiešām krievu tautības hakeri ir paši labākie esošie un potenciālie noziedzīgu nodarījumu informācijas sistēmu jomā subjekti pasaulē? Šajās publikācijās viennozīmīgi netika ievērots apstāklis, ka noziedzīgi nodarījumi informācijas sistēmu drošības jomā pēc sava rakstura ir

[55] Я. Омельченко. Киберполиция: про поимку хакера Нео, аферы на one.lv торговлю спамом. http://www.kriminal.lv/news/kiber-policiya-pro-poimku-hakera-neo-afery-na-one-lv-i-torgovlyu-spamom [aplūkots 2010. gada 22. oktobrī]

[56] DFMF SP portāls. http://fizmati.lv/zinas/datorika/krievu_hakeri_labakie_pasaule/ [aplūkots 2010. gada 30. septembrī]

[57] Vebplanētas mājas lapa http://www.webplanet.ru/news/security/2004/10/11/xakep.html [aplūkots 2009. gada 29. novembrī]

latenti. Tos ir grūtāk atklāt, un ne vienmēr cietusī persona saprot, ka ir kļuvusi par konkrētā noziedzīgā nodarījuma informācijas sistēmu jomā subjekta upuri.

Izpētot dažādas ārvalstu interneta vietnes var izveidot šādu kibernoziedznieku TOP tabulu:

Interneta vietne	Tops sākot ar augstāko vietu pēc kārtas
http://www.marvquin.com/blog/top-five-5-best-**criminal**-computer-hackers-all-time [aplūkots 2010. gada 30. septembrī]	Kevin Mitnick, Adrian Lamo, Jonathan James, Robert Tappan Morris, Kevin Poulsen
http://science.discovery.com/top-ten/2009/hackers/hackers.html [aplūkots 2010. gada 30. septembrī]	Robert Tappan Morris, Kevin Mitnick, Adrian Lamo, Gary McKinnon (*Solo*), Raphael Gray (*Curador*), John Draper, Kevin Poulsen (*Dark Dante*), Dmitri Galushkevich, Jonathan James (*c0mrade*), Benjamin Stark un Robert Lyttle (*The Deceptive Duo*)
http://geniushackers.com/blog/2008/03/06/top-ten-best-hackers-of-the-world/ [aplūkots 2010. gada 30. septembrī]	Kevin Mitnick, Gary McKinnon, Vladimir Levin, Kevin Poulsen, Timothy Lloyd, Robert Morris, David Smith,
http://www.zimbio.com/Hacking+Resources/articles/9/List+World+Best+Top+Hackers+Time [aplūkots 2010. gada 30. septembrī]	Gary McKinnon, Jonathan James, Adrian Lamo, Kevin Mitnick, Kevin Poulsen, Robert Tappan Morris, Vladimir Levin, David Smith, Mark Abene, Onel A. de Guzman, Chen Ing-hau, Mudge, Jon Lech Johansen, Dmitry Sklyarov, Dennis Moran, Richard Stallman, Stephen Wozniak,

3. tabula: Vadošo kibernoziedznieku popularitātes saraksts

Visas iepriekšējā tabulā minētās personas savā laikā ar savām darbībām ir radījušas apdraudējumu informācijas sistēmu drošībai. Katra no šīm personībām iegājusi hakeru slavas zālē ar ko īpašu, sākot ar datortārpu radīšanu, beidzot ar ielaušanos valdību militārajās sistēmās. Viedokli, ka krievu hakeri ir labākie pasaulē uztur daudzi mediji pamatojoties uz kibernoziegumu konferencēm, kas ik pa laikam norisinās pasaulē, tas tiek pamatots ar to, ka Krievijā ir labākie pasaules matemātiķi un arī, ja krievu programmētāji īpaši neizceļas, tomēr IT speciālisti ir ļoti

pieprasīti. Krievijas Federācijas Iekšlietu Ministrijas „K" nodaļa[58], kas specializējas noziegumu apkarošanas Informāciju tehnoloģiju vidū ir nākusi pie secinājuma, ka vairāk kā 75 % krievu hakeru ir personas, kas jaunākas par 25 gadiem, turklāt ar ļoti labu izglītību. Pavisam nesen pasaules ziņu dienesti ziņoja par to, kā Igaunijas hakeri mazāk kā 12 stundu laikā izņēma 9 miljonus dolāru no vairāk kā 2100 bankomātiem visā pasaulē, kur starp apsūdzēto vārdiem dominē pārsvara slāvu tautības uzvārdi.[59]

Iedalot kādai personai personīgos lietotāja identifikatorus, sistēmas administrators vai uzņēmuma vadība paredz arī šī lietotāja tiesību apjomus, cik daudz sistēmas lietotājs drīkst / nedrīkst darīt sistēmā. Līdzīgi, piemēram, valsts iestādēs, parasti, katram darbiniekam ir savs lietotāja vārds un parole ne tikai konkrētas valsts iestādes sistēmai, bet arī šai iestādei piederošam datoram. Kā arī sistēmas administrators bloķē piekļuvi populārām interneta vietnēm, piemēram, *www.draugiem.lv*, jo vienkāršs lietotājs savā darbam paredzētajā datorā var ielādēt kādu kaitīgu datorprogrammu un sistēmās resursi var tikt ietekmēti tai nelabvēlīgā veidā, kas var izraisīt dažādas pakāpes seku iestāšanos. Tomēr reālā situācija ir tāda, ka valsts iestāžu darbinieki tik un tā atrod veidus, kā "*sēdēt*" tajā pašā vietnē kā bloķētajā vietnē, neprasot tieši sistēmas administratoram piekļuvi šai vietnei, bet gan, piemēram, ievadot vietnes skaitlisko, nevis vārdisko adresi. Tātad, pārkāpj tiem noteikto darbību apjomu tiem piešķirtajā darba nolūkiem paredzētajā sistēmā un kļūst par iespējamajiem datornoziegumu subjektiem. Un šeit jau var runāt par datora ļaunprātīgu izmantošanu, nevis datora nepareizu ekspluatāciju, jo ne bez iemesla konkrētās vietnes ir bloķētas, valsts iestādes šādā veidā vēlējušās nodrošināt lielāku darbinieku efektivitāti, ņemot vērā, ka sociālie tīkli jau sāk pārņemt vidusmēra cilvēka ikdienu. Arī Tiesnešu ētikas komisija ir nonākusi pie šāda secinājuma un šis jautājums "..skaidrojums par tiesnesi kā *www.draugiem.lv* un citu līdzīgu sociālo tīklu lietotāju" ticis apspriests 08.10.2010. Tiesnešu ētikas komisijas sēdē. Tāpat arī notiek dažādu darba vajadzībām neparedzētu datorprogrammu instalēšana sistēmām neparedzētās vietās, sāknēšanas failu atrašanās vietu glabājot nevis tiem paredzētajās vietās, *C://Programm Files*, bet gan *My Documents* vai *Desktop*. Kā atbildība iestājas šajā gadījumā? Sistēmu administratora, kurš nav darījis visu, lai novērstu šādu apdraudējuma risku vai sistēmas lietotāja, kurš zinādams par savu pilnvaru apjomu tās ir pārsniedzis. Kā arī rodas problēmjautājums, vai datoradministratori, kuru pārziņā ir kādas

[58] KF IeM K nodaļa. http://www.mvd.ru/struct/10000220/10000287/ [aplūkots 2010. gada 30. septembrī]
[59] Igaunijas hakeriem uzrādīta apsūdzība par 9 miljonu dolāru zādzību.
http://www.apollo.lv/portal/news/articles/185219 [aplūkots 2010. gada 30. septembrī]

datorsistēmas, kuri testē to drošību mēģinot paši lauzt savas sistēmas, arī ir datornoziegumu subjekti kā tie, kas šīs sistēmas mēģina apiet vai uzlauzt bez pilnīgas saistības vai piederības pie tām.

4. Noziedzīgu nodarījumu informācijas sistēmu drošības jomā prevences prakse

Informācijas sistēmu drošības jomā ir izstrādāti dažādi normatīvie akti, vadlīnijas un sertifikācijas gan valsts, gan arī starptautiskajā līmenī, tāpēc darba autore uzskata, ka ir lietderīgi ieskicēt šīs informācijas sistēmu aizsardzības tendences.

4.1. Latvijas prevences prakse

Normatīvie akti kā prevencijas līdzeklis. Latvijā likumdevējs ir paredzējis vairākus legālus rīkus noziedzīgu nodarījumu pret informācijas sistēmu drošību jomā. Galveni no tiem ir Krimināllikums, Latvijas administratīvo pārkāpumu kodekss, Valsts informācijas sistēmu likums. Valsts IS drošības prasības tiek izstrādātas likumos un Ministru kabineta noteikumos, kuros ir uzskaitīti kritēriji informācijas sistēmu drošībai un izvirzītas prasības personām, kuras nes atbildību par to drošību. Piemēram, Valsts informācijas sistēmu likums reglamentē, ka Valsts IS drošības pārvaldniekam ir nepieciešams iziet apmācības kursu un nokārtot speciālu zināšanu pārbaudi, kuras rezultātā tai tiek piešķirts attiecīgs sertifikāts. Tas nozīmē, ka tikai profesionāli sagatavoti cilvēki var nodrošināt nepieciešamo IS aizsardzību. Privāto IS īpašnieki var izvirzīt citādus drošības kritērijus savā speciālistu komandā piesaistot kvalificētus programmētājus, vairāki uzņēmumi pat ir gatavi noalgot tieši tādas personas, kuras spēj uzlauzt šādas sistēmas šādā veidā atrodot sistēmu vājās vietas un to arvien pilnveidojot.

Ministru kabineta noteikumi paredz kritērijus un principus, pēc kuriem būtu jāvadās Valsts IS pārvaldniekiem. Kā arī var izsecināt, ka informācijai un informācijas sistēmām ir dažādas klasifikācijas un drošības pakāpes. Piemēram, Kritiskām valsts IS ir stingrākas aizsardzības prasības. (Sk. MK noteikumi Nr. 1445 "Kritisku valsts informācijas sistēmu un valsts informācijas sistēmu savietotāju aizsardzības prasības") Piešķirot informācijai dažādas pakāpes pieejamību vai statusu, var izvērtēt tās apdraudējuma pakāpi un izanalizēt iespējamos apdraudējuma avotus, personas, kas būtu ieinteresētas iegūt šādu informāciju, tādējādi katrai sistēmai veidojot oriģinālu aizsardzību, jo, vienota aizsardzība visām sistēmām var novest pie visu sistēmu aizsardzības līdzekļu pārvarēšanas, ja tiku apieti kaut vai vienas sistēmas aizsardzības līdzekļi.

2010. gada 28. oktobrī Saeima 3. lasījumā izskatīja un pieņēma Informācijas tehnoloģiju drošības likumu, kurš paredzams stāsies spēkā 2011. gada 1. februārī. No likuma projekta teksta izriet, ka likums būs saistošs ne tikai valsts un pašvaldību institūcijām, bet arī komersantiem un citām privāto tiesību juridiskajām personām. Likums paredz, ka informācijas tehnoloģiju (IT) drošība būs jāpārvalda tā, lai varētu savlaicīgi prognozēt un novērst apdraudējumus, kā arī pārvarēt tos un novērst sekas. Atbildīgajām personām būs jāapzina valsts un sabiedrības pamatfunkcijām nepieciešamās IT un jāorganizē to aizsardzība. Tiks izveidota Informācijas tehnoloģiju drošības incidentu novēršanas institūcija, kuras uzdevumus Satiksmes ministrijas pakļautībā pildīs Latvijas Universitātes Matemātikas un informātikas institūts. Tā veicinās IT drošību Latvijā, uzturot vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu, sniedzot atbalstu IT drošības incidentu novēršanā, publicējot ieteikumus, lai nepieļautu riskus, veicot pētniecisko darbu, organizējot izglītojošos pasākumus un mācības. Institūcija sniegs arī atbalstu valsts iestādēm valsts drošības sargāšanā, uzraugot valsts un pašvaldību institūciju, kā arī elektronisko sakaru komersantu pienākumu izpildi. Lai koordinētu ar IT drošību saistīto uzdevumu un pasākumu plānošanu un veikšanu, tiks izveidota Nacionālā IT drošības padome, kas aizstās pašreizējo Elektronisko sakaru un informācijas tehnoloģiju nozares konsultatīvo padomi drošības jautājumos. Likumā noteiktas arī minimālās prasības IT drošības jomā, kas jāievēro valsts un pašvaldību iestādēm. Paredzēta arī kārtība, kādā šīm institūcijām jārīkojas apdraudējuma gadījumos. Tāpat tiesību akts ietver normas publisko elektronisko sakaru tīklu drošībai. Jaunā likuma īstenošana būtiski stiprinās IT drošību Latvijā, kā arī uzlabos valsts spējas sadarboties ar starptautiskajiem partneriem šīs jomas aizsardzībā. Likums stāsies spēkā 2011.gada 1.februārī. Līdz tam paredzēts izdot Ministra kabineta noteikumus par IT kritisko infrastruktūru un publisko elektronisko sakaru tīklu drošību. Plānots veikt grozījumus arī citos normatīvajos aktos.

Informācija kā prevencijas līdzeklis. Kas attiecas uz valsts informācijas sistēmām, tad vairākas valsts iestādes kā nākotnes darbības koncepciju ir norādījušas – jaunu informācijas sistēmu izstrādi un normatīvo aktu pilnveidošanu šajā jomā. Valsts policijas plānotais 2010. gadā viens no darbības virzieniem – normatīvo aktu pilnveidošana, kas palīdzētu efektīvāk novērst noziedzīgus nodarījumus ne tikai informācijas sistēmu jomā, bet arī kibernoziegumu jomā vispārīgi. Saskaņā ar MK rīkojumu Nr. 248 "Par Pašvaldību vienotās informācijas sistēmas attīstības koncepciju 2010. – 2013. gadam" ir plānots ieviest vienotu pašvaldību IS. Pozitīvais

aspekts ir tāds, ka ir prognozēti vairāki sistēmas lietojumprogrammatūras attīstības varianti un to attīstības modeļi. Pieļaujot pat domu par atvērtā koda programmatūras nodrošinājumu, kas Latvijā nav īpaši populārs risinājums atvērtā koda pielietošanas trūkuma dēļ valsts IT risinājumos. Pašvaldību vienotās IS attīstība ir noteikta Reģionālās attīstības un pašvaldības lietu ministrijas (RAPLM) kompetencē. Atbilstoši Ministru kabineta lēmumam no 2009.gada 1.jūnija Reģionālās attīstības uz pašvaldību lietu ministrija ir pārņēmusi Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta funkcijas un turpmāk ir atbildīga par elektroniskās pārvaldes (e-pārvaldes), informācijas sabiedrības un informācijas tehnoloģiju politikas izstrādāšanu un koordinēšanu. Tomēr var pamanīt, ka arī Satiksmes ministrijas Elektronisko sakaru apakšnozares politikas mērķis ir nodrošināt kvalitatīvu un ērtu elektronisko sakaru pakalpojumu pieejamību visā Latvijas Republikas teritorijā. Abu ministriju uzdevumi un funkcijas brīžiem dublējas. Lietderīgāk būtu izveidot vienu organizāciju, kas nodarbotos ar e-pārvaldi, nevis pārdalīt katrai iestādei mazu daļiņu no e-pārvaldes un rīkot ik pa laikam viedokļu apmaiņas pasākumus, kuros tiktu iesaistītas gan valsts iestādes, gan citi interesenti informācijas sistēmu un citu e-lietu jomā, nevis veidot atkal jaunus un jaunus veidojumus, kas atbild par vienu un to pašu.

Latvijā darbojas DDIRV struktūrvienība, kas izveidota lai sniegtu konsultācijas un izstrādātu rekomendācijas datorsistēmu un tīklu administratoriem datoru drošības incidentu gadījumos, kas ir jebkāda darbība, kā rezultātā tiek vai var tikt ietekmēta datorsistēmu vai tīklu drošība. DDIRV pamata pakalpojumi ir apsteidzošās informācijas izplatīšana par iespējamiem apdraudējumiem, kā arī konsultācijas un rekomendācijas saistībā ar DDI. Valsts un pašvaldību institūciju un komersantu IT administratori var brīvprātīgi reģistrēties DDIRV, iegūstot iespēju DDIRV mājas lapā saņemt apsteidzošo informāciju par iespējamo apdraudējumu norādītajā IP adrešu laukā. Visi DDIRV mājas lapas apmeklētāji var iepazīties ar aktuālajiem jaunumiem, atrast informāciju par jaunākajiem vīrusiem un ievainojamībām, publikācijām saistībā ar interneta drošību, DDI statistiku u.c materiāliem. Jebkuram atsevišķas darba stacijas lietotājam, tai skaitā Valsts un pašvaldību institūciju datorsistēmu darba staciju lietotājiem, problēmas, kas saistītas ar DDI, vispirms jārisina ar savu IT administratoru vai Interneta pakalpojuma sniedzēju.

Risku analīzes sertifikācija kā prevencijas līdzeklis. IS drošības riskus analizē ievērojot konkrētus standartus. Šobrīd valsts sistēmas drošības riskus analizē ievērojot Latvijas standartā LVS ISO/IEC 17799:2002 “Informācijas tehnoloģija. Prakses kodekss informācijas

drošības pārvaldībai" noteiktās prasības. Savukārt šobrīd Latvijā kļūst populārs starptautiskais ISO 27001 standarts, kas nosaka prasības informācijas drošības vadības sistēmai. Šis standarts ļauj uzņēmumiem novērtēt IT drošības riskus un ieviest atbilstošu kontroli. Standarta galvenais mērķis ir uzņēmuma informācijas aizsardzība, standarta ievērošana palīdz nodrošināt uzņēmuma darbību jebkuros apstākļos. Sertifikātu piešķir uz trim gadiem un vismaz vienu reizi gadā tiek veikts uzraudzības audits. Standarts piemērots jebkuras nozares uzņēmumam, kas lieto jebkādus IT risinājumus. Turklāt Latvijā jau notiek ISO 27001 standarta ekspertu izglītošana un akreditācija, tas nozīmē, ka šī standarta realizācija kļūst lētāka ietaupot uz ekspertu pieaicināšanas rēķina.[60]

Saskaņā ar ISO standartu ir ieteicams pasargāt no neautorizētas piekļuves, tātad aizsargāt no personām, kurām šī informācija nav paredzēta. Tāpat arī ir ieteicams informāciju klasificēt, lai noteiktu, kādi aizsardzības pasākumi tai ir nepieciešami, piemēram, informāciju var iedalīt:

- konfidenciālā – kurai izkļūstot ārpus organizācijas, tai var rasties ievērojams finansiāls zaudējums un arī reputācijas kritums. Šīs informācijas atklāšanai nepieciešama īpašnieka atļauja. Ja šo informāciju nepieciešams atklāt kādai trešajai personai, tad nepieciešams arī konfidencialitātes līgums, piemēram, līgumu detaļas, jaunu produktu koncepcijas, u.tml.;
- Tikai iekšējās lietošanas informācija – šādas informācijas noplūde var radīt finansiālus zaudējumus, un iespējams arī apkaunojumu organizācijai. Parasti nenes nopietnu kaitējumu organizācijai. Šī informācija atrodas organizācijas darbinieku brīvā apgrozībā, piemēram, veidlapas, apmācības materiāli, u.tml.;
- Publiska informācija – ja šāda veida informācija izkļūst ārpus organizācijas robežām, tad kaitējums ar to nerodas. Piemēram, pārskati vai preses materiāli.

Šajā standartā ir arī noteikti arī konfidencialitātes pakāpes dažādiem informācijas veidiem, norādītas iespējamās informācijas neatļautas pieejas sekas un sniegtas rekomendācijas no fiziskās informācijas aizsardzības puses, t.i., tehnika u.c., kā arī ievērots cilvēciskais faktors, personu izvērtēšana un tām piešķirtās piekļuves pakāpes, atbildīgās personas, to uzdevumi, u.c., tiek rekomendētas arī drošības risku paziņošanas procedūras, e-pasta, interneta un sakaru tīklu iekšējās kārtības noteikumu realizēšana.

[60] Zars A. Aktuālā informācijas sistēmu drošības sertifikācija. Biznesa ideju žurnāls Kapitāls 08/2010 (152). 78.-79.lpp.

Fiziskās drošības nodrošināšana kā prevencijas līdzeklis. Runājot par datorsistēmu aizsardzību gandrīz vienmēr tiek domāts par loģisko datorsistēmu drošību, par to, lai kāds neielaužas sistēmā un neiznīcina datus, bet ne vienmēr cilvēki aizdomājas, ka fiziskā datu drošība arī ir svarīgs faktors datorsistēmas aizsardzībai. Piemēram, ja aplūko jebkuras valsts informācijas sistēmas aprakstu Valsts informācijas sistēmu reģistrā (VISR), tad gandrīz visām šīm sistēmām ir norādīts, kādi fiziskās aizsardzības elementi tām ir nodrošināti. Piemēram, Atrašanās vietas informācijas datubāzei fiziskās aizsardzības līdzekļi ir norādīti sekojoši: "telpas, kur atrodas serveri, tīkla aparatūra un darbstacijas, ir aizsargātās no ārējās fiziskās ietekmes un nepilnvarotu personu iekļūšanas (pieejas kontrole), aprīkotas ar speciālu ugunsdrošības signalizāciju, ventilācijas sistēmu. Serveru telpas papildus tiek nodrošinātas ar klimata kontroli, signalizāciju ar kodu pieejas kontroli, nepārtrauktu elektrobarošanas padevi, automātisku ugunsdzēšanas sistēmu. Tiek veikta informācijas rezerves kopēšana. Rezerves kopijas tiek glabātas divās ģeogrāfiski nošķirtās vietās." Kā redzams, datorsistēma var tikt apdraudēta ne tikai personai atrodoties kādā attālinātās piekļuves punktā, bet arī piekļūstot tai pašas sistēmas servera atrašanās vietas punktā, kur persona, iespējams, var neatļauti piekļūt svarīgiem datiem, vai pat iznīcināt informācijas sistēmas fiziskās aizsardzības elementus, tādējādi sabojājot vai iznīcinot informācijas sistēmu.

4.2. Ārvalstu prevences prakse

Krievija. Runājot par Krievijas pieeju kiberdraudu novēršanai, šeit vispirms jāmin Krievijas Federācijas Iekšlietu ministrijas "K" nodaļa (*Управление «К» МВД РФ*). Iesākumā, aptverot kiberdraudu izplatību, tika strādāts pie Krievijas Federācijas Krimināl kodeksa, kurā tika iekļauta 28. nodaļa "Noziegumi datorinformācijas jomā", kas sākumā paredzēja trīs nozieguma sastāvus (nelikumīga piekļuve ESM esošai informācijai, to sistēmām un tīkliem; kaitīgas programmatūras ESM radīšana, izplatīšana un lietošana; ESM, to sistēmas un tīklu ekspluatācijas noteikumu pārkāpšana). Šī kodeksa versija stājās spēkā 1997. gada janvārī. 1998. gadā Krievijas IeM struktūrās tika radīta īpaša apakšnodaļa cīņai ar noziegumiem informācijas tehnoloģiju sfērā. 2000. gadā tika izveidotas un uzsāka darbu 81 jauna teritoriālā struktūrvienība Krievijas Federācijā cīņai ar šāda veida noziegumiem. Sākot šādu jaunu noziegumu izmeklēšanu parādījās arī tiem raksturīgās problēmas to atklāšanā – nebija liela praktiska pieredze, trūka metodoloģijas šādu noziegumu izmeklēšanā, līdz ar to varēja spriest par šādu noziegumu izteikto latentitāti. 2001. gadā notika izmaiņas Krievijas IeM struktūrās un apakšnodaļa cīņai ar noziegumiem

informācijas tehnoloģiju sfērā pārtapa par Krievijas IeM "K" nodaļu, bet teritoriālās apakšvienības par "K" vienībām, kuru galvenie darbības virzieni ir sekojoši:

1) Cīņa ar noziegumiem datorinformācijas sfērā: prettiesiskas piekļuves faktu datorinformācijai konstatēšana un novēršana; cīņa ar prettiesisku programmu ESM izgatavošanu, izplatīšanu un lietošanu; pretdarbība krāpnieciskām darbībām, kas saistīta ar elektronisko maksāšanas sistēmu iespējām; cīņa ar nepilngadīgo pornogrāfisku materiālu izplatīšanu Interneta tīklā;
2) Prettiesisku darbību novēršana informācijas - telekomunikāciju tīklos, ieskaitot Interneta tīklu: nelikumīgas sakaru tīklu un vadu līniju lietošanas faktu konstatēšana un novēršana; pretdarbība krāpnieciskām darbībām, kas tiek veiktas izmantojot informācijas - telekomunikāciju tīklus, ieskaitot Interneta tīklu; komerciālās satelītkanālu un kabeļtelevīzijas prettiesiskas piekļuves novēršana.
3) Cīņa ar nelikumīgu radioelektronikas un speciālu tehnisko līdzekļu apriti;
4) Nelikumīgu darbību autortiesību un blakustiesību jomā konstatēšana un novēršana;
5) Cīņa ar starptautiskajiem noziegumiem informācijas tehnoloģiju sfērā: pretdarbība starptautiska rakstura noziegumiem informācijas tehnoloģiju sfērā; starptautiskā sadarbība.

"K" nodaļa regulāri publisko jaunāko noziegumu tendences informācijas tehnoloģiju sfērā gan savā mājas lapā, gan arī regulāri izplatot dažādas publikācijas, kas kļūst pieejamas iedzīvotājiem. [61]

Vācija. Vācijas krimināLkodeksā noziedzīgi nodarījumi informācijas sistēmu drošības sfērā ir iekļauti tā 15. nodaļā "Pārkāpumi privātās dzīves jomā". Tā 202a § paredzēta atbildība par datu spiegošanu – nelikumīgu datu iegūšanu paša vai citas personas vajadzībām, kas nav bijuši paredzēti šīs personas rīcībai un ir bijuši īpaši aizsargāti pret neautorizētu piekļuvi, turklāt datiem jābūt uzglabātiem vai pārraidītiem elektroniskā vai magnētiskā veidā. Šī paša kodeksa 202b § paredzēta atbildība par "fišingošanu" – nelikumīgu datu pārtveršanu, kas nav paredzēta šai personai, personiskā vai ar tehnisku līdzekļu palīdzību veidā no nepubliskas datu apstrādes iekārtas. Kodeksa 202b § paredzēta atbildība par darbību izdarīšanu, kas līdzvērtīgas spiegošanai vai "fišingošanai", t.i. veic priekšnosacījumus iepriekšminētos paragrāfos 202a un 202b paredzēto noziedzīgo darbību veikšanai – personīgām vai citas personas vajadzībām, pārdodot,

[61] Krievijas IeM "K" nodaļa. http://www.mvd.ru/struct/10000220/ [aplūkots 2010. gada 06. oktobrī]

nodrošinot citu personu ar, vai citādā veidā padarot pieejamas: paroles vai drošības kodus, programmatūru šādu nodarījumu veikšanai. Tomēr, saskaņā ar šo pašu kodeksu, ja persona labprātīgi atsakās no izplānota noziedzīga nodarījuma izdarīšanas, vai novērš izdarītās briesmas, vai novērš plānoto noziegumu, kā arī ja persona iznīcina vai padara nederīgus rīkus plānotā noziedzīgā nodarījuma izdarīšanai, vai, ja paziņo par to esamību publiskai varas iestādei, vai, ja tai padodas, tad tā nenes atbildību par dotā nozieguma izdarīšanu. Šādi nosacījumi atbrīvo personu no krimināatbildības. Šī paša kodeksa 348 § paredzēta atbildība par apzināti nepatiesu datu ievadīšanu publiskos dokumentos vai informācijas sistēmās, bet 303a § paredzēta atbildība par datu nelikumīgu dzēšanu, dzēšanu, bojāšanu vai to padarīšanu par nederīgiem 303b § paredzēta atbildība par fizisko informācijas sistēmu vai tās elementu bojāšanu.

Valsts informācijas drošības birojs (*Bundesamt für Sicherheit in der Informationstechnik*) ir pirmais un centrālais IT pakalpojumu drošības pakalpojumu sniedzējs Vācijas federālajai valdībai. Tomēr tas savus pakalpojumus sniedz arī IT ražotājiem, privātiem un komerciāliem ražotājiem un citiem informācijas pakalpojumu sniedzējiem. Birojs izmeklē drošības riskus, kas saistīti ar IT lietošanu un izstrādā preventīvus drošības pasākumus. Birojs sniedz informāciju par riskiem un draudiem, kas saistīti ar IT lietošanu un izstrādē to atrisināšanai piemērotus risinājumus. Šis darbs ietver IT drošības testēšanu un IT sistēmu izvērtēšanu. Lai novērstu un samazinātu šos riskus, biroja pakalpojumi ir orientēti uz dažādu mērķauditoriju, kurām sniedz arī konsultācijas. Biroja darbs ir organizēts četros departamentos – vienā centrālajā (administrācija) un trijos specializētajos. Katra departaments sastāv no divām apakšnodaļām. Piemēram, pirmais – programmatūras drošības, kritisko infrastruktūru un interneta drošības departaments - atbildīgs par drošu un funkcionālu elektronisko komunikāciju starp valsts pārvaldes iestādēm, pilsoņiem un uzņēmumiem. Papildus ražo IT drošības koncepcijas, tas ietver arī stratēģisko pieteikumu e-pārvaldi, piemēram, īstenojot "virtuālo pasta sūtījumu telpas", un konsultācijas un atbalstu esošajiem un eksperimentālajiem projektiem. Papildus attīsta administratīvās publisko atslēgu infrastruktūras, drošu e-pastu nosūtīšana garantē sertifikātu izsniegšanu un darbības tīmekļa serveru aizsardzību ar šifrēšanu. Atvērtā pirmkoda projektu attīstība arī cieši veicina konsultāciju pakalpojumu nodrošināšanu federālajām iestādēm. Viens no mērķiem ir attīstīt pamata drošības prasības un praktiskus risinājumus ugunsmūriem, tīkla infrastruktūrām un lietojumprogrammās. Nodaļa analizē un novērtē drošības īpašības protokoliem, interneta lietojumprogrammām, tīkliem un tīklu pakalpojumiem. Federālā datoru apdraudējumu ātrās reaģēšanas komanda darbojas kā

centrālais kontaktpunkts, lai atrisinātu datoru un tīkla drošības problēmas federālajās iestādes, ir arī daļa no nodaļas. "Īpašās IT ārkārtas situācijās" CERT speciālistu komanda, informē lietotājus nekavējoties par draudiem un to novēršanai veicamajiem pasākumiem. Tāpat arī pastāv šifrēšanas un pretizlūkošanas departaments un sertifikācijas departaments.

Arī Vācijas dažādu zemju un pilsētu policijas iecirkņi aktīvi informē par dažādu veidu kiberapdraudējumiem un tendencēm datornoziedzības jomā. Tāpat vienotā policijas sistēmā tiek plānotas dažādas sabiedrības informācijas aktivitātes, lai brīdinātu iedzīvotājus par iespējamiem kiberdraudiem, piemēram, "Drošības kompass", kas lietotāju iepazīstina ar TOP 10 drošības riskiem strādājot ar datoru.[62] Īpašu ievērību, piemēram, Bavārijas policija pievērš virtuālās bērnu pornogrāfijas atklāšanai un novēršanai. Izmeklēšanas metodes – meklēšanas darbs tīmeklī, kā arī iedzīvotāju ziņojumi.

Vācu policija nonākusi pie secinājuma, ka arī "balto apkaklīšu" noziedzīgajos nodarījumos arvien vairāk sāk parādīties kibernoziedzības elementi, galvenokārt, kas saistīti ar krāpniecību.

[62] Sicherheitskompass. http://www.polizeiberatung.de/vorbeugung/gefahren_im_internet/sicherheitskompass/ [aplūkots 2010. gada 11. oktobrī]

Kopsavilkums

Informācijas sistēmas drošība ir tāds informācijas sistēmas stāvoklis, kad darbojoties informācijas sistēmai, netiek traucēta tās konfidencialitāte, integritāte un pieejamība. Ievērojot Starptautiskos līgumus un konvencijas, īstenojot ilgstošu vienotu tiesību aktu piemērošanu Starptautiska līmenī ir reāli samazināmu noziedzīgu nodarījumu informācijas sistēmu drošības jomā riski. Krimināltiesiskā atbildība par vairāku noziedzīgu nodarījumu, kuru tiešais objekts ir informācijas sistēmu drošība, iestājas gadījumos, kad tiek konstatēts vismaz ievērojams kaitējums.

Bakalaura darba izstrādes gaitā ir apstiprinājusies sākotnēji izvirzītā hipotēze

- noziedzīgi nodarījumi informācijas sistēmu drošības jomā ir saistīti ar to, ka informācijas tehnoloģijas attīstās daudz intensīvāk, salīdzinot ar to drošību nodrošinošo krimināltiesisko regulējumu. Pētījuma rezultāti sniedz iespējas autorei izdarīt sekojošus secinājumus un izvirzīt atbilstošus priekšlikumus:

1) sabiedrībā mūsdienās ir vāji attīstīta izpratne par apdraudējuma riskiem informācijas sistēmu drošības jomā, ko pierāda veiktās aptaujas;
2) Krimināllikumā XX nodaļas sevišķās daļas normās Informācijas tehnoloģiju drošības jomā vai Latvijas administratīvo pārkāpumu kodeksā nepieciešams paredzēt atbildību par tādiem tīšiem noziedzīgiem nodarījumiem informācijas sistēmu drošības jomā, gadījumos, kas nav saistīti ar ievērojama kaitējuma nodarīšanu;
3) Krimināllikuma sevišķajā daļā jāietver speciāla apakšnodaļa, kas paredzētu atbildību par kibernoziegumu izdarīšanu;
4) nepieciešams regulējums, lai definētu personas, kura ir atbildīga par tai uzticētās informācijas sistēmas drošību, krimināltiesisko atbildību, jo krimināllikums neparedz KL 245.p. gadījumā atbildību par „bezdarbību";
5) nepastāv stabilas tiesu prakses par noziedzīgiem nodarījumiem informācijas sistēmu drošības jomā;
6) nepieciešams īstenot vēl plašākus informatīvos pasākumus iedzīvotāju informētībai par to, kas tieši ir noziedzīgi nodarījumi informācijas sistēmu drošības jomā un kā mazināt to riskus, kur vērsties šāda apdraudējuma gadījumā;

7) nepieciešams mācīties no ārvalstu pieredzes un attīstīt publiskā - privātā sektora partnerattiecības noziedzīgu nodarījumu informācijas sistēmu drošības jomā prevencei;
8) nepieciešams izstrādāt noteikumus, kas regulētu kārtību, kādā tiek aprēķināti zaudējumi informācijas sistēmu drošības incidentu gadījumos;
9) informācijas tehnoloģijas attīstās daudz intensīvāk, salīdzinot ar to drošību nodrošinošo tiesisko regulējumu.

Anotācija latviešu valodā

Noziedzīgi nodarījumi informācijas sistēmu drošības jomā ir līdz galam neskaidrs un nepilnīgi regulēts noziedzīgu nodarījumu veids. Nepastāv stabilas tiesu prakses jautājumos, kas skar informācijas sistēmu drošību. Bakalaura darba autore veica patstāvīgu kriminoloģisku pētījumu veicot iedzīvotāju aptauju un intervējot attiecīgās nozares speciālistus.

Bakalaura darba 1. nodaļā aplūkots jautājums par to, kas ir informācijas sistēmas, kādi ir to apdraudējumi.

Bakalaura darba 2. nodaļā aplūkoti Krimināllikumā paredzētie noziedzīgie nodarījumi informācijas sistēmu drošības jomā.

Bakalaura darba 3. nodaļā ir izpētītas galvenās noziedzīgu nodarījumu informācijas sistēmu drošības jomā subjektu grupas, kā arī noziedzīgu nodarījumu informācijas sistēmu drošības jomā izplatības raksturojums.

Bakalaura darba 4. nodaļā sniegts ieskats Latvijas un ārvalstu prevencijas praksē noziedzīgu nodarījumu informācijas sistēmu drošības jomā.

Bakalaura darba pielikumos ir atspoguļoti iedzīvotāju aptaujas pētījuma rezultāti, kas atspoguļo iedzīvotāju vispārējo izpratni par kibernoziedzību un nepieciešamību pienācīgi aizsargāt datus. Kā arī pielikumā ir pievienota intervija ar Valsts policijas Galvenās Kriminālpolicijas pārvaldes 4. nodaļas priekšnieku Aleksandru Buko.

Ir pierādīta hipotēze: noziedzīgi nodarījumi informācijas sistēmu drošības jomā ir saistīti ar to, ka informācijas tehnoloģijas attīstās daudz intensīvāk, salīdzinot ar to drošību nodrošinošo krimināltiesisko regulējumu.

Anotācija angļu valodā

Annotation

Criminal offences in the sphere of safety of information systems are obscure and not sufficiently regulated form of the criminal offences. There is no stable judicial practice on the matters, referred to the safety of the information systems. The author of bachelor paper made an independent criminological research by carrying out the interrogation of inhabitants and taking interviews from the specialists of referable branch.

In 1st chapter of bachelor paper is explored, what is the information systems, which threats exists for them.

In 2nd chapter of bachelor paper are explored criminal offences, provided by Criminal Law in sphere of security of information systems.

In 3rd chapter of bachelor paper are explored the main groups of subjects of criminal offences in the sphere of safety of information systems, and so the characteristic of the spread of criminal offences in the sphere of safety of the information systems.

In 4th chapter of bachelor paper is given insight in the Latvian and foreign practice of prevention of the criminal offences in the sphere of security of information systems.

In the attachments to the bachelor paper are reflected the results of research of the interrogation of inhabitants, which reflect the attitude of inhabitants about cyber crimes in general and the need for data protection. Also in the attachment is found interview with the chief of the 4th division of the Main administration of the Criminal police of the State police Alexander Buko.

The hypothesis is proven: criminal offences in the sphere of safety of information systems are connected with the fact that information technologies develop much more intensive than the legal adjustment, which guarantees their safety.

Izmantotās literatūras un juridisko aktu saraksts

Literatūra

1. Ķinis U. Kibernoziegumi. Rīga: SIA „Biznesa augstskola Turība", 2007.
2. [B.a.] Mācību grāmata. Kriminoloģija. [B.v.] Nordik, 2004.
3. Krastiņš U, Liholaja V., Niedre A. Krimināltiesības vispārīgā daļa. Trešais papildinātais izdevums. Rīga: Tiesu namu aģentūra, 2008.
4. Krastiņš U, Liholaja V., Niedre A. Krimināltiesības sevišķā daļa. Trešais papildinātais izdevums. Rīga: Tiesu namu aģentūra, 2009.
5. Drivinieks V. Kibernoziegumi. Bakalaura darbs. Rīga: Latvijas Universitāte, 2009.
6. Zars A. Aktuālā informācijas sistēmu drošības sertifikācija. Biznesa ideju žurnāls Kapitāls 08/2010 (152).

Palīgmateriāli no interneta

1. Cybercrime. Cybercrime. http://www.techterms.com/definition/cybercrime [aplūkots 2010. gada 22. septembrī]
2. Inventor Joseph Marie Jacquard. http://www.ideafinder.com/history/inventors/jacquard.htm [aplūkots 2010. gada 22. septembrī]
3. Valsts informācijas sistēmu reģistrs. http://www.visr.eps.gov.lv/visr/. [aplūkots 2010. gada 23. septembrī]
4. Top five (5) best criminal hackers of all time. http://www.marvquin.com/blog/top-five-5-best-criminal-computer-hackers-all-time [aplūkots 2010. gada 30. septembrī]
5. Top 10 hackers. http://science.discovery.com/top-ten/2009/hackers/hackers.html [aplūkots 2010. gada 30. septembrī]
6. Top ten best hackers of the world. http://geniushackers.com/blog/2008/03/06/top-ten-best-hackers-of-the-world/ [aplūkots 2010. gada 30. septembrī]
7. List of World Best Top Hackers of All Time. http://www.zimbio.com/Hacking+Resources/articles/9/List+World+Best+Top+Hackers+Time [aplūkots 2010. gada 30. septembrī]

8. KF IeM K nodaļa. http://www.mvd.ru/struct/10000220/10000287/ [aplūkots 2010. gada 30. septembrī]
9. Igaunijas hakeriem uzrādīta apsūdzība par 9 miljonu dolāru zādzību. http://www.apollo.lv/portal/news/articles/185219 [aplūkots 2010. gada 30. septembrī]
10. Raksts. http://www.2v.lv/index.php?option=com_content&view=article&id=402:ar-autisma-paveidu-sirgstoo-britu-hakeri-makkinnonu-tomr-izdos-savienotajm-valstm&catid=39:tehnoloijas&Itemid=59 [aplūkots 2009. gada 29. novembrī]
11. Valsts policijas 2007. gada pārskats. http://www.vp.gov.lv/?sadala=189 [aplūkots 2010. gada 01. oktobrī]
12. Valsts policijas 2008. gada pārskats. http://www.vp.gov.lv/?sadala=189 [aplūkots 2010. gada 01. oktobrī]
13. Valsts policijas 2009. gada pārskats. http://www.vp.gov.lv/?sadala=189 [aplūkots 2010. gada 04. oktobrī]
14. Krievijas IeM "K" nodaļa. http://www.mvd.ru/struct/10000220/ [aplūkots 2010. gada 16. oktobrī]
15. Sicherheitskompass. http://www.polizeiberatung.de/vorbeugung/gefahren_im_internet/sicherheitskompass/ [aplūkots 2010. gada 11. oktobrī]
16. Terminoloģijas portāls. http://termini.letonika.lv/, [aplūkots 2010. gada 19. oktobrī]
17. Latvijas tiesu portāls. http://www.tiesas.lv/index.php?id=2044 [aplūkots 2010. gada 20. oktobrī]
18. LR IeM Informācijas centrs. Kriminālā statistika. http://www.ic.iem.gov.lv/?q=lv/node/75 [aplūkots 2010. gada 20. oktobrī]
19. Skolēns ar vienu klikšķi var pakļaut skolu kiberuzbrukumiem. http://www.apollo.lv/portal/news/articles/216479 [aplūkots 2010. gada 22. oktobrī]
20. Lielbritānijā par vērienīgu internetkrāpniecību apsūdzēti arī hakeri no Latvijas. http://www.apollo.lv/portal/news/articles/215980 [aplūkots 2010. gada 30. septembrī]
21. Pirms vēlēšanām aģentūra LETA pārvar kiberuzbrukumu. http://www.apollo.lv/portal/news/articles/216089 [aplūkots 2010. gada 01. oktobrī]
22. Hakeri izgudrojuši shēmu, kā inficēt datorus caur "YouTube". http://www.apollo.lv/portal/news/articles/206049 [aplūkots 2010. gada 15. jūnijā]

23. Hakeri nozaguši augsti stāvošu “iPad” īpašnieku elektroniskās adreses. http://www.apollo.lv/portal/news/articles/205775 [aplūkots 2010. gada 11. jūnijā]
24. Noticis kārtējais uzbrukums “Facebook” lietotājiem. http://www.apollo.lv/portal/news/articles/204960 [aplūkots 2010. gada 06. martā]
25. Saniknots datortīklu administrators iznīcinājis Moldovas sporta arhīvu. http://www.apollo.lv/portal/news/articles/218760 [aplūkots 2010. gada 28. oktobrī]
26. Я. Омельченко. Киберполиция: про поимку хакера Нео, аферы на one.lv торговлю спамом. http://www.kriminal.lv/news/kiber-policiya-pro-poimku-hakera-neo-afery-na-one-lv-i-torgovlyu-spamom [aplūkots 2010. gada 22. oktobrī]
27. I. Poikāns. Vienkārši par Neo stratēģiju. http://213.175.75.4/hot/?rid=41090. [aplūkots 2010. gada 22. novembrī]
28. Soroka. Vai kibernoziedzība ir nopietns drauds Latvijas attīstībai. http://www.saki.lv/viedokli/462-vai-kibernoziedzba-ir-nopietns-drauds-latvijas-attstbai [aplūkots 2010. gada 09.septembrī]
29. IT eksperti: par VID datu noplūdi jāatbild valdībai. http://www.apollo.lv/portal/news/articles/208923 [aplūkots 2010. gada 20. augustā]

Normatīvie akti

1. 23.11.2001. "Konvencija par kibernoziegumiem” ("LV", 171 (3539), 26.10.2006.) [stājās spēkā 01.06.2007.]
2. 02.05.2002. likums "Valsts informācijas sistēmu likums" ("LV", 76 (2651), 22.05.2002.) [stājās spēkā 05.06.2002.]
3. 17.06.1998. likums "Krimināllikums" ("LV", 199/200 (1260/1261), 08.07.1998.) [stājās spēkā 01.04.1999.]
4. 28.04.2005. likums "Grozījumi Krimināllikumā" ("LV", 78 (3236), 18.05.2005.) [stājās spēkā 01.06.2005.]
5. 28.10.2004. likums "Elektronisko sakaru likums" ("LV", 183 (3131), 17.11.2004.) [stājās spēkā 01.12.2004.]
6. 07.12.1984. likums "Latvijas Administratīvo pārkāpumu kodekss" (Ziņotājs, 51, 20.12.1984.) [stājas spēkā 01.07.1985.]
7. 11.10.2005. MK noteikumi Nr. 765 “Valsts informācijas sistēmu vispārējās drošības prasības” ("LV", 164 (3322), 14.10.2005.) [stājās spēkā 15.10.2005.]

8. 15.12.2009. MK noteikumi Nr. 1445 “Kritisku valsts informācijas sistēmu un valsts informācijas sistēmu savietotāju aizsardzības prasības” ("LV", 200 (4186), 21.12.2009.) [stājās spēkā 01.01.2010.]
9. 22.12.2009. MK instrukcija Nr.20 "Valsts pārvaldes funkciju izpildi apdraudošu kiberuzbrukumu noteikšanas instrukcija" ("LV", 203 (4189), 28.12.2009.) [stājas spēkā 29.12.2009.]
10. MK rīkojums Nr. 248 “Par Pašvaldību vienotās informācijas sistēmas attīstības koncepciju 2010. – 2013. gadam” ("LV", 73 (4265), 11.05.2010.) [stājās spēkā 06.05.2010.]

Tiesu prakse

1. Latvijas Republikas Augstākās tiesas Senāta Krimināllietu departamenta 2006. gada 18. janvāra lēmums lietā SKK – 01- 0007/06.
2. Latvijas Republikas Augstākās tiesas Senāta Krimināllietu departamenta 2006. gada 11. septembra lēmums lietā SKK – 410/2006.

Pielikumi

Pielikums Nr.1

Anketa sabiedriskajai aptaujai par tēmu „kibernoziegumi".

1) Jūsu dzimums:
- ☐ S
- ☐ V

2) Vecuma grupa:
- ☐ 18 - 20
- ☐ 21 - 30
- ☐ 31 - 40
- ☐ 40 +

3) Kāda ir jūsu attieksme pret "*hakeriem*"?
- ☐ Pozitīva
- ☐ Negatīva
- ☐ Vienaldzīga

4) Cik ilgu laiku jūs pavada pie datora?
- ☐ Līdz 5h dienā
- ☐ Līdz 10 h dienā
- ☐ Virs 10h

5) Ko persona saprot ar tādiem vārdiem, kā „*kibernoziegums*" vai „*datornoziegums*"?

6) Kādas sekas pēc personas domām izraisa kibernoziegumi?

7) Vai jūsuprāt kiberapdraudējumi pārsvarā nāk no:
- ☐ Latvijas
- ☐ Krievijas
- ☐ ASV
- ☐ Cits variants: _____

8) Vai kibernoziegumus ir viegli atklāt?
- ☐ Jā
- ☐ Nē
- ☐ Neiespējami

9) Vai uzskatāt, ka esat izdarījuši darbību, kas skaitītos "datornoziegums" un vai ir par tāda veida noziegumiem kādreiz saukta pie atbildības?

10) Kādus savus datus jūs vēlētos aizsargāt kiberapdraudējuma gadījumā (*piem., ja kāds būtu piekļuvis jūsu datorā esošai informācijai*)?

11) Vai izmantojat kādas datu bāzes, informācijas sistēmas?

12) Kādā veidā jūs aizsargājat savu datoru / informācijas sistēmu pret tā uzlaušanu? (*Ja tiek izmantotas speciālas programmas, tad vai tās ir licencētas?*)

13) Vai jūsu darba vietā ir bloķēta piekļuve kādām interneta vietnēm (piem., *www.draugiem.lv, u.c.)* ?

14) Vai jums ir izdevies piekļūt kādai darba vietā bloķētai interneta vietnei citādākā veidā? (*Kādā?*)

15) Kā jums šķiet, vai kādā no Valsts informācijas sistēmām ir jūsu dati?

Anketas sabiedriskajai aptaujai par tēmu „kibernoziegumi" rezultātu apkopojums

Bakalaura darba izstrādes laikā tika aptaujātas 59 personas. Tostarp arī 7 (11,9%) Vācijas iedzīvotāji, starp kuriem 3 sievietes un 4 vīrieši, kuru atbildes, tiek iekļautas kopējo atbilžu skaitā. Pavisam aptaujāti 18 vīrieši (30,5%) un 41 sieviete (69,5%). Starp aptaujātajām personām aptaujāti tiesu darbinieki, apdrošināšanas firmas darbinieki, skolnieki, studenti, to skaitā arī juridiskās un datorzinātņu fakultātes studenti, garāmgājēji.

Uz 2. jautājumu, vecuma grupu sadalījums ir sekojošs:

Vecuma grupa	**Sieviešu skaits**	**Vīriešu skaits**
18-20 gadi	2 (3,4%)	2 (3,4%)
21-30 gadi	25 (42,4%)	10 (16,9%)
31-40 gadi	7 (11,9%)	3 (5,1%)
Virs 40 gadiem	7 (11,9 %)	3 (5,1%)

Zemāk atbildes procentuāli tiks grupētas pēc dzimuma un vecuma apakšgrupās.

Sieviešu atbilžu varianti

Uz 3.jautājumu: „Kāda ir jūsu attieksme pret "*hakeriem*"?":

	Pozitīva	**Negatīva**	**Vienaldzīga**
18-20 gadi	-	50%	50%
21-30 gadi	12%	36%	52%
31-40 gadi	14,3%	28,6%	57,1%
Virs 40 gadiem	-	57,1%	42,9%

Uz 4.jautājumu: „Cik ilgu laiku jūs pavada pie datora?"

	Līdz 5h/d	**Līdz 10h/d**	**Virs 10h**
18-20 gadi	100%	-	-
21-30 gadi	24%	56%	20%
31-40 gadi	-	100%	-
Virs 40 gadiem	42,9%	42,9%	14,2%

Uz 5. jautājumu: „Ko persona saprot ar tādiem vārdiem, kā „kibernoziegums" vai „datornoziegums"?"

	IS drošības jomā	**Nav izpratnes**	**Datorsaistīti noziegumi**	**Noziegums informācijas pārraides procesā**
18-20 gadi	100%	-	-	-
21-30 gadi	60%	12%	24%	4%

31-40 gadi	57,1%	14,3%	14,3%	14,3%
Virs 40 gadiem	57,1%	-	42,9%	-

Uz 6. jautājumu: „Kādas sekas pēc personas domām izraisa kibernoziegumi?"

	Nezina	**Finansiālas**	**Manipulācija ar informāciju**	**Kriminālā atbildība**	**Tehnikas bojājumi**	**Morālas**
18-20 gadi	50%	50%	-	-	-	-
21-30 gadi	16%	12%	49%	14,3%	14,3%	24%
31-40 gadi	0	0	57,1%	14,3%	-	28,6%
Virs 40 gadiem	57,1%	14,3%	-	14,3%	14,3%	-

Uz 7. jautājumu: „Kibernoziegumi pārsvarā nāk no?"

	Latvijas	**Krievijas**	**ASV**	**Visām valstīm**	**ASV+Krievija**	**Nezina**	**Āzija**
18-20 gadi	-	-	50%	50%	-	-	-
21-30 gadi	4%	12%	32%	28%	16%	4%	4%
31-40 gadi	0	14,3%	14,3%	28,6%	42,9%	-	-
Virs 40 gadiem	-	14,3%	42,9%	28,6%	-	-	14,3%

"*Ķīna, Indija.*"

Uz 8. jautājumu: „Vai kibernoziegumus ir viegli atklāt?"

	Jā	**Nē**	**Neiespējami**	**Nezina**
18-20 gadi	50%	50%	-	-
21-30 gadi	-	92%	-	8%
31-40 gadi	-	100%	-	-
Virs 40 gadiem	-	100%	-	-

Uz 9. jautājumu: vai persona uzskata, ka ir izdarījusi kibernoziegumu?

	Jā	**Nē**	**Nezina**
18-20 gadi	-	100%	-
21-30 gadi	24%	68%	8%
31-40 gadi	85,7%	14,3%	-
Virs 40 gadiem	28,3%	71,4%	-

Uz 10. jautājumu – kādus savus datus persona vēlētos aizsargāt kiberapdraudējuma gadījumā:

	Visus	**Dokumenti (darba, mācību)**	**Foto, saraksti**	**Kodus (bankas, u.c.)**	**Neglabā tādus datus datorā**
18-20 gadi	100%	-	-	-	-
21-30 gadi	56%	8%	20%	12%	4%
31-40 gadi	57,2%	-	14,3%	14,3%	14,3%
Virs 40 gadiem	71,4%	14,3%	14,3%	-	-

„Uzrakstītos spriedumus, lēmumus."

Uz 11. jautājumu – vai persona izmanto datu bāzes vai informācijas sistēmas?:

	Jā	**Nē**	**Nezina**
18-20 gadi	50%	50%	-
21-30 gadi	80%	16%	4%
31-40 gadi	100%	-	-
Virs 40 gadiem	57,1%	-	42,9%

„Google, Skype."(kas nav IS)
„Universitātes IS."
„TIS, Lursoft, NAIS"

Uz 12. jautājumu – kādā veidā persona aizsargā savu datoru no kiberapdraudējumiem:

	Par to domā speciālisti	**Nelicencēts antivīruss**	**Nekā**	**Nezina**	**Bezmaksas antivīruss**	**Licencēts antivīruss**
18-20 gadi	-	-	50%	-	-	50%
21-30 gadi	8%	12%	36%	12%	12%	20%
31-40 gadi	28,6%	-	28,6%	28,6%	14,3%	-
Virs 40 gadiem	-	-	14,3%	14,3%	14,3%	57,1%

Uz 13. jautājumu – vai darba vietā ir bloķēta piekļuve kādām interneta vietnēm?:

	Jā	**Nē**	**Nezinu**	**Nav darba**
18-20 gadi	50%	50%	-	-
21-30 gadi	76%	16%	-	8%
31-40 gadi	85,7%	-	14,3%	-
Virs 40 gadiem	57,1%	28,6%	14,3%	-

Uz 14. jautājumu – vai ir izdevies piekļūt darba vietā bloķētai interneta vietnei savādāk?:

	Jā	**Nē**	**Nezinu**	**Nav darba**
18-20 gadi	-	100%	-	-
21-30 gadi	36%	56%	-	8%
31-40 gadi	42,9%	57,1%	-	-
Virs 40 gadiem	28,6%	57,1%	14,3%	-

„Īpašā veidā, kas zināms visiem pārējiem darbiniekiem."
„Izmantojot skaitlisko adresi."

Uz 15. jautājumu – vai personai šķiet, ka valsts informācijas sistēmā ir tās dati?:

	Jā	**Nē**	**Nezinu**
18-20 gadi	100%	-	-
21-30 gadi	92%	-	8%
31-40 gadi	71,4%	-	28,6%
Virs 40 gadiem	85,7%	-	13,4%

„Iedzīvotāju reģistrā, VSAA, VID, PMLP."

"Zemesgrāmata"

Vīriešu atbilžu varianti

Uz 3.jautājumu: „Kāda ir jūsu attieksme pret "*hakeriem*"?":

	Pozitīva	**Negatīva**	**Vienaldzīga**
18-20 gadi	50%	-	50%
21-30 gadi	30%	20%	50%
31-40 gadi	-	66,7%	33,3%
Virs 40 gadiem	-	100%	-

Uz 4.jautājumu: „Cik ilgu laiku jūs pavada pie datora?"

	Līdz 5h/d	**Līdz 10h/d**	**Virs 10h**
18-20 gadi	-	100%	-
21-30 gadi	20%	60%	20%
31-40 gadi	-	100%	-
Virs 40 gadiem	66,7%	33,3%	-

Uz 5. jautājumu: „Ko persona saprot ar tādiem vārdiem, kā „kibernoziegums" vai „datornoziegums"?"

	IS drošības jomā	**Nav izpratnes**	**Datorsaistīti noziegumi**	**Noziegums informācijas pārraides procesā**
18-20 gadi	50%	-	50%	-
21-30 gadi	70%	-	30%	-
31-40 gadi	100%	-	-	-
Virs 40 gadiem	66,7%	33,3%	-	-

Uz 6. jautājumu: „Kādas sekas pēc personas domām izraisa kibernoziegumi?"

	Nezina	**Finansiālas**	**Manipulācija ar datiem**	**Kriminālā atbildība**	**Tehnikas bojājumi**	**Morālas**
18-20 gadi	-	-	50%	50%	-	-
21-30 gadi	10%	40%	10%	10%	30%	-
31-40 gadi	33,3%	-	33,3%	-	-	33,3%
Virs 40 gadiem	-	33,3%	-	-	-	66,7%

„Datu noplūde no maza uzņēmuma var tam nemaksāt neko, bet lielam uzņēmumam tas var maksāt miljonus".

Uz 7. jautājumu: „Kibernoziegumi pārsvarā nāk no?"

	Latvijas	**Krievijas**	**ASV**	**Visām valstīm**	**ASV+Krievija**	**Nezina**	**Āzija**
18-20 gadi	-	50%	50%	-	-	-	-
21-30 gadi	-	40%	10%	40%	-	-	10%

31-40 gadi	-	33,3%	66,7%	-	-	-	-
Virs 40 gadiem	-	-	33,3%	33,3%	-	33,3%	-

Uz 8. jautājumu: „Vai kibernoziegumus ir viegli atklāt?”

	Jā	**Nē**	**Neiespējami**	**Nezina**
18-20 gadi	-	100%	-	-
21-30 gadi	-	90%	10%	-
31-40 gadi	-	33,3%	66,7%	-
Virs 40 gadiem	33,3%	33,3%	33,3%	-

Uz 9. jautājumu: vai persona uzskata, ka ir izdarījusi kibernoziegumu?

	Jā	**Nē**	**Nezina**
18-20 gadi	50%	-	50%
21-30 gadi	50%	50%	-
31-40 gadi	-	100%	-
Virs 40 gadiem	-	100%	-

Uz 10. jautājumu – kādus savus datus persona vēlētos aizsargāt kiberapdraudējuma gadījumā:

	Visus	**Dokumenti (darba, mācību)**	**Foto, saraksti**	**Kodus (bankas, u.c.)**	**Neglabā tādus datus datorā**
18-20 gadi	50%	-	-	-	50%
21-30 gadi	50%	-	-	40%	10%
31-40 gadi	-	66,7%	-	-	33,3%
Virs 40 gadiem	100%	-	-	-	-

Uz 11. jautājumu – vai persona izmanto datu bāzes vai informācijas sistēmas?:

	Jā	**Nē**	**Nezina**
18-20 gadi	50%	50%	-
21-30 gadi	60%	30%	10%
31-40 gadi	66,7%	33,3%	-
Virs 40 gadiem	33,3%	-	66,7%

„Sarkanā Krusta IS.”

Uz 12. jautājumu – kādā veidā persona aizsargā savu datoru no kiberapdraudējumiem:

	Par to domā speciālisti	**Nelicencēts antivīruss**	**Nekā**	**Nezina**	**Bezmaksas antivīruss**	**Licencēts antivīruss**
18-20 gadi	-	50%	50%	-	-	-
21-30 gadi	-	20%	10%	10%	20%	40%
31-40 gadi	-	-	33,3%	-	-	66,7%
Virs 40 gadiem	-	-	-	-	33,3%	66,7%

„Bezmaksas interneta antivīruss domāju, ka ir legāls, ja jau tiek piedāvāts visiem.”
„Fiziskā aizsardzība – slēgtas durvis, divi suņi, signalizācija.”

Uz 13. jautājumu – vai darba vietā ir bloķēta piekļuve kādām interneta vietnēm?:

	Jā	**Nē**	**Nezinu**	**Nav darba**
18-20 gadi	100%	-	-	-
21-30 gadi	40%	50%	-	10%
31-40 gadi	66,7%	33,3%	-	-
Virs 40 gadiem	33,3%	33,3%	33,3%	-

„Sakarā ar to, ka tas pasliktinot darba produktivitāti."

Uz 14. jautājumu – vai ir izdevies piekļūt darba vietā bloķētai interneta vietnei savādāk?:

	Jā	**Nē**	**Nezinu**	**Nav darba**
18-20 gadi	100%	-	-	-
21-30 gadi	60%	40%	-	-
31-40 gadi	33,3%	66,7%	-	-
Virs 40 gadiem	-	100%	-	-

„Izmantojot zināmu ciparu kombināciju, ko (kuru uztaisījusi administrācija, lai pati varētu iet draugos) un kuru zina visi kolēģi."
„Nevar teikt."
"Interneta plūsmas tunelēšana."

Uz 15. jautājumu – vai personai šķiet, ka valsts informācijas sistēmā ir tās dati?:

	Jā	**Nē**	**Nezinu**
18-20 gadi	100%	-	-
21-30 gadi	90%	10%	-
31-40 gadi	66,7%	-	33,3%
Virs 40 gadiem	100%	-	-

„Kad ārzemēs strādāju, tad ārvalstu policijas IS."
„Policijas IS, jo man ir ieroča nēsāšanas atļauja."
„Noteikti, ka ir iedzīvotāju reģistram, VID arī, droši vien, ka NEO arī gan jau ka ir."
„Ir, un tā nav pienācīgi aizsargāta."

Pielikums Nr. 3

Jautājumi ekspertiem par tēmu "Noziedzīgu nodarījumu informācijas sistēmu drošības jomā krimināltiesiskie un kriminoloģiskie aspekti"

1. Kādas institūcijas nodrošina informācijas sistēmu drošību Latvijā? Vai ir kāda koordinējošā institūcija?
2. Kas ir "kiberpolicija" Latvijā, kam tā ir pakļauta un kādi ir tās galvenie darbības virzieni?
3. Kāda ir noziedzīgu nodarījumu informācijas sistēmu drošības jomā (*KL 241-245.p.*) statistika uz no 2007. gada līdz šim brīdim? Vai Informācijas centra sniegtā un tiesu statistika atspoguļo reālo situāciju noziedzīgu nodarījumu informācijas sistēmu drošības jomā?
4. Vai ir jūtams pieaugums noziedzīgu nodarījumu informācijas sistēmu drošības jomā? Vai ir jūtams pieaugums kādos konkrētos nodarījumu veidos?
5. Vai noziedzīgu nodarījumu informācijas sistēmu drošības jomā ir viegli atklāt?
6. Kā tiek īstenota noziedzīgu nodarījumu informācijas sistēmu drošības jomā prevence Latvijas mērogā?
7. Kā tiek īstenota noziedzīgu nodarījumu informācijas sistēmu drošības jomā prevence ārvalstīs?
8. Vai Latvijas hakeri gūst panākumus īstenojot kiberuzbrukumus informācijas sistēmām?
9. Vai noziedzīgajiem nodarījumiem informācijas sistēmu drošības jomā ir tendence pieaugt svarīgu valstisku notikumu laikā, piemēram, pirms vēlēšanām?
10. Kādas valsts informācijas sistēmas jūs varētu raksturot kā "kritiskas valsts IS"?
11. Vai Neo ir radījis būtisku kaitējumi, ielaužoties VID EDS?
12. Vai VID EDS ir kritiskas valsts IS pazīmes?
13. Vai ir kādi tieši Latvijas IS sistēmām raksturīgas īpašības, kas tās pakļauj riskam atšķirībā no citu valstu IS?
14. Latvijā "kibernoziegumus" regulē KL 241-244.p. Vai normatīvo aktu regulējums ir pietiekams, lai aizsargātu Latvijas iedzīvotāju intereses noziedzīga nodarījuma, kas vērsts pret IS drošību, gadījumā?
    a. Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai
    b. Automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju

c. Nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm
d. Datu, programmatūras un iekārtu iegūšana, izgatavošana, izmainīšana, glabāšana un izplatīšana nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām
e. Informācijas sistēmas drošības noteikumu pārkāpšana

15. Kā jūs varētu raksturot noziedzīgu nodarījumu IS drošības jomā subjektus?
16. Vai kaitējuma konstatēšana ir obligāta, lai sauktu pie atbildības personu par svešas IS kompromitēšanu?
17. Kā uzņēmums var aizsargāt savas intereses, ja kaitējums pēc būtības nav konstatēts, bet ir veiktas darbības, kas nepārprotami apdraud informācijas sistēmu?
18. Kas ir CERT? Un kā tas darbojas?
19. Kas var vērsties pie CERT?
20. Kādas ir CERT attīstības tendences?

Pielikums Nr. 4

Jautājumi par tēmu "Noziedzīgu nodarījumu informācijas sistēmu drošības jomā krimināltiesiskie un kriminoloģiskie aspekti"

1. *Kādas institūcijas nodrošina informācijas sistēmu drošību Latvijā? Vai ir kāda koordinējošā institūcija?*

Šim jautājumam ir vairāki aspekti. Pirmkārt, par IT drošību iestādē atbild iestādes vadītājs vai īpaši pilnvarota persona (piemēram, drošības pārvaldnieks valsts IS gadījumā). Otrkārt, ir jānodala tās sistēmas, kurām IT drošība kā īpašs režīms ir obligāts pienākums (piemēram, Valsts IS, bankas IS), un sistēmas, kuru drošības režīmu un risku analīzi nosaka pats īpašnieks (piemēram, privātajā sektorā). Treškārt, līdz informācijas tehnoloģiju drošības likuma spēkā stāšanos, par IT drošību valstiskā līmenī atbild vairākas institūcijas (politiski – Satiksmes ministrija (izriet no Elektronisko sakaru likuma); RAPLM (izriet no VIS likuma); valsts pārvaldē – Datu valsts inspekcija; noziedzīgu nodarījumu prevencijā – Valsts policija un Drošības policija).

2. *Kas ir "kiberpolicija" Latvijā, kam tā ir pakļauta un kādi ir tās galvenie darbības virzieni?*

Grūti atbildēt, kas ir „kiberpolicija". Valsts policijas GKrPP EPP 4.nodaļa ir kriminālpolicijas struktūrvienība, tai piemīt kriminālpolicijas tradicionālas darba metodes un taktika.

3. *Kāda ir noziedzīgu nodarījumu informācijas sistēmu drošības jomā (KL 241-245.p.) statistika uz no 2007. gada līdz šim brīdim? Vai Informācijas centra sniegtā un tiesu statistika atspoguļo reālo situāciju noziedzīgu nodarījumu informācijas sistēmu drošības jomā?*

Manuprāt, pie noziedzīgiem nodarījumiem pret automatizētas datu apstrādes sistēmas drošību ir pieskaitāmi šādi noziedzīgu nodarījumu sastāvi (Krimināllikuma panti): 144.pants - Korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšana; 177.[1] pants - Krāpšana automatizētā datu apstrādes sistēmā; 193.[1] pants - Datu, programmatūras un iekārtu iegūšana, izgatavošana, izplatīšana, izmantošana un glabāšana nelikumīgām darbībām ar finanšu instrumentiem un maksāšanas līdzekļiem; 200.panta 2.daļa – Komercnoslēpumu saturošu ziņu neatļauta iegūšana un izpaušana un finanšu instrumentu tirgus iekšējās informācijas neatļauta izpaušana; 241.pants - Patvaļīga piekļūšana automatizētai 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; 245.pants - Informācijas sistēmas drošības noteikumu pārkāpšana.

2006.gadā valstī tika reģistrētas pavisam 75 krimināllietas, 2007.gadā – 47 krimināllietas un 2008.gada 10 mēnešos – 114. Pētot kibernoziedzības līmeni Latvijā, tās izplatību, dinamiku un attīstību, vitāli svarīgi izmantot Iekšlietu Ministrijas Informācijas centra datus par Latvijā reģistrētajiem noziedzīgajiem nodarījumiem. Ir jāatzīst, ka pat tik precīzi dati nevar sniegt patiesu ainu, jo ir jāņem vērā gan cilvēciskais faktors (piemēram, juridiski neprecīzi kvalificējot nodarījumu), gan likumu normu pilnveidošanu (piemēram, Kriminālprocesa likuma spēkā stāšanos, Krimināllikuma 28.04.2005.g. grozījumus u.c.), gan atsevišķu tiesību normu īpatnības (piemēram, Kriminālprocesa likuma 398.panta 1.daļa, kas nosaka, ka kriminālprocesu uzsākot, izmeklējamo rīcību var kvalificēt tikai pēc piederības pie noziedzīgu nodarījumu grupas objekta), gan kibernoziedzības augsto latentuma līmeni utt.

4. *Vai ir jūtams pieaugums noziedzīgu nodarījumu informācijas sistēmu drošības jomā? Vai ir jūtams pieaugums kādos konkrētos nodarījumu veidos?*

Katru gadu ir vērojams EPP 4.nodaļā uzsākto kriminālprocesu skaita pieaugums par aptuveni 10% gadā. Analizējot konkrētus nodarījumus, var secināt, ka nepārtraukti pieaug reģistrētu noziedzīgu nodarījumu pret korespondences noslēpumu (KL 144.p.) un kaitīgu programmu izplatīšanas (KL 244.p.) skaits.

5. *Vai noziedzīgu nodarījumu informācijas sistēmu drošības jomā ir viegli atklāt?*

Viens no stereotipiem kibernoziegumu jomā ir tāds, ka kibernoziegumu izmeklēšana ir ļoti sarežģīts un darbietilpīgs process. Šis apgalvojums ir neprecīzs (apzinoties gan publiski pieejamu informāciju par šo noziegumu izmeklēšanu, kas ir apgūstama nedēļas laikā; gan izmeklēšanas programmnodrošinājuma esamību vairākos gadījumos sistematizējot darbības utt.) un „izņemts" no konteksta (analizējot birokrātisku un statisku starptautisko krimināltiesisko sadarbību kibernoziegumu krimināllietās). Viena no būtiskām problēmām ir personu nevelēšanās iedziļināties kibernoziegumu krimināllietas materiālos, kā rezultātā izvairoties no šīs lietas virzības. Interesanta šķiet ārvalstu pieredze tieši izskaidrošanas un demonstrēšanas jautājumā – tā piemēram, vairāki ārvalstu tiesībaizsardzības iestāžu pārstāvji (piemēram, ASV FIB, Anglijas *SOCA* utt.) elektronisko pierādījumu iegūšanas laikā izmanto speciālu programmatūru, to manipulāciju fiksēšanai displeja darba virsmā. Vēlāk šie materiāli tiek uzrādīti prokuroriem un

tiesnešiem, tieši aprakstot izmeklējamo rīcību. Šāda prakse arī tiek iedzīvināta Latvijā, saskaņojot ar vietējo reglamentāciju.

6. *Kā tiek īstenota noziedzīgu nodarījumu informācijas sistēmu drošības jomā prevence Latvijas mērogā?*

Patlaban kibernoziegumu novēršanas aktivitātes Valsts policijas līmenī tiek organizētas šādos virzienos:

- darbs ar iedzīvotājiem (izmantojot masu saziņas līdzekļus, kā arī citas metodes);
- partnerattiecības ar elektronisko sakaru komersantiem;
- partnerattiecības ar kredītiestādēm;
- sadarbība ar Interneta publiskās pieejas punktu administrāciju;
- sadarbības ar Interneta resursu uzturētājiem;
- starptautiskā 24 stundu dienā un 7 dienu nedēļā sadarbība

Savukārt, Kibernoziedzības novēršanā var izdalīt šādas primāras problēmas:

- iedzīvotāju informētības līmenis, drošības rekomendāciju nepietiekamība;
- nacionālo tiesību atšķirības, izvairīšanas no starptautiskās sadarbības un pretrunīgie krimināltiesiskie principi;
- publiskā-privātā sektora partnerattiecību ieviešana;
- starptautiskā sadarbība 24/7 kontaktpunktu skatījumā;
- kriminoloģiskā plānošana, prognoze.

7. *Kā tiek īstenota noziedzīgu nodarījumu informācijas sistēmu drošības jomā prevence ārvalstīs?*

Pamatā tiek izmantots privātā-publiskā sektora partnerattiecību modelis. Tā piemēram, FIB Interneta noziegumu sūdzību centra "*FBI Internet Crime complaint center*" galvenie darba virzieni ir – 1) tika izveidota alianse NCFTA (*National Cyber-Forensics and Training Alliance*) – partnerattiecības starp privātstruktūrām (Interneta veikali un citi komersanti, Interneta izsoles, kredītiestādes, Interneta pakalpojumu sniedzēji utt), FIB Kibernoziegumu apkarošanas departamentu un tās nodaļām (nodaļas, kas cīnās ar bērnu pornogrāfijas izplatīšanu Internetā; ar „datoruzlaušanām"; ar Interneta krāpšanām; ar autortiesību pārkāpumiem; datortehnisko ekspertīžu nodaļa utt.), izglītības iestādēm. Šī alianse apstrādā visas sūdzības par Interneta un informācijas tehnoloģijas noziegumiem (krāpšanas, „uzlaušanas", intelektuālā īpašuma pārkāpumi, identifikācijas zādzības, "SPAM" surogātpasta vēstules, naudas „atmazgāšana" utt.),

šīs sūdzības tiek kopīgi analizētas (kā rezultātā privātstruktūras sniedz palīdzību un informāciju policijai aizsargājot savas sistēmas/pakalpojumus/klientus no tādiem pārkāpumiem) un pēc šīs analīzes informācija tiek oficiāli sniegta FIB Kibernoziegumu departamenta nodaļām turpmākam darbam; 2) – ciešā sadarbība ar bezpeļņas organizāciju "NW3C centrs" (*National White collar crime center* – "balto apkaklīšu noziegumu nacionālais centrs"), kas sniedz tehnisko palīdzību datu apstrādē.

8. *Vai Latvijas hakeri gūst panākumus īstenojot kiberuzbrukumus informācijas sistēmām?*

Kiberuzbrukumu kontekstā nevarēšu precīzi nodalīt Latvijas pārkāpējus no šī reģiona pārkāpējiem, jo viņu noziedzīgas saites ir ļoti ciešas un brīžiem nenodalāmas.

9. *Vai noziedzīgajiem nodarījumiem informācijas sistēmu drošības jomā ir tendence pieaugt svarīgu valstisku notikumu laikā, piemēram, pirms vēlēšanām?*

Ja runājam par drošības riskiem, tad noteikti pieaug.

10. *Kādas valsts informācijas sistēmas jūs varētu raksturot kā "kritiskas valsts IS"?*

Šo jautājumu patlaban mēģina risināt ministru kabineta līmenī, tāpēc pirms kāda lēmuma pieņemšanas negribētu izdarīt priekšlaicīgus secinājumus. Taču raugoties no kaitējuma, kādu var nodarīt šo sistēmu darbības apzināta traucēšana, var nepārprotami secināt, ka šis kaitējums valsts un tautsaimniecības interesēm mērojams lielos apmēros.

11. *Vai Neo ir radījis būtisku kaitējumi, ielaužoties VID EDS?*

Šis ir viens no apstākļiem, kas izmeklēšanā ir jāpamato.

12. *Vai VID EDS ir kritiskas valsts IS pazīmes?*

Uzskatu, ka ir.

13. *Vai ir kādi tieši Latvijas IS sistēmām raksturīgas īpašības, kas tās pakļauj riskam atšķirībā no citu valstu IS?*

Lai atbildētu, ir jāpārzina ārvalstu IT infrastruktūra, kas nereti ir ierobežotas pieejamības informācija.

14. *Latvijā "kibernoziegumus" regulē KL 241-244.p. Vai normatīvo aktu regulējums ir pietiekams, lai aizsargātu Latvijas iedzīvotāju intereses noziedzīga nodarījuma, kas vērsts pret IS drošību, gadījumā?*

Salīdzinot ar ārvalstīm, Latvijai ir viens no modernākajiem materiālo un procesuālo tiesību normu regulējumiem. Taču, protams, ir nepieciešami arī atsevišķi labojumi kļūdām, kas pieļautas normas ieviešot, vai problēmām, kas atklājās tiesību normu piemērošanas procesā. Taču, nevar

apgalvot, ka patlaban kāda no tiesību normām, vai šīs normas neesamība traucē kibernoziedzības apkarošanu.

15. Kā jūs varētu raksturot noziedzīgu nodarījumu IS drošības jomā subjektus?

Jautājums ir atsevišķa pētījuma vērts. Centīšos kodolīgi izklāstīt savu viedokli. Kibernoziedzniekus nosacīti var klasificēt šādās grupās:

- dažāda rakstura kibernodarījumus izdara esošie vai bijušie darbinieki, šo parādību risku speciālisti dēvē par iekšējo faktoru. Šiem cilvēkiem nav obligāti ir izcilas IT zināšanas, viņu kvalifikācija ir pietiekama konkrētu pienākumu pildīšanai. Pienākumu specifikas vai attiecīgas sistēmas vai datu neadekvātas aizsardzības dēļ, šiem cilvēkiem ir piekļuve konkrētiem datiem (bieži vien šādi dati tiek klasificēti kā komercnoslēpums vai dienesta informācija). Tie var būt godīgi darbinieki ar labiem nodomiem, kas, pateicoties nogurdinošai, neatbilstošai apmācībai vai nolaidībai, izdara netīšu darbību, iznīcinot ievērojamu datu daudzumu. Tie var būt arī neapmierināti vai negodīgi darbinieki, kas negodīgi izmanto atļauto pieeju sistēmai vai pārkāpj atļautās pieejas apjomu, lai tīši iejauktos sistēmā ar nolūku personīgi iedzīvoties vai radīt zaudējumus organizācijai.
- Personas, komersantos strādājošie darbinieki, kas pārkāpumus izdara aiz nevērības, neuzmanības, ziņkārības vai arī nepietiekamām zināšanām, nejauši veicot tādas darbības, kas nodara kaitējumu. Šādas rīcības piemēru ir pietiekoši daudz, kad persona darbojoties Internetā nejauši lejupielādējusi bērnu seksuālās izmantošanas materiālus; vai aktivizējot e-pasta vēstules pielikumu veicinājusi kaitīgas programmatūras izplatīšanu komerctīklā. Šajā grupā ietilpst arī tā saucamie „*script kiddies*", respektīvi, personas, kas izmanto kādu kaitīgu izstrādājumu (kodu vai programmnodrošinājumu) ziņkārības dēļ vai bez īpašas motivācijas.
- Profesionāli pārkāpēji – veicot nelikumīgas darbības vienatnē vai speciāli organizētajās grupās. Pārkāpumi pamatā izpaužas mantiska rakstura kriminālajās darbībās, piemēram, nelikumīgas darbības ar svešu personu maksāšanas līdzekļu datiem, krāpšanas, nelikumīgi iegūtu līdzekļu legalizācija, komerciāla rakstura bērnu seksuālās izmatošanas materiālu izplatīšana utt. Profesionāli noziedznieki bieži nav augsti kvalificēti IT speciālisti, viņi veic kādas noteiktas, nereti līdz automātismam iestrādātas darbības. Šādi pārkāpēji bieži ir kādas ķēdes vai grupas sastāvdaļa, veicot noteiktas darbības vai piedāvājot noteiktu pakalpojumu. Šādus cilvēkus mēdz izmantot arī tradicionālās noziedzības grupējumi.

- Entuziasti ar kreatīvām spējām. Šo grupu mēdz „stereotipiski" apzīmēt ar žargona vārdu *hakeri* („*hacker"*) jeb lauzēji. Vārdu *hakers* IT speciālisti sākotnēji izmantoja, apzīmējot augsti kvalificētu programmētāju, un līdz ar to šis vārds nekādi nebija attiecināts uz noziegumu izdarīšanu. Vēlāk ar šo vārdu apzīmēja kvalificētu kibernoziegumu izdarītāju (sadzīves līmenī arī joprojām), taču speciālistu vidū jau kādu laiku tas netiek izmantots noziedznieka raksturojumam, ar to apzīmē personas, kurām piemīt spējas nepārtraukti patstāvīgi pārbaudīt jaunas tehnoloģijas, paaugstināt savas zināšanas, apšaubīt aizsardzības efektivitāti kā tādu un meklēt aizsardzības pārvarēšanas iespējas. Jānorāda, ka šādas īpašības, protams, var izmantot tiesībpārkāpumu realizācijai, taču tā nav obligāta (lielākoties izņēmuma) prasība. Tāpēc šo kibernoziedznieku grupu šāda rakstura pētījumā ir vērts apzīmēt ar vārdu „lauzējs". Lauzējiem piemīt kvalificētas zināšanas IT jomā, kas atšķirībā no citiem speciālistiem neizpaužas kāda apstiprinoša sertifikāta vai diploma iegūšanā. Šīs personas aizsardzības jauninājumus vai kādas tehnoloģijas uztver kā izaicinājumu savu spēju pārbaudei un nepārtraukti cenšas atklāt kādu nepilnību, noziedzīgu motīvu dēļ.

16. Vai kaitējuma konstatēšana ir obligāta, lai sauktu pie atbildības personu par svešas IS kompromitēšanu?

Ne vienmēr. Krimināllikuma 244.panta sastāvs ir formāls, līdz ar to neprasa nekādas cēloņsakarības konstatāciju un pierādīšanu.

17. Kā uzņēmums var aizsargāt savas intereses, ja kaitējums pēc būtības nav konstatēts, bet ir veiktas darbības, kas nepārprotami apdraud informācijas sistēmu?

Ir jāaptaujā komersants, kas viņam tajā brīdī ir svarīgāks – nepieļaut lielāko kaitējumu un darīt visu apdraudējuma novēršanai vai sodīt pārkāpēju. Šis jautājums ir diezgan komplicēts, jo ir jāapsver visas pozīcijas (piemēram, kriminālmeklēšanas taktika, IT drošības pamatnostādnes utt.).

18. *Kas ir CERT? Un kā tas darbojas?*

CERT darbību regulēs informācijas tehnoloģiju drošības likums. Divos vārdos – publiskajām sektoram sadarbība ir obligāta, privātajām – ir vēlama.

19. Kas var vērsties pie CERT?

Arī likums. Jebkurš, kas saskārās ar incidentu.

20. *Kādas ir CERT attīstības tendences?*

To pietuvināšana akadēmiskajam sektoram – respektīvi, tas aizvien vairāk veiks pētniecisko darbu un uzkrās pieredzi.

Dokumentārā lapa

Bakalaura darbs "Noziedzīgu nodarījumu informācijas sistēmu drošības jomā krimināltiesiskie un kriminoloģiskie aspekti" izstrādāts LU Juridiskajā fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autore: Ingrīda Irguļska _____

Rekomendēju darbu aizstāvēšanai

Vadītājs: Dr. iur., docents Andrejs Vilks _____

Darbs iesniegts Krimināltiesisko zinātņu katedrā _____

Metodiķe: Iveta Balode _____

Darbs aizstāvēts bakalaura gala pārbaudījuma komisijas sēdē

_____ prot. Nr. ____, vērtējums __(_____)

Komisijas sekretāre: _____