Uldis Miķelsons. Informācijas sistēmu drošība

Mūsdienās grūti iedomāties tādu valsts pārvaldes institūcijas darbības vai uzņēmējdarbības jomu, kas tieši vai netieši nebūtu atkarīga no dažādiem informācijas tehnoloģiju (IT) resursiem. Turklāt pastāvīgi vērojama aizvien pieaugoša tendence gan valsts pārvaldi, gan uzņēmējdarbību sistēmiski saistīt ar elektroniskas informācijas apstrādi, pārraidi un uzglabāšanu. Daudzās valsts, pašvaldību vai nevalstiskās organizācijās un uzņēmumos tiek uzturētas datorizētas informācijas sistēmas (IS) elektroniskas informācijas apstrādei, notiek elektroniska saziņa gan organizāciju, uzņēmuma iekšienē, gan ar sadarbības partneriem, tajā skaitā starptautiskā mērogā. Mūsdienās sabiedrības dzīves kvalitatāte daudzās jomās faktiski ir kļuvusi būtiski atkarīga no tā, cik stabili, kvalitatīvi un droši ir lietotie IT risinājumi.

Tomēr daudzi cilvēki, kuru skaitā ir arī valsts pārvaldes institūciju un uzņēmumu vadošas amatpersonas, nav specializējušies IT drošības jomā, tāpēc nepārzina tos vai citus nozīmīgus aspektus IS veidošanai un uzturēšanai, kas ietekmē IS drošību. Dažkārt cilvēki mēdz paļauties uz lietotās programmatūras uzstādījumiem pēc noklusējuma, nepievērsdami daudz uzmanības konkrētās IS konfigurācijai, programmatūras atjaunošanai un drošības aspektu novērtēšanai.

Taču mūsdienās dažādi apdraudējumi informācijas sistēmām,[1] kas var arī radīt nozīmīgus kaitējumus, ir ļoti izplatīti. Nepieciešamību pastiprināti pievērst uzmanību IS drošībai noteic faktiskā situācija valsts pārvaldes institūciju, uzņēmumu, arī fizisko personu tiesisko un ekonomisko interešu aizsardzībā gan globālā, gan nacionālā, gan korporatīvā un lokālā mērogā.

Lai mazinātu apdraudējuma risku IS pareizai darbībai un elektroniskās informācijas konfidencialitātei, pieejamībai un integritātei, lietderīgi katrā organizācijā un uzņēmumā izstrādāt un praktiski ieviest informācijas sistēmas drošības noteikumus (ISDN), kas ietver gan juridiskus, gan organizatoriskus, gan metodiskus sistēmiski un visaptveroši izstrādātus risinājumus. Šiem noteikumiem jābūt integrētiem visas organizācijas, uzņēmuma drošības politikā, turklāt tiem jābūt dinamiskiem, pastāvīgi īstenojot IS drošības apdraudējumu auditu un risku analīzi, lai pilnveidotu ISDN nepieciešamajos aspektos, kā arī pastāvīgi jākontrolē to izpilde.

Šajā publikācijā aplūkoti pamataspekti, ko var apsvērt, valsts pārvaldes organizācijās vai uzņēmumos izstrādājot ISDN un pārraugot to piemērošanu. Pamatā te aplūkoti juridiskie un metodiskie aspekti, bet tehniskie aizskarti minimāli, jo to risināšana ir atkarīga no konkrētās IS īpatnībām.

[1] Šeit netiek skatīti tehniskie aspekti, tāpēc vieglākas uztveramības dēļ nav arī atsevišķi uzskatītas tehniskās iekārtas /sistēmas, kuras var būt apdraudētas, bet tā vietā lieto apvienojošu apzīmējumu „informācijas sistēmas". Kā zināms, apdraudēti ir gan personālie datori, gan serveri, gan mobilie telefoni (viedtelefoni), un visa veida automatizētas datu apstrādes sistēmas, kas aizvien plašāk tiek lietotas sabiedrībā – sākot ar bankomātiem, beidzot ar automašīnu un dažādu speciālu iekārtu vadības blokiem.

Informācijas sistēmu aizsardzības nozīme

Pirms uzsākt ISDN juridisko un metodisko aspektu izskatīšanu, sākumā lietderīgi novērtēt šī jautājuma nozīmi vispār.

Apsverot IS aizsardzības nozīmes problemātiku, sākotnēji var pievērst uzmanību, ka vairākas IS apdraudējumu formas mūsdienās dažkārt tiek pielīdzinātas pat terorismam.[2] Un politiskā līmenī runā pat par specifiska veida karu – *cyberwar*[3] vai *iWar*[4] vai *netwar*,[5] kā ceturtās paaudzes karu, kad zūd robežlīnija starp karu un mieru, jo tam raksturīgi t.s. *asimetriskie* uzbrukumi, kad lielu kaitējumu var nodarīt personu grupas vai pat atsevišķs cilvēks ar nesalīdzināmi mazākiem resursiem, nekā ir apdraudētajai valstij / organizācijai. Tēlaini izsakoties, iespējams nodarīt milzīgu kaitējumu, neizejot no savas istabas. Teroristiskas un ekstrēmiskas organizācijas,[6] un arī vairāku valstu specdienesti[7] šajā nolūkā IT resursus izmanto tāpēc, ka tas sniedz ārkārtīgi lielas iespējas, kas var būt vērstas pret visu mērķa valsts kritiskās infrastruktūras un sabiedrības pārvaldes sistēmu,[8] dēļ kā attīstīto valstu sabiedrību mūsdienās mēdz raksturot kā viegli ievainojamu *(vulnerable society)*. Terorismam un kriminālām darbībām radušies virkne jaunu, vilinošu mērķu – telekomunikāciju tīkli, energoapgādes un transporta sistēmu vadība, dispečeru dienesti un aizsardzības sistēmas, finanšu sistēmas, pilsētu apgādes, ražošanas un militārās loģistikas ķēdes, plašsaziņas līdzekļi utt.

Daudzpusīgā rakstura dēļ IS drošības jautājumi vairākkārt apspriesti dažādās starptautiskās organizācijās, tajā skaitā gan ANO līmenī (tur šie jautājumi deleģēti ekspertiem no IGF (*Internet Governance Forum*) un ITU (*International Telecommunication Union*)), gan Eiropas Padomē un Eiropas Savienībā, kur kopš 1999.gada pieņemti vairāki tiesību plānošanas dokumenti, gan Eiropas Drošības un sadarbības organizācijā OSCE, gan Ekonomiskās sadarbības un attīstības organizācijā OECD, gan arī NATO, kas pat izvērtējusi šādu apdraudējumu attiecināmību uz NATO dibināšanas

---

2 http://en.wikipedia.org/wiki/Cyber-terrorism

3 http://en.wikipedia.org/wiki/Cyber-warfare

4 Jēdzienu "iWar" lieto NATO, terminoloģiski nošķirot 'Internetā sakņotu karu' no kiberkara, informācijas kara vai elektromagnētiska uzbrukuma / aizsardzības kara paveidiem u.tml.: http://en.wikipedia.org/wiki/IWar
Tomēr terminu "iWar" mēdz lietot arī žurnālisti plašākā nozīmē: http://www.psycom.net/iwar.1.html

5 gopher://aerv.nl/0/english/computer/cyberwar/cyberwar.txt

6 Piemēram, organizācijas *al-Qaeda* apdraudējums kibervidē: http://news.bbc.co.uk/2/hi/americas/6197446.stm
Politiski motivēti bija arī koordinētie plašie kiberuzbrukumi NATO datoriem Kosovas konflikta laikā 1999.gadā, Igaunijai 2007.gadā, Gruzijai 2008.gadā u.c.

7 Piemēram, ASV izveidojusi militāru struktūrvienību *U.S. Cyber Command*, kā arī pilnveido jaunas paaudzes globālu informācijas tīklu *Global Information Grid* tieši nolūkā nodrošināt kibervidē militāros un izlūkošanas uzdevumus. Līdzīgi ir arī vairākās citās valstīs (saskaņā ar *McAfee* 2007.gada pētījumu – 120 valstīs), kaut arī ne visur to atklāj publiski. Tajā skaitā Ķīnā izveidots specializēts datortīkls *GhostNet* spiegošanas un kaitējuma nodarīšanai, kura darbība konstatēta Indijā, Vācijā, Apvienotajā Karalistē un ASV, taču Ķīnas varas pārstāvji noliedz saistību ar to: http://en.wikipedia.org/wiki/GhostNet
Izraēlas un Palestīnas konfliktam paralēli pastāvīgi tiek īstenoti arī apdraudējumi kibervidē: http://cyberwarfaremag.wordpress.com/2009/01/10/the-palestine-israeli-conflict-on-the-web/
Arī Apvienotās Karalistes tehniskās izlūkošanas dienesta GCHQ vadītājs atklāja, ka kiberkarš ir mūsdienu realitāte, t.sk. mēnesī notiek ap 1000 uzbrukumi britu valsts IS: http://www.reuters.com/article/idUSTRE69C2YS20101013

8 Cyber Security Strategy. / Cyber Security Strategy, Ministry of Defence, Estonia. – Tallinn, 2008. – 36 p.

līguma[9] 5.panta nosacījumu, 2010.gada maijā iekļaujot to jaunajā Stratēģiskajā koncepcijā un izskatot NATO Bukarestes samitā un Lisabonas samitā.

2008.gada 28.oktobrī Tallinā izveidotais NATO Kooperatīvais kiberdrošības centrs (*Centre of Excellence*),[10] kas ir militarizēta organizācija, kaut arī nav NATO komandcentra sastāvā, nodrošina IT jomas speciālistu veiktu izpēti NATO kritiskās infrastruktūras IS kiberdrošības jautājumos, apdraudējumu analīzi un pretdarbības – kiberdrošības apdraudējumiem – stratēģijas, taktisko un tehnisko metožu (t.sk. ielaušanās atklāšanas, modelēšanas, tīkla monitoringa līdzekļu utt.) izstrādi, kā arī sekmē starpinstitucionālu un starptautisku sadarbību un apmācību šajā jomā, ieskaitot arī konferenču organizēšanu. Ik gadu tas arī rīko mācības, piemēram, «Kiberkoalīcija 2010» simulē daudzus vienlaicīgus kiberuzbrukumus NATO un alianses dalībvalstīm, lai pārbaudītu to stratēģisko lēmumu pieņemšanas procesu. Šo centru finansē un tajā līdzdarbojas septiņas NATO dalībvalstis, t.sk. Latvija. NATO arī nolēma izveidot ātrās reaģēšanas komandu, kas, līdz 2013.gadam nodrošinot pilnīgu pārklājumu, palīdzēs jebkurai NATO valstij cīnīties pret kiberuzbrukumiem, kā arī pati būs gatava veikt kiberuzbrukumus. Te var piebilst, ka pirms Lisabonas samita NATO Kiberaizsardzības un pretpasākumu nodaļas vadītājs atzina, ka kiberuzbrukumu draudi ir pastāvīgi un NATO aliansei ik dienu notiek līdz 100 kiberuzbrukumiem.

Eiropas Savienības telekomunikāciju ministri ir apstiprinājuši priekšlikumu izveidot institūciju, kas atbildīga par drošības vairošanu internetā. Eiropas Tīklu un informācijas drošības aģentūra ENISA[11] konsultēs regulējošās institūcijas par riskiem, kas apdraud elektroniskās sistēmas, un risinās ar datoraparatūru un programmatūras produktiem saistītas problēmas, kā arī sadarbībā ar dalībvalstīm organizēs regulāras mācības reaģēšanai uz kiberapdraudējumiem. interneta drošības jautājumos šī aģentūra sadarbosies arī ar ES blokā neietilpstošajām valstīm un organizācijām. 2010.gadā novembrī ES definēja ES iekšējās drošības stratēģiju, kur starp vairāku cita veida apdraudējumu novēršanas mērķiem uzmanība pievērsta arī kiberdrošībai. Tajā skaitā līdz ar iepriekšējo pasākumu turpināšanu paredzēts, ka līdz 2012.gadam ne vien katrā dalībvalstī, bet pašās ES institūcijās izveidos CERT jeb reaģēšanas grupas datorapdraudējumu gadījumos, kuras savstarpēji sadarbosies. Bez tam līdz 2013.gadam paredzēts izveidot Eiropas informācijas apmaiņas un brīdināšanas sistēmu EISAS.[12]

Arī nacionālā līmenī IS drošības jautājumiem velta daudzpusīgu uzmanību – tie tiek iekļauti valsts politikas plānošanas dokumentos, tiem pievēršas ne vien IT jomas speciālisti, bet arī nevalstiskās organizācijas, tos apgūst uzņēmējdarbības vadības programmās, ieteikumi šajā jomā tiek sniegtas iedzīvotājiem ar plašsaziņas līdzekļu starpniecību utt.

---

9 The North Atlantic Treaty / Washington D.C. - 4 April, 1949. http://www.nato.int/cps/en/natolive/official_texts_17120.htm

10 http://www.ccdcoe.org/

11 http://www.enisa.europa.eu/

12 http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf

Tomēr neapšaubāmi efektīvs drošības risinājums interneta vidē vispār nav iespējams, jo pārmērīga kontrole vienlaikus nozīmē cilvēku brīvību nepieļaujamu ierobežošanu.[13] Vienu no šajā ziņā būtiskiem jautājumiem minēja Edvīns Karnītis publikācijā «Interneta regulēšana: gatavojot Latvijas pozīciju ANO darba grupai atbilstīgi Vispasaules informācijas sabiedrības sammita deklarācijai», kas publicēta Sabiedrisko pakalpojumu regulēšanas komisijas mājaslapā: «Pretrunīga, taču diskutējama ir ideja par identifikācijas koda ieviešanu katram interneta lietotājam, kas, izslēdzot anonīmas pieejas iespējas, disciplinētu lietotājus un paaugstinātu viņu atbildību par savām darbībām, paaugstinātu drošības līmeni, tomēr vienlaikus pavājinātu privātuma aizsardzību.» Turpat E.Karnītis iezīmē arī citu problēmu: «2001.gada 11.septembra notikumi parādīja, ka internetā ir brīvi pieejama detalizēta informācija, kas ir ļoti noderīga teroristiem – par bīstamām ķimikālijām, pilsētu dzeramā ūdens apgādi, naftas un gāzes cauruļvadiem, kodolobjektiem, radioaktīvo materiālu transportu un pat reaktīvo lidmašīnu pilotu trenažieri».

IS drošības politikas, kā nacionālās drošības politikas elements, pamatprincipi iestrādāti arī Latvijas Republikas *Nacionālās drošības koncepcijā.* Tajā skaitā 2010.gada 24.augustā apstiprinātā koncepcija noteic, ka «informācijas tehnoloģiju apdraudējuma novēršanas jomā Latvijas stratēģiskais mērķis ir nodrošināt informācijas tehnoloģiju drošību, kā arī pilnveidot esošos aizsardzības mehānismus, samazinot t.s. cilvēciskā faktora radītos riskus informācijas tehnoloģiju izmantošanā. Latvijas prioritātes kibertelpā esošo apdraudējumu novēršanai ir tiesiskā regulējuma pilnveidošana, starpinstitucionālās un starptautiskās sadarbības pilnveidošana, apdraudējuma identificēšanas un reaģēšanas pilnveidošana un informācijas tehnoloģiju lietotāju zināšanu pilnveidošana.»[14]

IS drošības nosacījumi reglamentēti arī *Krimināllikumā*, t.sk. tā 245.pantā paredzot noziedzīgu nodarījumu «Informācijas sistēmas drošības noteikumu pārkāpšana»; nepieciešamās normas iestrādātas arī citos normatīvajos aktos: Likumā par valsts noslēpumu, Fizisko personu datu aizsardzības likumā, Valsts informācijas sistēmu likumā u.c., būtiski principi iestrādāti arī dažādos Latvijas IT projektos un to praktiskos risinājumos.

Līdzīgi kā citās valstīs, arī Latvijā izveidota institūcija, kuras kompetencē ir IS drošības incidentu novēršana valsts informācijas sistēmās – Valsts informācijas tīkla aģentūra[15] izveidoja Datoru drošības incidentu reaģēšanas vienību[16] (analoģisku US-CERT jeb *Computer Emergency Readiness Team*), kas īsteno virkni valsts un pašvaldību institūciju IS aizsardzības uzdevumus, kā arī informācijas pārraides drošumu Valsts nozīmes datu pārraides tīklā. Atbilstīgus uzdevumus

[13] Tas jau izraisa asociācijas ar Džordža Orvela antiutopisko romānu «1984». Pret to vēršas arī cilvēktiesību organizācijas, t.sk. nosaucot valstis, kurās tiek ierobežota saziņas brīvības internetā. Piemēram, Ķīnā tiek ieviesta prasība identificēt gan visus mobilo telefonu lietotājus, gan interneta lietotājus. Līdzīgi ir arī vairākās islāma valstīs.

[14] http://polsis.mk.gov.lv/LoadAtt/file55886.doc

[15] Likvidējot šo aģentūru, 2010.gadā tās funkcijas nodotas Latvijas Valsts radio un televīzijas centram, bet pārejas periodā DDIRV funkcijas nodotas Satiksmes ministrijai. Turpmāk to regulēs saskaņā ar *Informācijas tehnoloģiju drošības pārvaldības likumu*.

[16] http://www.ddirv.lv/

vairākos Latvijas mērogā nozīmīgos privātos tīklos risina Latvijas Universitātes Matemātikas un informātikas institūta Tīklu risinājumu daļas struktūrvienība CERT-NIC.LV,[17] kas ir arī atbilstīga starptautiska foruma FIRST[18] biedrs.

Neapšaubāmi, IS drošība vienlīdz svarīga ir gan valsts un pašvaldību institūcijām, gan arī uzņēmumiem.

Dažādi IS apdraudējumi, t.sk., kaitīgu programmu (*vīrusu, tārpu, Trojas zirgu* u.tml.) izplatīšana, datorurķu (*hackers*), kredītkaršu viltotāju (*carders*), datorkrāpnieku un interneta vandāļu *(script kiddies)* aktivitātes mūsdienās bieži ir vērstas uz ekonomiska labuma gūšanu, piemēram, ar uzņēmuma vai privātpersonas finanšu norēķinos izmantotās informācijas ieguvi.

Turklāt IS drošības apdraudējumi, ja tie kļuvuši publiski zināmi, var radīt ne tikai finansiālas un juridiskas sekas, bet negatīvi ietekmēt arī organizācijas / uzņēmuma reputāciju.

Jau 1992.gadā pieņemtajās ANO Ekonomiskās sadarbības attīstības organizācijas *Informāciju sistēmu drošības vadlīnijās*[19] norādīts: «Drošības kļūmes var radīt tiešus un pakārtotus zaudējumus. Tiešie zaudējumi ir tādi, kas radušies aparatūrai (procesoriem, darba stacijām, drukas iekārtām, diskiem, sakaru iekārtām), programmatūrai (sistēmas un lietotājprogrammām), dokumentācijai (specifikācijām, rokasgrāmatām un darbības procedūrām), personālam (operatoriem, lietotājiem un vadības, tehniskajiem un palīgdarbiniekiem), kā arī fiziskajai videi (datoru telpām, gaisa kondicionēšanas un enerģijas padeves iekārtām) u.c. Kaut gan tiešie zaudējumi var veidot daļu no kopējiem zaudējumiem dēļ drošības nosacījumu neievērošanas, tomēr nepieciešamais ieguldījums sistēmas izveidošanā un darbībā parasti ir ļoti liels.

Pakārtotie jeb netiešie zaudējumi var rasties, ja IS nedarbojas tā, kā paredzēts. Netiešie zaudējumi, kas radušies no drošības kļūmēm, var būt šādi: preču, naudas līdzekļu vai intelektuālā īpašuma zudumi; vērtīgas informācijas zudums; konkurences spējas zaudējums; naudas plūsmas pasliktināšanās; pasūtījumu vai visas uzņēmējdarbības zaudējums; ražošanas efektivitātes, darba ražīguma un drošības zaudējums; klientu vai piegādātāju labvēlības zaudēšana; sodi likumu noteikto pienākumu nepildīšanas dēļ; sabiedrības nesapratne un uzticības zaudēšana. Netiešie zaudējumi veido lielāko daļu no zaudējumiem, ko izraisa drošības kļūmes.»

Apvienotās Karalistes Tirdzniecības un rūpniecības departamenta atbalstītajā *Informācijas drošības pārkāpumu pētījumā 2004*, kuru veica auditorfirma *PricewaterhouseCoopers,* konstatēts, ka lielākā daļa uzņēmumu Apvienatajā Karalistē IS drošībai iegulda tikai līdz 3%, bet lielākie uzņēmumi – līdz 4% no budžeta. Tomēr ieteicamais līmenis ieguldījumiem IS drošībai ir vismaz 5% līdz 10% no budžeta. Viens no iemesliem šādai situācijai ir tas, ka drošība joprojām tiek uzskatīta nevis par investīcijām uzņēmējdarbībā, bet gan par izdevumiem. Arī uzņēmumu

[17] http://cert.nic.lv/
[18] http://www.first.org/
[19] OECD Guidelines for the Security of Information systems.

augstākajai vadībai, pat ja tā sniegusi formālus paziņojumus par informācijas drošību kā prioritāti, tomēr ir tendence uzskatīt ieguldījumus šajā jomā par uzspiestiem izdevumiem, nevis veidu, kā nodrošināt uzņēmējdarbības labus rezultātus.

Var pieminēt arī firmas *Ernst&Young* 2001.gadā veikto ASV 500 lielāko uzņēmumu aptauju, kurā noskaidrots, ka vislielāko uzmanību IS aizsardzībai pievērš, pirmkārt, telekomunikāciju firmas, otrkārt, uzņēmumi, kas darbojas finanšu jomā, treškārt, plašsaziņas līdzekļu uzņēmumi. Vismazāk uzmanību šiem jautājumiem pievērš uzņēmumi, kas darbojas enerģētikas jomā. Vislabāk tiek aizsargātas datu bāzes, vissliktāk – elektroniskā pasta sistēmas. Saskaņā ar šajā pētījumā konstatēto, biznesa struktūras, kļūstot par upuri krāpšanai, parasti zaudē vairāk naudu, nekā privātpersonas.

Pēdējā laikā aizvien vairāk izplatās arī tādi apdraudējumu veidi, kā, piemēram, izspiešana, uzņēmumiem pieprasot naudu, lai tiktu pārtraukta IS darbības traucēšana (*DoS* un *DDoS – Distributed Denial of Service*). Turklāt dažādu kaitējumu veikšanu var pat pieteikt biznesa konkurenti – internetā atrodami arī *hakeru* piedāvājumi veikt uzbrukumu IS par atlīdzību, arī piedāvājumi iegādāties kaitīgas programmas (par cenu pat sākot no 12 ASV dolāriem) un *botnetus* jeb botu tīklus (datoru kopums, kas inficēti ar vienoti no attāluma vadāmu programmatūru, lai ar tiem sūtītu mēstules, veiktu plašu intensīvu uzbrukumu citiem serveriem utt.). internetā var viegli atrast arī pamācības, kā izdarīt uzbrukumus IS, un dažādi jau sagatavoti programmlīdzekļi noteiktām programmu ievainojamībām (*exploits*), kas daudziem pat nepieredzējušiem vandāļiem (*script kiddies*) var radīt iluzoru priekšstatu, ka viņi viegli varētu kļūt par *hakeriem*, ar to pašapliecinoties līdzīgi domājošu cilvēku acīs.

Dažkārt uzņēmumi cieš ievērojamus zaudējumus arī profesionāli veiktas rūpnieciskās spiegošanas dēļ, kas var būt īstenota arī ar IS resursu starpniecību. Bez tam, profesionāli, pat ar valsts atbalstu var būt veikta arī kaitniecība vai spiegošana pret valsts IS.

Piemēram, atšķirībā no vairuma kaitīgu programmu, kas ik dienas parādās internetā un ir vērstas uz plašu datoru spektru ar mērķi no tā gūt finanšu labumu (vairāk kā 60% ir banku trojāņi), 2009.gadā radīta kaitīga programma *Win32/Stuxnet* (tā pirmoreiz publiski tika atpazīta 2010.gada jūnijā Baltkrievijā), kuras uzbukumu mērķis ir specifiskas rūpnieciskās sistēmas, kas drošības apsvērumu dēļ parasti pat nav pieslēgtas internetam, proti – Vācijas koncerna Siemens izstrādāto SCADA klases *WinCC* un *PCS7* rūpniecisku informācijas sistēmu ļaunprātīga ietekmēšana, lai iegūtu datus un centralizētu vadību pār šīm sistēmām. Tās parasti lieto naftas cauruļvadu, elektrostaciju, lielu sakaru sistēmu, lidostu, kuģu un pat militāru objektu ražošanas, infrastruktūras un apkalpošanas procesu uzraudzībai un vadībai.
Pētnieki atklāja, ka šī pašreproducējošā, *Windows* operatētājsistēmās ar USB atmiņas ierīcēm pārnēsājamā programma *Stuxnet* inficējusi daudzas Siemens izstrādātās sistēmas Indijā, Indonēzijā un Pakistānā, taču visvairāk inficēšanās notikusi Irānā. Daudzi uzskata, ka šo kaitīgo programmu izstrādājusi augsti kvalificētu speciālistu komanda, izmantojot ievērojamu finanšu ieguldījumu, un ar Izraēlas izlūkdienesta atbalstu, jo ir konstatētas pazīmes, ka šīs programmas izstrādātājiem bija pieejama izlūkošanas informācija par Irānas Bušēras atomelektrostacijas vadības sistēmu. Konstatēts, ka šī programma izstrādāta, lai īpaši meklētu noteiktus frekvences pārveidotājus, turklāt ar noteiktu darba frekvenci, lai, to specifiski izmainot, traucētu saistīto motoru ātrumu, radot neregulāras un grūti nosakāmas problēmas attiecīgajā sistēmā. Pētnieki uzskata, ka *Stuxnet* radīts tieši ar mērķi bojāt Irānas atomiekārtu vadības sistēmas. Bet tas jau parāda kiberkara specifiku, kur kaitīgas programmas galvenais uzdevums ir nevis peļņas gūšana vai pat inficēto sistēmu izspiegošana, bet tieši kaitniecība. Irānas amatpersonas vēlāk arī atzina, ka tika inficēta Bušēras AES informācijas sistēmu.
Saistībā ar šo gadījumu Siemens vēlāk uzsvēra, ka Microsoft programmu nodrošinājums „nevar tikt izmantots kritiski svarīgu ražošanas procesu vadīšanā". Antivīrusu firma Kaspersky Labs arī norādīja, ka cilvēki var izvairīties no

apdraudējuma, vienkārši nelietojot Microsoft programmatūru.[20]

Cita kaitīga programma *Agent.btz* (tārpa *SillyFDC* variants), kas 2008.gadā plaši visā pasaulē izplatījās datoros ar *Windows* operatētājsistēmu, kurās iekļuva ar USB atmiņas ierīcēm, izmantojot *Windows* operatētājsistēmas *Autorun.inf* funkcionalitāti, tāpat bija ar virkni pazīmēm, ka to mērķtiecīgi izstrādājusi augsti profesionāla speciālistu komanda ar kādas valsts atbalstu. Taču tās mērķis bija tieši spiegošana.
ASV Aizsardzības departamenta Pentagona iekšējā tīklā pēc tās konstatēšanas[21] pat tika liegts darbiniekiem lietot USB atmiņas ierīces. Kā paziņoja Pentagona pārstāvis, šī kaitīgā programma iekšējā datortīklā, kur apstrādā klasificētu informāciju, nonāca no portatīvā datora, kurā sākotnēji tā bija iekļuvusi no USB atmiņas kartes kādā ASV militārajā bāzē Tuvo austrumu valstī. Pentagona pārstāvis arī norādīja, ka šo kaitīgo programmu mērķtiecīgi izplatījis kādas valsts izlūkdienests.
ASV laikraksts "Los Angeles Times" publiskoja paziņojumu, ka tas bijis Krievijas izlūkdienests.[22]

Dažādi apdraudējumu veidi kibervidē un elektroniskas saziņas sistēmās aizvien turpina attīstīties, līdz ar ko aplūkotā joma visā pasaulē mūsdienās kļuvusi ļoti aktuāla. Te var pieminēt, ka kopš 1988.gada pat iedibināta IS drošības diena – katru gadu 30.novembrī.

[20] http://en.wikipedia.org/wiki/Stuxnet
[21] http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html
[22] http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28

Informācijas sistēmu drošības juridiskie aspekti

Globālā mērogā nepastāv vienoti juridiskie standarti, kas būtu kopīgi visām vai, vismaz, vairumam valstu, attiecībā uz drošību kibertelpā. Tam iemesls ir gan ātrums un daudzveidība, kā attīstās kibertelpa un tās izmantošanas jomas, gan arī dažādu valstu atšķirīgās intereses (kā jau iepriekš norādīts, ir pat militāra kibertelpas izmantošana). Starptautiski ir vien dažādi līgumi, tiesību politikas dokumenti un rekomendācijas.

Arī nacionālā mērogā nav faktiski iespējams kibertelpu vai vismaz tās drošības aspektus strikti regulēt ar tiesību aktiem. Tāpēc normatīvā reglamentācija var būt efektīvi izstrādāta vienīgi attiecībā uz noteiktu juridisko personu īpašumā vai valdījumā esošo informācijas sistēmu drošību.

Valsts un pašvaldību institūcijām informācijas sistēmu drošības noteikumu (ISDN) izstrādi noteic normatīvie akti – *Valsts informācijas sistēmu likuma*[23] 4.pants noteic nepieciešamību reglamentēt drošības prasības valsts informācijas sistēmām, šajā nolūkā izstrādājot atbilstīgus Ministru kabineta noteikumus.

Sākotnēji var norādīt, ka ar *Valsts informācijas sistēmu likuma* pārejas noteikumu nosacījumiem no 2002.gada 1.novembra spēku zaudēja Ministru kabineta noteikumi Nr. 106 *Informācijas sistēmu drošības noteikumi*.[24] Šie noteikumi bija pieņemti saskaņā ar *Krimināllikuma* pārejas noteikumu 3.panta 1.apakšpunktu tādēļ, lai nodrošinātu *Krimināllikuma* 245.panta piemērošanu. Saskaņā ar minētajiem noteikumiem, kriminālatbildību par *Krimināllikuma* 245.panta pārkāpumu var piemērot, ja MK Noteikumiem Nr. 106 atbilstīgas IS organizācijas amatpersona, kas ir atbildīga par IS drošības noteikumu ieviešanu un nodrošināšanu, tīši vai netīši pieļāvusi tādu IS drošības noteikumu pārkāpumu (vai vispār nav ieviesusi atbilstīgus IS drošības noteikumus), kas bijis iemesls, ka šim uzņēmumam vai organizācijai nodarīts būtisks kaitējums.

Te gan jāpiebilst, ka šie noteikumi tā arī netika praktiski ieviesti. Iemeslus, kāpēc Latvijā tas nav noticis, raksturojis Uldis Ķinis.[25]

Minētais *Valsts informācijas sistēmu likums* attiecas uz tām informācijas sistēmām, kuras lietojot, tiek nodrošināta informācijas aprite normatīvajos aktos un Latvijai saistošos starptautiskajos līgumos noteikto funkciju izpildei, tajā skaitā arī uz IS, ko pašvaldību institūcijas veido un uztur kā valsts informācijas sistēmas sastāvdaļu.

Saskaņā ar *Valsts informācijas sistēmu likuma* 4.panta (2) daļas normu nepieciešamie Ministru kabineta noteikumi Nr. 765. *Valsts informācijas sistēmu vispārējās drošības prasības*[26]

[23] Valsts informācijas sistēmu likums. / Ar grozījumiem uz 2011.gada 1.janvāri. Latvijas Vēstnesis Nr. 76, 2002.gada 22.maijā.

[24] Informācijas sistēmu drošības noteikumi. / Ministru kabineta noteikumi Nr.106. Zaudēja spēku 2002.gada 1.novembrī. Latvijas Vēstnesis Nr. 109/110, 2000.gada 24.martā.

[25] Sk. Informācijas un komunikāciju tiesības. / Autoru kolektīvs, U. Ķiņa juridiskajā redakcijā. – Rīga: Biznesa augstskola Turība, 2002. – II sēj.:309. – 315. lpp.

[26] Valsts informācijas sistēmu vispārējās drošības prasības. / Ministru kabineta noteikumi Nr.765. Ar grozījumiem uz 2011.gada 4.februāri. Latvijas Vēstnesis Nr.164, 2005.gada 14.oktobrī.

pieņemti 2005.gada 11.oktobrī un stājās spēkā 2005.gada 15.oktobrī. Vienlaikus ar tiem pieņemti arī Ministru kabineta noteikumi Nr. 764 *Valsts informācijas sistēmu vispārējās tehniskās prasības*.[27]

Valsts informācijas sistēmu likuma normas neattiecas uz tām IS, ko veido un uztur saskaņā ar likumu *Par valsts noslēpumu*[28] – par valsts noslēpuma objektu atzītas informācijas apritei, informācijas apritei saskaņā ar *Operatīvās darbības likumu*,[29] kā arī šis likums neattiecas uz IS, ko valsts un pašvaldību institūcijas veido un uztur iekšējās lietošanas informācijas apritei.

Saskaņā ar likumu *Par valsts noslēpumu* izdoti Ministru kabineta noteikumi Nr. 21 *Valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu institūciju klasificētās informācijas aizsardzības noteikumi*,[30] kas nosaka prasības IS drošībai, ja tajās tiek apstrādāta, uzglabāta un pārraidīta klasificēta informācija. Tādas IS var būt ne vien valsts un pašvaldību institūcijām, bet arī komersantiem (komercsabiedrībām), kas, pildot valsts vai pašvaldības pasūtījumu, kļūst par valsts noslēpuma, NATO vai Eiropas Savienības klasificētās informācijas subjektiem.

2005.gadā tika pieņemti arī MK noteikumi Nr. 280 *Kārtība, kādā aizsargājama informācija dienesta vajadzībām,*[31] ar ko nosaka informācijas dienesta vajadzībām aizsardzības kārtību valsts pārvaldes un pašvaldību institūcijās, kā arī komercsabiedrībās, kas, pildot valsts vai pašvaldības pasūtījumu, kļūst par informācijas dienesta vajadzībām subjektiem.

Bez tam jānorāda, ka IS drošības noteikumu izstrādi paredz arī *Fizisko personu datu aizsardzības likums*.[32] Šā likuma 21. - 22. pants noteic, ka visas valsts un pašvaldību institūcijas, citas fiziskās un juridiskās personas, kas veic vai vēlas uzsākt personas datu apstrādi un veido personas datu apstrādes sistēmas, reģistrē tās šā likuma noteiktajā kārtībā (izņēmumi ir attiecībā uz tādām IS, kurās informācijas reģistrēšanu veic sabiedriskās drošības, noziedzības apkarošanas vai valsts drošības un aizsardzības jomās). Vienlaikus ar reģistrācijas pieteikumu attiecīgas IS īpašnieks (valdītājs) iesniedz Datu valsts inspekcijai arī informāciju par tehniskiem un organizatoriskiem pasākumiem, kas nodrošina personas datu aizsardzību.

Tā kā fizisko personu datu apstrādi var veikt arī uzņēmumi (tajā skaitā arī reģistrējot sensitīvus savu darbinieku personas datus), tas nozīmē, ka konkrētas IS lietošanas specifikai atbilstīgu ISDN izstrāde var būt nepieciešama arī daudzos uzņēmumos.

---

[27] Valsts informācijas sistēmu vispārējās tehniskās prasības. / Ministru kabineta noteikumi Nr.764. Ar grozījumiem uz 2009.gada 3.jūniju. Latvijas Vēstnesis Nr.164, 2005.gada 14.oktobrī.

[28] Likums "Par valsts noslēpumu". / Ar grozījumiem uz 2010.gada 13.janvāri. Latvijas Vēstnesis Nr.181, 1996.gada 29.jūnijā.

[29] Operatīvās darbības likums. / Ar grozījumiem uz 2010.gada 1.janvāri. Latvijas Vēstnesis Nr.131, 1993.gada 30.decembrī.

[30] Valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu institūciju klasificētās informācijas aizsardzības noteikumi. / Ministru kabineta noteikumi Nr.21. Ar grozījumiem uz 2008.gada 1.oktobri. Latvijas Vēstnesis Nr.17, 2004.gada 3.februārī.

[31] Kārtība, kādā aizsargājama informācija dienesta vajadzībām. / Ministru kabineta noteikumi Nr.280. Ar grozījumiem uz 2005.gada 5.novembri. Latvijas Vēstnesis Nr.68, 2005.gada 29.aprīlī.

[32] Fizisko personu datu aizsardzības likums. / Ar grozījumiem uz 2010.gada 2.jūniju. Latvijas Vēstnesis Nr.123/124, 2000.gada 6.aprīlī.

Fizisko personu datu aizsardzības likuma 26.pants noteic, ka personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības nosaka Ministru kabinets, kas ir Ministru kabineta noteikumi Nr. 40 *Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības*.[33]

Jāpiemin arī Finanšu un kapitāla tirgus komisijas izdotie noteikumi Latvijas kredītiestādēm *Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi*.[34]

Bez tam saistībā ar šo jomu ir MK noteikumi Nr. 1131 *Valsts informācijas sistēmu savietotāju izveidošanas, uzturēšanas un darbības kārtība un valsts informācijas sistēmas funkcionalitātes nodrošināšanas kārtība integrētas valsts informācijas sistēmas ietvaros*[35] un MK noteikumi Nr. 1445 *Kritisku valsts informācijas sistēmu un valsts informācijas sistēmu savietotāju aizsardzības prasības*,[36] kas attiecas uz kritisko valsts IS pārziņiem un institūcijām, kuras nodrošina valsts IS savietotāju darbību. Tajos noteiktas prasības elektroenerģijas piegādei un nodrošinājumam, sistēmas datu apmaiņas nodrošināšanas prasības, sistēmas fiziskās aizsardzības prasības, sistēmas loģiskās aizsardzības prasības, prasības sistēmas monitoringam, prasības sistēmas infrastruktūras apkalpošanai, prasības personām, kuras apkalpo sistēmu.

Savukārt MK instrukcijā Nr. 20 *Valsts pārvaldes funkciju izpildi apdraudošu kiberuzbrukumu noteikšana*[37] tika noteikts kiberuzbrukuma jēdziens,[38] noteikta institūcija, kurai ir koordinējošā loma kiberuzbrukuma ierobežošanā un seku likvidēšanā – DDIRV, uzskaitītas pazīmes, pēc kurām valsts IS pārziņiem atpazīt kiberuzbrukumu, noteikts pazīmju kopums, pēc kurām nosaka valsts pārvaldi apdraudošu kiberuzbrukumu, un valsts institūciju, kas nosaka šo apdraudējumu, noteikts darbības algoritms valsts pārvaldei jebkura pamanīta kiberuzbrukuma gadījumā.

2010.gadā plānots izdot arī *Valsts informācijas sistēmas drošības pārvaldnieka apmācību un zināšanu pārbaudes kārtība, kā arī sertifikāta izsniegšanas, atjaunošanas, darbības izbeigšanas un anulēšanas kārtība*, pielikumā pievienojot arī apmācības programmu.

Lai pilnveidotu tiesisko reglamentāciju šajā jomā, 2010.gadā izveidotā starpresoru darba

---

[33] Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības. / Ministru kabineta Noteikumi Nr.40. Ar grozījumiem uz 2007.gada 1.septembri. Latvijas Vēstnesis Nr.19, 2001.gada 2.februārī.

[34] Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi. / Finanšu un kapitāla tirgus komisijas normatīvie noteikumi Nr.278. Latvijas Vēstnesis Nr.162, 2010.gada 13.oktobrī.

[35] Valsts informācijas sistēmu savietotāju izveidošanas, uzturēšanas un darbības kārtība un valsts informācijas sistēmas funkcionalitātes nodrošināšanas kārtība integrētas valsts informācijas sistēmas ietvaros. / Ministru kabineta noteikumi Nr.1131. Latvijas Vēstnesis Nr.161, 2009.gada 9.oktobrī.

[36] Kritisku valsts informācijas sistēmu un valsts informācijas sistēmu savietotāju aizsardzības prasības. / Ministru kabineta noteikumi Nr.1445. Latvijas Vēstnesis Nr.200, 2009.gada 21.decembrī.

[37] Valsts pārvaldes funkciju izpildi apdraudošu kiberuzbrukumu noteikšanas instrukcija. / Ministru kabineta instrukcija Nr.20. Zaudēja spēku ar 2011.gada 4.februāri. Latvijas Vēstnesis Nr.203, 2009.gada 28.decembrī.

[38] Kiberuzbrukums šo noteikumu izpratnē ir: (2.1.) 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; (2.2.) automatizētā datu apstrādes sistēmā esošās informācijas patvaļīga grozīšana, bojāšana, iznīcināšana, pasliktināšana vai aizklāšana (pieejamības ierobežošana) vai apzināti nepatiesas informācijas ievadīšana automatizētā datu apstrādes sistēmā; (2.3.) apzināta ierīces (arī datorprogrammas) izmantošana, kura paredzēta patvaļīgai automatizētas datu apstrādes sistēmas resursu ietekmēšanai.

grupa – Elektronisko sakaru un informācijas tehnoloģiju nozares konsultatīvā padome drošības jautājumos, sadarbībā ar Satiksmes ministriju, izstrādāja ***Informācijas tehnoloģiju drošības likumu***,[39] kuru Saeima pieņēma 2010.gada 28.oktobrī.

Šis likums izstrādāts, lai sekmētu 2010.gada augusta beigās pieņemtajā *Nacionālās drošības koncepcijā* paredzētās Latvijas prioritātes IT drošības apdraudējuma novēršanā. Tā mērķis ir uzlabot IT drošību, nosakot svarīgākās prasības, lai garantētu tādu būtisku pakalpojumu saņemšanu, kuru sniegšanai tiek izmantotas informācijas tehnoloģijas.[40] IT drošība ir sargājama tā, lai varētu savlaicīgi prognozēt un novērst, kā arī pārvarēt šīs drošības apdraudējumu un likvidēt tā sekas. Šis likums tiek attiecināts uz valsts un pašvaldību institūcijām, kā arī uz komersantiem un citām privāto tiesību juridiskajām personām. Ar šo likumu definē *Informācijas tehnoloģiju kritisko infrastruktūru* (to apstiprina Ministru kabinets) un tās aizsardzības pamatprincipus, lai nodrošinātu valstij un sabiedrībai būtisku pamatfunkciju veikšana, nodrošinot šī infrastruktūras integritāti, pieejamību un konfidencialitāti. Šis likums reglamentē arī *IT drošības incidentu novēršanas institūciju* un tās funkcijas (kas arī ir plašākā daļa šajā likumprojektā), tāpat arī *IT drošības incidentu* un nepieciešamo rīcību tā gadījumā, kā arī par IT drošības pārvaldību atbildīgās amatpersonas valsts un pašvaldību institūcijās un valsts un pašvaldību institūciju *Informācijas tehnoloģiju drošības noteikumus*. Šis likums relgamentē atsevišķus aspektus arī elektronisko sakaru komersantu pienākumos attiecībā uz publisko elektronisko sakaru tīklu drošību. Tas paredz arī izveidot *Nacionālo informācijas tehnoloģiju drošības padomi*.

Saskaņā ar šo 'jumta likumu' jāveic arī vairāku citu normatīvo aktu izstrāde un grozīšana, līdz ar ko tā praktiska ieviešana būs sarežģīts process. Piemēram, paredzēts no *Valsts informācijas sistēmu likuma* un tam pakārtotiem MK noteikumiem pilnībā izslēgt reglamentāciju par kritiskām valsts informācijas sistēmām.

Likuma pieņemšanā tika atbalstīts Satversmes aizsardzības biroja priekšlikums par atbildīgo institūciju šajā jomā noteikt Latvijas Universitātes Matemātikas un informātikas institūtu, izveidojot *Informācijas tehnoloģiju drošības incidentu novēršanas institūtu* (ITDINI), kurā faktiski apvienotu iepriekšējo DDIRV un CERT.NIC.LV funkcijas. Vairākos aspektos ITDINI mijiedarbosies ar valsts drošības iestādēm, kuras saskaņā ar *Nacionālās drošības likuma* reglamentāciju veic virkni funkciju attiecībā uz kritisko infrastruktūru (tās daļa ir arī informācijas tehnoloģiju kritiskā infrastruktūra). Tāpēc paredzēts, ka ITDINI amatpersonām nepieciešama pielaide valsts noslēpumu saturošai informācijai.

Informācijas sistēmu drošības metodiskie aspekti

[39] Informācijas tehnoloģiju drošības likums. / Latvijas Vēstnesis Nr.178, 2010.gada 10.novembrī.

[40] Informācijas tehnoloģijas šā likuma izpratnē ir tehnoloģijas, kuras tām paredzēto uzdevumu izpildei veic informācijas elektronisko apstrādi, tai skaitā izveidošanu, dzēšanu, glabāšanu, attēlošanu vai pārsūtīšanu.

Iespējamie apdraudējumi IS drošībai ir viens no pamatfaktoriem, kas jāievēro ne vien tādu IS izveidē un uzturēšanā, kurās tiek apstrādāta valsts interesēm svarīga un ar likumiem, starptautiskajiem līgumiem un citiem normatīvajiem aktiem aizsargāta informācija, bet arī tādu IS izveidē un uzturēšanā, kur tiek apstrādāta uzņēmumu sekmīgai darbībai nozīmīga informācija. Kaut arī pilnīga IS drošība praktiski nav iespējama, tomēr maksimāli daudz pūles jāveltī aizsardzībai pret IS apdraudējumiem jebkādu informācijas tehnoloģiju projektu īstenošanā gan valsts pārvaldes jomā, gan arī uzņēmējdarbībā. Un arī lielai daļai privātpersonu ir svarīga viņu īpašumā vai valdījumā esošo datorsistēmu un tajā apstrādātās, uzglabātās un pārraidītās informācijas drošība.

Sākotnēji gan jānorāda, ka šeit metodiskie un atsevišķi ar tiem saistītie organizatoriskie un tehniskie aspekti aplūkoti vien pamataspektu līmenī, kas piemērots personām, kuras nav specializējušās IT drošības jautājumos, taču vēlas gūt vispārīgu priekšstatu par šās jomas pamatjautājumiem.

ANO Ekonomiskās sadarbības attīstības organizācijas *Informāciju sistēmu drošības vadlīnijās*[41] minēts: «Jāatceras, ka attiecībā uz individuālām situācijām nevar būt viens vienīgs drošības risinājums. Vajadzības pēc drošības ir būtiski atšķirīgas dažādos sektoros, dažādās firmās, dažādās struktūrvienībās un pat vienai un tai pašai IS tās lietošanas laika gaitā. Informētas un izsvērtas lietotāja vajadzību izpratnes trūkums var izraisīt lielu bezmērķīgas tehnoloģiskās standartizācijas risku. Pirmais produktīvais solis ir atzīt to dažādību un neviendabīgumu, kas piemīt lietotāju vajadzībām pēc informācijas sistēmu aizsargierīcēm.»

Būtībā ***Informācijas sistēmas drošības noteikumi*** (ISDN) ir organizācijas / uzņēmuma vadības[42] dokumentētie lēmumi par informācijas sistēmu drošību, kas izstrādāti atbilstīgi noteiktiem principiem un faktiskajiem IS uzbūves un lietošanas apstākļiem un mērķiem. Tātad, pirmām kārtām, tā ir vadības attieksme pret IS drošību – vai vadību interesē, kā ir izveidota uzņēmuma IS drošības sistēma, cik daudz katrs darbinieks zina par šādas sistēmas esamību, saviem pienākumiem un atbildību. Arī par to, kas ir atļauts un kas nav un kā uzņēmumā ir pareizi sadalīta atbildība.

IS drošības politikas izstrādes iniciatīvu uzņēmumā lietderīgi saistīt ar pārvaldes formu – ja tam ir vertikāla pārvaldes struktūra, kur zemāka ranga darbinieku amata pienākumi paredz veikt vien nemainīgas ikdienas funkcijas, tad vadītājam pašam galvenokārt jāzņemas atbildība par IS drošības sistēmas pilnveidošanas kontroli, jo zemāka ranga darbinieki var nebūt īpaši motivēti pēc savas iniciatīvas rūpēties par uzņēmuma drošības pastāvīgu pilnveidošanu. Savukārt, ja uzņēmuma

[41] OECD Guidelines for the Security of Information systems. Explanatory Memorandum to Accompany the Guidelines for the Security of Information Systems. / Accepted 26 November, 1992.; Latest update 1 July, 1997. Replaced by the 2002 OECD Guidelines. - http://www.oecd.Org/dsti/sti/it/secur/prod/e_secur.htm

[42] Ievērojot, ka valsts informācijas sistēmu aizsardzības nosacījumi un kārtība ir reglamentēta ar normatīvajiem aktiem, šeit autors velta uzmanību galvenokārt tikai uzņēmumu IS aizsardzības aspektiem. Tāpēc arī turpmāk izklāstā lielākoties runāts vien par uzņēmumu IS drošību. Protams, šeit aplūkotie aspekti var būt apsvērti arī valsts vai nevalstisko organizāciju IS aizsardzības organizēšanā.

vadītājs nevēlas vai zināšanu trūkuma dēļ nespēj pats pilnvērtīgi uzņemties atbildību par šo jomu, tad uzņēmumā, vismaz šajā aspektā, var būt lietderīga horizontāla pārvaldes struktūra, kur liela daļa atbildības un iniciatīvas brīvība deleģēta vidēja ranga struktūrvienību (tajā skaitā arī Informācijas sistēmu daļas) vadītājiem, un viņi tiek motivēti censties pastāvīgi pilnveidot viņu struktūrvienības darbību – gan ar elastīgu darba apmaksas sistēmu, kas ir atbilstīga viņu ieguldījumam un pozitīvai iniciatīvai, gan ar citiem motivēšanas paņēmieniem, kas vērsti uz iespēju viņiem paaugstināt savu kompetenci un to pilnvērtīgi arī īstenot (atbilstīgi t.s. *ārējai* un *iekšējai* motivācijas sistēmai).

Te gan jāuzsver, ka jebkurā gadījumā atbildību par IS drošību, ja tas saistīts ar likumos noteikto fizisko un juridisko personu tiesību un interešu aizsardzību, pamatā gulstas uz organizācijas / uzņēmuma vadītāju.

Informācijas sistēmas drošības nodrošināšanas viena no metodiskajām pamatīpatnībām ir **kontroles un funkcionalitātes līdzsvars**, gan tehniski, gan ar organizatoriskiem pasākumiem. Vienlaikus nepieciešams rūpēties gan par visu informācijas sistēmā veikto darbību un notikumu kontroli, gan par IS funkcionalitāti un lietošanas ērtumu; nav vēlamas galējības nedz vienā, nedz otrā virzienā. Līdzsvaru gan nevajag interpretēt kā ieganstu būt paviršam kontroles vai funkcionalitātes nodrošināšanas aspektā. Te var minēt Satiksmes ministrijas ieteikumu *Metodiskie norādījumi par informācijas ievietošanu internetā*[43] 25. punkta nosacījumu: «Mājas lapa ir pieejama, arī izmantojot maksimālos drošības uzstādījumus». Šāda pieeja attiecas gan uz uzņēmuma vadītāju un drošības dienesta vadītāja mijiedarbību ar datorspeciālistiem, gan arī uz pašas IS veidošanu un uzturēšanu.

IS drošības politikas atsevišķi organizatoriskie risinājumi papildus aplūkoti turpmāk. Šeit vēl lietderīgi norādīt uz metodisko pamatu ISDN veidošanā – vispārpieņemtiem IS drošības **standartiem**.

Latvijas standarts (LVS) nodrošinājis Eiropas Standartizācijas komitejas[44] informācijas tehnoloģiju standartu pieejamību LVS informācijas fondā. LVS standartizācijas tehniskā komiteja – Informācijas tehnoloģijas – Latvijas standarta statusā adaptējusi šajā jomā arī būtiskos starptautiskos standartus,[45] tajā skaitā ISO/IEC 17799 *Informācijas tehnoloģija: Prakses kodekss informācijas drošības pārvaldībai*, patlaban jau atceltais ISO/IEC 15408 *Informācijas tehnoloģija. Drošības metodes. Kritēriji informācijas tehnoloģiju drošības novērtēšanai: Ievads un vispārējais modelis; Drošības funkcionālās prasības; Drošības garantēšanas prasības*; ISO/IEC TR 13335 *Informācijas tehnoloģija. Vadlīnijas informācijas tehnoloģijas pārvaldīšanai: Informācijas tehnoloģiju drošības koncepcija un modeļi; Informācijas tehnoloģiju drošības pārvaldīšana un plānošana; Aizsardzības līdzekļu izvēle; Tīklu drošības pārvaldīšanas ieteikumi*, kuri pašlaik

[43] Metodiskie norādījumi par informācijas ievietošanu internetā. / Satiksmes ministrijas ieteikumi Nr. 01-21/2. Latvijas Vēstnesis Nr.85, 2002.gada 6.jūnijā.

[44] http://www.cen.eu/cen/pages/default.aspx

[45] http://www.iso.org/iso/home.htm ; http://en.wikipedia.org/wiki/ISO/IEC_27000-series

iekļauti ISO 27000 sērijā. IS drošības politikas īstenošanai lietderīgi izmantot arī *CobiT* (*Control Objectives for Information and related Technology*)[46] un citus standartus.

LVS ISO/IEC 27002 (agrākais ISO/IEC 17799) ietver kompleksus praktiskus nosacījumus informācijas drošības vadībai, tāpēc tas var būt pielietots arī kā novērtējuma kritērijs IS drošības risinājumam organizatoriskā līmenī, tajā skaitā administratīvajiem, procedūras un tehniskiem aspektiem. Tas ietver desmit novērtējuma jomas: 1) drošības politika; 2) drošības organizatoriskā struktūra; 3) informācijas resursu klasifikācija; 4) personāla ietekme uz IS drošību; 5) fiziskā drošība; 6) saziņa un darbību pārvaldība; 7) piekļuves kontrole; 8) sistēmas risinājums un uzturēšana; 9) darbības nepārtrauktības pārvaldība; 10) atbilstība normatīviem. Šis standarts neizvirza nosacījumus IS lietojamām tehnoloģijām, iekārtām un nesniedz informācijas tehnoloģiju pārvaldības konceptuālu struktūru, bet tas aplūko informāciju kā kopumu, kas var būt apstrādāta un uzglabāta visdažādākajos veidos. Tas, ka standarts nav atkarīgs no konkrētiem tehniskiem līdzekļiem un risinājumiem, no vienas puses, nedod skaidru priekšstatu, kā praktiski īstenot tā vai cita IS elementa aizsardzību, taču, no otras puses, dod brīvību izvēlēties IS tehniskos un informācijas resursus.

Pašlaik Latvijā gan atceltais ISO/IEC 15408, kas IT jomas speciālistu vidū plašāk pazīstams kā *Common Criteria for Information Technology Security Evaluation*,[47] pilnvērtīgi apraksta kritērijus drošības nodrošinājumam tehnisko un informācijas resursu, tajā skaitā programmatūras pielietojumā. Tas nodala vienpadsmit pamatklases IS drošības funkcijām: 1) audits; 2) identifikācija un autentifikācija; 3) kriptogrāfiskā aizsardzība; 4) konfidencialitāte; 5) datu pārraide; 6) lietotāju datu aizsardzība; 7) drošības pārvalde; 8) IS drošības funkciju aizsardzība; 9) resursu lietošana; 10) piekļuve sistēmai; 11) pielietoto līdzekļu drošums (*reliability*). Tās tiek iedalītas vēl sīkāk, līdz ar to ļaujot izveidot arī precīzus drošības novērtējuma profilus konkrētiem praktiskiem risinājumiem. Šis standarts ir piemērots IS drošības auditu veikšanai gan kā metodika, gan kā kritēriji, lai novērtētu IS nepilnības.

Informācijas drošības pārvaldība atbilstīgi starptautisko standartu prasībām nozīmē, ka organizācija, uzņēmums, kas to īsteno, izvirzījusi IS drošību kā vienu no prioritātēm. Tāpēc šo standartu ieviešana ļauj iegūt gan tā sadarbības partneru un klientu uzticību, gan daudz drošāk prognozējamu attīstību.

Tomēr jāpiebilst, ka standarti norāda risinājumu shēmu un ļauj novērtēt dažādu produktu atbilstības līmeni, taču neizskaidro, kā viens vai otrs jautājums risināms praktiski. Tāpēc konkrētu IS drošības risinājumu izstrādē jābalstītās uz vairākiem aspektiem vienlaikus: 1) šās jomas standartiem un pamatprincipiem, 2) speciālistu izstrādātām vadlīnijām un rekomendācijām, 3) spēkā esošām tiesību normām, kā arī 4) konkrētās IS tehniskajām un darbības īpatnībām, nodrošinot, lai

[46] http://www.isaca.org/cobit.htm
[47] http://www.niap-ccevs.org/cc-scheme/cc_docs/ ; http://www.commoncriteriaportal.org/

ISDN iekļautu vienotā organizācijas drošības sistēmā, šie noteikumi būtu atbilstīgi faktiskajiem apdraudējumiem un tiktu arī praktiski īstenoti.

Ievērojot IS apdraudējumu pārrobežu raksturu un to būtisko ietekmi uz uzņēmējdarbības un fizisko personu interešu aizsardzības, kā arī valsts pārvaldes jomu, ANO Ekonomiskās sadarbības un attīstības organizācijas (OECD)[48] Informācijas, datoru un sakaru politikas komitejas ekspertu grupa izstrādāja un 1992.gadā OECD pieņēma *Informācijas sistēmu drošības vadlīnijas*,[49] kuras akceptēja 24 OECD dalībvalstis, tajā skaitā arī Latvija (pēdējās korekcijas tajā veiktas 1997.gadā). Šo vadlīniju pamataspektu raksturojumu sniedzis Uldis Ķinis,[50] tāpēc ISDN izstrādei lietderīgi izskatīt arī viņa vērtējumu par to. Tomēr, ievērojot IT jomas straujo attīstību kopš 1992.gada, OECD pēc 1997.gada turpināja darbu pie IS drošības vadlīniju pilnveides, īpaši paātrinot to pēc 2001.gada 11.septembrī ASV notikušā terora akta. Šā darba rezultātā 2002.gadā OECD pieņēma dokumentu *Informācijas sistēmu un datortīklu drošības vadlīnijas: Drošības kultūras veidošana.*[51]

ISDN izstrādei lietderīgi iepazīties arī ar ārvalstīs šajā jomā vispārpieņemtiem pamatprincipiem. Piemēram var nosaukt autoritatīva IS drošības eksperta Čārlija Vuda grāmatu «Vieglais ceļš uz informācijas drošības politiku»,[52] kur izskaidroti principi, ko izmanto ISDN izstrādē, kā arī minēti daudzi piemēri. Šādu informāciju var atrast arī specializētās interneta mājaslapās.[53]

IS drošības metodisko aspektu raksturojumu var iesākt, īsi paskaidrojot pamatjēdzienus.

Informācijas sistēmu drošību OECD vadlīnijas, gluži tāpat, kā iepriekš minētais standarts ISO/IEC 17799, definē kā **informācijas pieejamības, konfidencialitātes un integritātes nodrošināšanu informācijas sistēmā**.

Šā mērķa sasniegšanai jāveic noteiktu *juridisko*, *organizatorisko* un *tehnisko* pasākumu komplekss, ko apzīmē kā **IS drošības politika**.

IS drošības politika jāiekļauj attiecīgā uzņēmuma kopējā drošības politikā. IS drošības politika nosaka pamatnostādnes IS drošības pārvaldības izveidei un uzturēšanai, tajā skaitā konceptuālu IS drošības pārvaldības principu, nosacījumu un pamatmērķu aprakstu. Citiem vārdiem, IS drošības politika satur prasības, kuras noteicis informācijas īpašnieks (turētājs), un apraksta pasākumus šo prasību nodrošināšanai. IS drošības politika jānostiprina ar uzņēmuma normatīvajiem dokumentiem.

IS drošības politikas galvenie organizatoriski tehniskie pasākumi ir **drošības auditi**, **drošības pārskati** un **drošības monitorings**. Šo pasākumu galarezultāti jāatspoguļo **IS drošības**

---

48 Organisation for Economic Co-operation and Development. - http://www.oecd.org/sti/cultureofsecurity_

49 OECD Guidelines for the Security of Information systems.

50 Informācijas un komunikāciju tiesības. / Autoru kolektīvs, U. Ķiņa juridiskajā redakcijā. - Rīga: Biznesa augstskola Turība, 2002. - 1 sēj.: 278. - 298. lpp.

51 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. / Adopted as a Recommendation of the OECD Council at its 1037 Session on 25 July, 2002.

52 Charles C. Wood. Information Security Policies Made Easy. A Comprehension Set of Information Security Policies. (Version 9). – Baseline Software, 2002. - 730 p.

53 Sk., piemēram: The SANS Institute - http://www.sans.org/resources/policies

novērtēšanas dokumentācijā.

Ar uzņēmuma IS drošības noteikumiem reglamentē IS informācijas un tehnisko resursu pārvaldi (administrēšanu), atbildīgo darbinieku un IS lietotāju tiesības, pienākumus un atbildību, informācijas klasifikāciju, informācijas un tehnisko resursu aizsardzības organizatoriski tehniskos pasākumus u.c.

Vienkāršoti definējot, informācijas **pieejamība** ir informācijas pastāvēšana un saglabāšana tā, lai pēc pieprasījuma noteiktā laikā pilnvaroti lietotāji tai varētu piekļūt; **integritāte** ir informācijas saglabāšana pilnībā un neizmainīta, nodrošinot arī to, ka pilnvaroti lietotāji var atbilstīgo informāciju izmainīt; **konfidencialitāte** ir informācijas apstrāde, uzglabāšana un pārraide, pārsūtīšana tā, lai šai informācijai var piekļūt tikai personas, kuras ir pilnvarotas to saņemt.

IS apdraudējums ir ar nodomu (tīši) vai aiz neuzmanības izdarīta darbība vai bezdarbība, vai iespējams notikums, kas var izraisīt nevēlamu informācijas sistēmā apstrādātas informācijas vai datu dzēšanu, izmainīšanu, nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, piekļuves zaudēšanu informācijai vai citas patvaļīgas izmaiņas informācijas resursos, vai arī tehnisko resursu nevēlamu nomaiņu, bojāšanu, patvaļīgu lietošanu vai citas nevēlamas darbības ar tehniskiem resursiem.

IS fiziskā aizsardzība ir tehnisko resursu aizsardzība pret fiziskas iedarbības radītu informācijas sistēmas apdraudējumu (piemēram, ugunsgrēks, applūšana, elektriskā sprieguma pazemināšanās vai pārspriegums elektroenerģijas pievades datortīklā, tehnisko resursu zādzība vai to tīša sabojāšana, ekspluatācijas noteikumiem neatbilstīgs mitrums, gaisa temperatūra, putekļi, dūmi telpā, vibrācija, ārējs spēcīgs elektromagnētiskais lauks u.c).

IS loģiskā aizsardzība ir informācijas resursu aizsardzība, ko īsteno ar programmatūras līdzekļiem (piemēram, identificējot informācijas sistēmas lietotāju, pārbaudot viņa pilnvaru atbilstību noteiktām darbībām informācijas sistēmā, pasargājot informāciju no tīšas vai nejaušas nevēlamas izmainīšanas, dzēšanas vai izpaušanas, novēršot patvaļīgu piekļūšanu informācijas resursiem, novēršot IS pārslogošanu, kas var izsaukt tās darbības pārtraukumus u.c).

Papildus var definēt **kriptogrāfisko aizsardzību** – informācijas loģiskās aizsardzības noteiktas metodes, kuras programmātiski nodrošina ar matemātisku pārveidojumu algoritmu informācijas integritāti un konfidencialitāti; kriptogrāfiskā aizsardzības var būt īstenota ar simetrisko vai asimetrisko šifrēšanu, tajā skaitā vienvirziena šifrēšanu ar kriprogrāfiskās kontrolsummas jeb *hash* funkciju, arī ar datorsteganogrāfijas metodi. Parole ir simbolu virkne, kura zināma lietotājam un kuras kopija atrodas informācijas sistēmā, un ar kuru autentificē lietotāju jeb pierāda tā identitāti saistībā ar noteiktām informācijas resursu piekļuves un apstrādes funkcijām.

Ugunsmūris *(firewall)* ir programmatūras un aparatūras komplekss, kas savieno lokālo datortīklu (Intranet) vai atsevišķu resursdatoru ar globālo datortīklu (Internet), informācijas sistēmas

aizsardzību pret apdraudējumiem no interneta, tajā skaitā no patvaļīgas piekļuves. Ugunsmūris var būt izveidots tikai ar programmatūras palīdzību uz lietotāja resursdatora vai lokālā datortīkla failu servera, taču lietderīgi tam lietot atsevišķu starpniekserveri jeb *proxy* serveri.

IS auditācijas pieraksti ir programmatūras automatizēti veidoti pieraksti, kuros reģistrēta informācija par notikumiem informācijas sistēmā – datums, pulksteņlaiks, notikuma identifikācijas pazīmes (gan saistībā ar IS lietotāju darbībām, gan saistībā ar noteiktiem IS informācijas un tehniskajiem resursiem, piemēram, piekļuvi noteiktiem failiem, gan saistībā ar programmatūras darbību), līdz ar to nodrošinot informāciju gan IS drošības apdraudējumu konstatēšanai, gan arī kā pierādījumus par notikumiem IS.

IS drošības audits ir periodiski vai nepieciešamības gadījumā ārpuskārtas kompleksi veikts pārbaudes pasākums uzņēmuma IS drošības sistēmas izvērtēšanā ar nolūku noteikt, vai IS ir izveidota, tiek uzturēta un lietota saskaņā ar ISDN, kā arī uzņēmuma kopējās drošības sistēmas nosacījumiem.

IS drošības auditu var veikt gan kā iekšējo, gan kā ārējo (neatkarīgo). Kvalificētu IS auditu var veikt profesionālu organizāciju, tādu kā Informācijas sistēmu audita un kontroles asociācijas ISACA biedri,[54] kuri ieguvuši CISM,[55] CISSP[56] vai citu atbilstīgu sertifikātu.[57]

Te var piebilst, ka atsevišķas firmas ar interneta starpniecību piedāvā attālinātu IS drošības auditu, tomēr nav lietderīgi paļauties tikai uz tādu, jo, kaut arī tas ir diezgan vienkārši īstenojams, tomēr ir nepilnīgs. Tāda audita gaitā dažkārt var noteikt līdz 90% no tādiem iespējamiem IS informācijas resursu apdraudējumiem, kādus var radīt ar interneta pieslēgumu un attiecīgās IS lietotāji, taču tas vispār neietver citāda veida apdraudējuma faktorus informācijas sistēmai.

IS informācijas resursu drošības auditam datortīklā var lietot specializētas programmas, kas startējas no CD diska vai USB atmiņas ierīces, piemēram, atvērtā koda bezmaksas programmatūras komplektus *Back-Track*,[58] *Auditor Security Linux*[59] u.c., kā arī dažādus komerciālus produktus.

Tomēr kvalitatīvas IS drošības auditam ne tikai jālieto speciāla programmatūra un jāanalizē IS veidotie auditācijas pieraksti *(.log* faili), bet arī ir lietderīgi veikt personāla intervijas, pārbaudīt dokumentus, veikt dažādu darbību un nosacījumu modelēšanu un pārbaudi telpās, kur izvietota IS. Intervijās iegūto informāciju vēlams pārbaudīt, iegūstot informāciju no citiem avotiem. Vienmēr jāatceras, ka galvenais apdraudējuma avots nereti ir nevis IS tehnisko un informācijas resursu darbības īpatnības, bet gan cilvēki – IS lietotāji un personāls, kuri var pieļaut paviršības, kļūdas vai pat ļaunprātību.

---

54 http://www.isaca.lv/gl/index.php?topic=Biedri
55 http://en.wikipedia.org/wiki/Certified_Information_Security_Manager
56 http://en.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional
57 http://en.wikipedia.org/wiki/Category:Information_technology_qualifications
http://en.wikipedia.org/wiki/Category:Computer_security_qualifications
58 http://www.backtrack-linux.org/
59 http://linux.softpedia.com/get/System/Operating-Systems/Linux-Distributions/Auditor-Security-Linux-2616.shtml

Svarīgi apzināties, ka drošības audits nenozīmē tikai IS informācijas resursu ārējo apdraudējumu tehnisko iespēju novērtēšanu. Tas cieši jāsaista ar uzņēmuma drošības politiku, uzņēmuma darbinieku un klientu kompetenci (strikti nodalot piekļuves tiesības vienīgi tādiem informācijas resursiem, kas ir nepieciešami pilnvaroto funkciju veikšanai), atbildību, viņu darbībām, tiesībām un pienākumiem, kā arī citiem faktoriem, tajā skaitā fizikālajiem faktoriem telpās, kur izvietoti IS tehniskie resursi. Piemēram, IS drošībai svarīgi arī, lai nebūtu pieļauta nepiederošu personu piekļuve tehniskiem resursiem, lai telpās būtu ierīkota signalizācija u.tml.

Veicot drošības auditu, lietderīgi risināt šādus pamatuzdevumus:

1. Noteikt iespējamos IS apdraudējumus, t.sk. arī tos, kurus var radīt pats IS pārzinis un lietotāji, un novērtēt to īstenošanās varbūtību;
2. Novērtēt iespējamo kaitējumu uzņēmumam vai personai, kura nodod informāciju IS, ja notiek kaut kādi drošības apdraudējumi;
3. Noteikt līdzekļus, kas lietojami IS apdraudējuma novēršanai;
4. Novērtēt, vai pēc veiktajiem IS drošības pasākumiem informācijas sistēmas apdraudējuma varbūtība un iespējamais kaitējums ir pieņemams IS drošībai;
5. Novērtēt veikto IS drošības pasākumu lietderību;
6. Izstrādāt informācijas resursu un tehnisko resursu atjaunošanas un IS darbības atjaunošanas plānu informācijas sistēmai – gadījumiem, ja nodarīts kaitējums.

Vēl jānorāda, ka prasību veikt IS auditu (tas ietver arī IS drošības auditu) noteic arī normatīvie akti – ja uzņēmumā ir fizisko personas datu apstrādes sistēma, tad tās audita nepieciešamību nosaka jau pieminētais *Fizisko personu datu aizsardzības likums* un Ministru kabineta noteikumi Nr. 40 *Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības*. Šo noteikumu 6.punkts paredz, ka IS pārzinis katru gadu veic fizisko personas datu apstrādes sistēmu iekšējo auditu un sagatavo pārskatu par informācijas drošības jomā veiktajiem pasākumiem. *Fizisko personu datu aizsardzības likuma* 26.panta (2) daļa noteic, ka katru gadu valsts un pašvaldību institūcijas iesniedz Datu valsts inspekcijai personas datu apstrādes sistēmu iekšējā audita atzinumu un pārskatu par informācijas drošības jomā veiktajiem pasākumiem (te gan jāpiebilst, ka daudzpusīgs IS drošības audits ietver vairāk uzdevumus, nekā tikai paredz minētie normatīvie akti).

Šajā sakarā Datu valsts inspekcija ir izstrādājusi «Personas datu apstrādes sistēmu audita rokasgrāmatu»,[60] kas var būt palīgs sistēmu pārziņiem, kuri vēlas paši veikt vai pasūtīt IS auditu, lai pārliecinātos par atbilstību *Fizisko personu datu aizsardzības likumam* un vispārējiem personas datu aizsardzības principiem.

IS drošības pārskats – nepieciešamības gadījumā īstenots visaptverošs un sistēmisks visu drošības faktoru novērtējums, pamatojoties uz detalizētiem veikto drošības auditu galarezultātiem,

[60] http://www.dvi.gov.lv/fpda/files/fpda_audita_rokasgramata.pdf

IS veicamo darbību un lietojuma detalizētu aprakstu un IS tehnisko un informācijas resursu darbības aprakstu, ar nolūku noteikt konstatētos un iespējamos IS apdraudējumus un nepieciešamās darbības IS drošības nodrošinājumam. Drošības pārskata sagatavošanā jāveic arī to uzņēmuma dokumentu izvērtēšana, kas attiecas uz uzņēmuma drošību, tajā skaitā IS drošību, kā arī jāizvērtē drošības monitoringa veikšanas pilnīgums un kvalitāte, veikto uzņēmuma darbības kvalitātes auditu rezultāti, personāla apmācības principi, viņu kvalifikācija un atbildība u.c. Drošības pārskatu var veikt arī kā papildinājumu, ja tiek veikta kaut kāda incidenta izmeklēšana. Ja IS drošības pārskata sagatavošanā tiek konstatēti riska faktori attiecībā uz citiem uzņēmuma darbības aspektiem (piemēram, ēku ugunsdrošība, personu ieejas kontrole, nepieciešamo normatīvo dokumentu iztrūkums vai tamlīdzīgi), arī par to informācija jāietver šajā pārskatā.

IS drošības pārskata pamatelementi ir: 1) pārskata sagatavošana un plānošana; 2) pārskata īstenošana un līdztekus veiktie pasākumi; 3) konstatēto un iespējamo IS apdraudējumu un korektīvo darbību definēšana; 4) pārskata atzinums un papildpasākumi. IS drošības pārskata veikšanā lietderīgi iesaistīt neatkarīgus, kvalificētus IS drošības speciālistus.

IS drošības monitorings ir pastāvīga kontrole attiecībā uz IS drošības būtiskākajiem iespējamiem apdraudējumiem, veicot IS auditācijas pierakstu analīzi un IS darbības kontroli. Tās pamatmērķis ir nodrošināt, lai tiktu uzturēts noteikts IS drošības līmenis. IS drošības monitoringu vēlams veikt saistīti ar IS administrēšanas funkcijām, salīdzinot IS faktisko darbību attiecīgajā brīdī ar noteiktajiem drošības kritērijiem. Visi nozīmīgie konstatētie apstākļi jādokumentē.

IS monitoringam parasti lieto specializētu programmatūru – 'ielaušanās atklāšanas sistēmas' IDS (*Intrusion Detection Systems*) un IPS (*Intrusion Prevention Systems*),[61] piemēram, tādas kā atvērtā koda bezmaksas programma *Snort,* kā arī dažādas komerciālas programmas, kas ļauj konstatēt ielaušanās pazīmes informācijas sistēmā (t.sk. gan datortīkla segmentā, gan arī atsevišķā resursdatorā) un IS administratoru brīdina par iespējamo apdraudējumu.

Šādas funkcijas ir ietvertas arī vairākās ugunsmūra programmās, turklāt ugunsmūra programmu auditācijas pierakstus var arī automatizēti izanalizēt ar specializētām programmām, lai konstatētu no IS drošības viedokļa nozīmīgus notikumus informācijas sistēmā. Bez kontroles un brīdināšanas funkcijām vairākām šādām programmām iestrādātas arī programmātiskas pretdarbības funkcijas, lai apgrūtinātu IS apdraudējumus, arī informācijas (pierādījumu) fiksēšana par notikušajiem ielaušanās mēģinājumiem, kā arī regulāra sistēmas failu integritātes pārbaude un brīdināšana par izmaiņām, kas notikušas ar tiem. Piemēram šāda tipa programmām var minēt *Tripwire,*[62] *AIDE (Advanced Intrusion Detection Environment),*[63] *Osiris,*[64] *Samhain*[65] u.c.

---

61 http://www.securityfocus.com/infocus/1514; http://www.networkintrusion.co.uk/ids.htm
62 http://www.tripwire.org
63 http://sourceforge.net/projects/aide
64 http://osiris.shmoo.com
65 http://samhain.sourceforge.net

IS pārvaldīšanai var norādīt šādus pamataspektus:

Uzņēmuma vadītājs, saskaņā ar ISDN, rakstiski norīko darbiniekus, kuri atbild par IS informācijas un tehnisko resursu drošību, rakstiski iepazīstinot viņus ar pienākumiem, tiesībām un atbildību. Uzņēmuma vadītājs vai viņa pilnvarota persona rakstiski norīko *pārzini* IS informācijas un tehniskajiem resursiem, ja vien uzņēmuma vadītājs pats nav uzņēmies šo funkciju (IS resursu pārzinis var būt attiecīgā uzņēmuma Informācijas sistēmas daļas vadītājs, bet mazos uzņēmumos tas var būt arī brīvlīguma darbinieks, kuram uzticēta uzņēmuma IS administrēšana un web lapas uzturēšana). Uzņēmuma vadītājam IS pārzinis jānodrošina ar nepieciešamajiem līdzekļiem – tehniskajiem un informācijas resursiem, kas nepieciešami IS drošības nodrošināšanai.

Jāatceras, ka par ISDN pārkāpumu noteiktos gadījumos var būt arī krimināla vai cita normatīvajos aktos noteiktā atbildība.

To personu vidū, kuras ir norīkotas kā atbildīgās par informācijas sistēmas drošību, jābūt arī informācijas sistēmas pārzinim, taču vismaz vienai no šīm personām vajadzētu būt arī tai, kura nav IS pārzinis. Par informācijas sistēmas drošību atbildīgo personu, kura nav IS pārzinis, – *drošības speciālistu* – norīko no tādām personām, kuras neatrodas informācijas sistēmas pārziņa pakļautībā (tas var būt attiecīgā uzņēmuma Drošības dienesta vadītājs), savukārt par IS pārzini norīko tādu personu, kura neatrodas drošības speciālista pakļautībā.

Ikviena persona, kura iesaistīta kaut kādu ar IS pārvaldīšanu vai IS drošību saistītu darbību veikšanai (var būt arī attiecīgajā uzņēmumā pamatdarbā nestrādājošs speciālists) pilnvaras apstiprina gan IS pārzinis, gan drošības speciālists.

Informācijas sistēmas pārzinis drošības speciālistam pēc viņa pieprasījuma nekavējoties sniedz visu informāciju par IS, saistībā ar veiktajām darbībām un notikumiem tajā. Bez tam IS pārzinis drošības speciālistam iesniedz veikto IS drošības auditu ziņojumus un IS drošības pārskata atzinumus, kā arī citu informāciju par IS informācijas resursu un tehnisko resursu stāvokli, notikumiem IS, kas var būt nozīmīgi apdraudējumi, kā arī visām veiktajām darbībām ar IS, kas saistītas ar tās drošību. Uz šo dokumentu pamata (ja nepieciešams, papildus vēl konsultējoties ar neatkarīgu datorspeciālistu) drošības speciālists var iesniegt priekšlikumus uzņēmuma vadītājam par nepieciešamajiem pasākumiem IS drošības nodrošināšanai.

Katram jaunam ar informācijas resursiem un tehniskajiem resursiem saistītam projektam jāveic **riska analīze**. Tā vajadzīga arī tad, ja IS notikušas izmaiņas, kas var ietekmēt IS drošību, kā arī riska analīzi veic periodisko drošības auditu ietvaros.

Riska analīze nepieciešama, lai novērtētu IS apdraudējuma varbūtību, kā arī iespējamo kaitējumu uzņēmumam vai personai, kura nodod informāciju IS, vai arī normatīvo aktu aizsargātām interesēm, ja nav nodrošināta IS drošība. Riska analīzi veic kā drošības audita sastāvdaļu, saskaņā ar metodiku, ko izstrādā IS pārzinis vai pieaicināti speciālisti un kuru saskaņo arī ar attiecīgā

uzņēmuma drošības speciālistu (kurš var pieaicināt konsultantus tās izvērtēšanai) un apstiprina uzņēmuma vadītājs.

Pirms nozīmīgu izmaiņu ieviešanas IS riska analīzes ietvaros lietderīgi pārbaudīt šo izmaiņu ietekmi uz IS darbību un lietošanu drošā vidē (piemēram, uz atsevišķa šim nolūkam izveidota datortīkla, kas nav savienots ar pārējo datortīklu), modelējot visus iespējamos apdraudējuma faktorus IS darbības stabilitātei un drošībai.

Informācijas sistēmas **pārziņa pienākumi** var būt noteikti šādi:

1. Veikt informācijas un tehnisko resursu aizsardzības pasākumus;
2. Veikt informācijas un tehnisko resursu drošības auditu un riska analīzi, nepieciešamības gadījumā šajā procesā iesaistot arī informācijas devējus;
3. Nodrošināt, ka IS tiek izdarīti auditācijas pieraksti un saskaņā ar ISDN nodrošināt to saglabāšanu un pieejamību pārbaudei;
4. Piešķirt uzņēmuma darbiniekiem tiesības piekļūt un rīkoties ar IS resursiem, kā arī organizēt kontroli pār šo resursu izmantošanu;
5. Nodrošināt informācijas resursu rezerves kopiju izgatavošanu un drošu glabāšanu, kā arī nodrošināt informācijas un tehnisko resursu atjaunošanu, ja IS darbība bijusi traucēta vai pilnībā pārtraukta;
6. Informēt informācijas devējus par nepieciešamību veikt informācijas klasificēšanu un ka informāciju var uzskatīt par vispārējas lietošanas informāciju, ja informācijas devējs tai nav piešķīris nekādu vērtības un (vai) konfidencialitātes pakāpi;
7. Nodrošināt visu darbinieku apmācību un zināšanu pārbaudi par informācijas un tehnisko resursu aizsardzību atbilstīgi viņu darba specifikai, kā arī rakstiski noteikt darbinieku pienākumus informācijas un tehnisko resursu drošības jomā.

IS apstrādāto, uzglabāto un pārraidīto informāciju var **klasificēt** pēc *vērtības* un *konfidencialitātes* pakāpes. Informācijai vērtības un / vai konfidencialitātes pakāpi piešķir informācijas devējs vai IS uzņēmuma vadītājs, vai arī IS pārzinis.

Ja informāciju aizsargā normatīvie akti (piemēram, korespondeces noslēpums, fizisko personu dati, valsts noslēpums u.c.), tad šās informācijas apstrādes, pieejamības un aizsardzības kartībai jāatbilst attiecīgo normatīvo aktu nosacījumiem.[66]

Vērtības pakāpi informācijai piešķir atkarībā no kaitējuma, kas var tikt nodarīts uzņēmumam vai personai, kura nodod informāciju IS, ja netiek nodrošināta informācijas integritāte un / vai pieejamība.

Konfidencialitātes pakāpi informācijai piešķir atkarībā no kaitējuma, kas var tikt nodarīts uzņēmumam vai personai, kura nodod informāciju IS, ja netiek nodrošināta informācijas

[66] Organizācijas, uzņēmuma ISDN ir zemākās hierarhiskās pakāpes normatīvais akts, tāpēc jāpiemēro augstāka spēka normatīvs akts (likums, Ministru kabineta noteikumi vai c.), ja tas reglamentē attiecīgo jomu.

konfidencialitāte.

Definējot to ar uzņēmuma ISDN, informācijai var piešķirt vērtības pakāpi: ***vērtīga informācija***, ja tās integritātes vai pieejamības nenodrošināšanas gadījumā informācijas devējam vai uzņēmumam var būt nodarīts būtisks kaitējums.[67]

Saskaņā ar uzņēmuma IS drošības noteikumiem, informācijai var piešķirt konfidencialitātes pakāpi: ***komercnoslēpums***, ja tai noteikts ierobežots saņēmēju loks un ja tās konfidencialitātes nenodrošināšanas gadījumā informācijas devējam vai uzņēmumam var būt nodarīts būtisks kaitējums.[68]

Lietderīgi ISDN noteikt un visos nepieciešamajos gadījumos arī norādīt termiņu, kāds ir vērtības vai konfidencialitātes pakāpei, kas piešķirta attiecīgajai informācijai.

Informācija, kurai nav piešķirta vērtības vai konfidencialitātes pakāpe un kuru neaizsargā arī normatīvie akti, ir *vispārējas lietošanas informācija*. Tādas informācijas integritāte, pieejamība un konfidencialitāte netiek īpaši aizsargāta.

Noteiktas klasifikācijas pakāpes piešķiršana informācijai nav atkarīga no informācijas nesēja veida (piemēram, vai tā atsūtīta ar e-pastu vai to ievada datu bāzē darbinieks no papīra dokumentiem; vai to saglabā uz servera vai kāda darbinieka portatīvajā datorā u.tml.). Uz pārnēsājamiem informācijas nesējiem jāizdara attiecīgi uzraksti, norādot piešķirtā informācijas klasifikācijas pakāpi. Uz pārnēsājamām ierīcēm informācijas uzglabāšanai (diskiem, USB atmiņas ierīcēm u.c.), kuros ir informācija ar konfidencialitātes vai vērtības pakāpi, norāda to.

Autentifikācijas informācijai, kas tiek lietota, lai tehniski piekļūtu IS glabātajai informācijai ar konfidencialitātes pakāpi, lietderīgi piešķirt tādu pašu pakāpi.

Ja ar citiem uzņēmuma iekšējiem normatīvajiem aktiem nav noteikta piekļuve noteiktam komercnoslēpumam, tad uzņēmuma vadītājs rakstiski nosaka to personu loku, kurām ir piekļuve tai, norādot arī konkrētas informācijas veidu un lietošanas tiesības. Izvēloties informācijas sistēmas aizsardzības pasākumus, jāievēro tajā apstrādātajai informācijai piešķirtās konfidencialitātes un vērtības pakāpes.

Serveriem un resursdatoriem, kur tiek uzglabāta vērtīga informācija un / vai komercnoslēpums, jāatrodas apstākļos, kas atbilst nosacījumiem par apdraudējumam adekvātu fizisko aizsardzību, un informācijas nesējus, kā arī portatīvos datorus ar tādu informāciju aizliegts atstāt vietās, kur nav nodrošināta to fiziskā aizsardzība. Resursdatorus, kur tiek uzglabāts komercnoslēpums, ja vien šī informācija nav šifrēta ar pietiekami drošu šifrēšanas metodi (*skat. turpmāk*), nepieslēdz ārējam datorīklam vai lokālajam datortīklam, no kura tehniski ir iespējama

[67] Jēdziens «būtisks kaitējums» var būt definēts uzņēmuma ISDN, taču jāievēro, ka tāda definīcija ietverta arī likumā *Par Krimināllikuma spēkā stāšanās un piemērošanas kārtību*.

[68] Ja iespējamais kaitējums nav būtisks, tad nav lietderīgi attiecīgo informāciju klasificēt kā komercnoslēpumu, jo informācijas aizsardzība ir efektīva vien tad, ja aizsargājamā informācija ir skaidri definēta, nosakot arī visus tās aizsardzības pasākumus. Ja uzņēmums vadītājs vadītos pēc pieejas, ka pilnīgi visa informācija, ko apstrādā uzņēmumā, ir komercnoslēpums, tad, visticamāk, tā netiktu pietiekami efektīvi aizsargāta.

izeja uz ārēju datortīklu. Jebkādas ierīces, kurās uzglabāts komercnoslēpums, pieļaujams iznest no attiecīgā uzņēmuma teritorijas tikai ar uzņēmuma vadītāja vai attiecīgās informācijas īpašnieka, valdītāja vai arī viņu pilnvarotas personas rakstisku atļauju.

Ja telpai nav droša fiziskā aizsardzība, tad resursdatorā glabātā komercnoslēpumu saturošā informācija jāšifrē. Tāpat ar kriptogrāfiskām metodēm jānodrošina integritāte vērtīgai informācijai, kas tiek sūtīta pa datu pārraides tīklu, kurš attiecīgo IS savieno ar citu uzņēmumu IS, vai kas savieno uzņēmuma telpas tā, ka tās šķērso teritoriju, kura nav attiecīgā uzņēmuma aizsardzībā.

Tomēr uzņēmuma ISDN var noteikt arī, ka komercnoslēpumu uzglabā un pārraida datortīklā tikai šifrētā veidā, neatkarīgi no datoru atrašanās vietas, lietojot pietiekami drošu šifrēšanas metodi.

Te var piebilst, ka par pietiekami drošu uzskata šifrēšanas metodi, kas iespējamo dešifrēšanas laiku uz jaudīgas aparatūras[69] ar efektīvām dešisfrēšanas programmām pagarina līdz tādam laika periodam, kad tās izmantošana vairs nevar radīt būtisku kaitējumu.

ANO Ekonomiskās sadarbības attīstības organizācijas «Informāciju sistēmu drošības vadlīnijās»[70] minēts: «Drošības līdzekļiem jābūt pietiekamiem, lai to apiešana prasītu lielākus līdzekļus par iespējamo ieguvumu no ielaušanās IS.»

Par pietiekami drošu šifrēšanas metodi mēdz uzskatīt, piemēram, *PGP* programmatūru ar ne mazāk kā šāda garuma atslēgu: 1536 bitu atslēga – līdz 2010.gadam vai 2048 bitu atslēga – līdz 2015.gadam. Citāda garuma šifra atslēgas izvēle jābalsta uz kriptogrāfijas algoritmu īpatnību izvērtējuma.[71]

Vērtīga informācija visā glabāšanas laikā jāaizsargā ar kriptogrāfiskām metodēm, kas nodrošina tās atjaunošanu, ja notikusi šīs informācijas izmainīšana, dzēšana vai attiecīgā datu nesēja iznīcināšana.

Par pietiekamu kriptogrāfisko aizsardzību pareizai informācijas atjaunošanai – no rezerves kopijas – uzskata vienvirziena šifrēšanu ar *hash* funkciju, lietojot *MD5* algoritmu ar 128 bitu garuma kriptogrāfisko kontrolsummu (*message digest*). Citāda matemātiskā algoritma un citāda garuma kriptogrāfiskās kontrolsummas izvēle jābalsta uz *hash* funkciju īpatnību novērtējuma.[72]

IS pārzinis norīko atbildīgos jeb lietotājus katram uzņēmumā lietotajam personālajam un portatīvajam datoram. Visu personālo un portatīvo datoru, kur glabājas komercnoslēpumu saturoša un / vai vērtīga informācija, aizsardzībai jāizmanto vismaz divas loģiskās aizsardzības metodes, tajā skaitā ne vien attiecīgās informācijas šifrēšana un / vai kriptogrāfiskā aizsardzība (*kā norādīts augstāk*), bet arī datora ieslēgšanas parole, kā arī priekš attiecīgām datora lietotāja jābūt izveidotam

---

[69] Diemžēl, vai par laimi, ievērojot tehnoloģiju straujo attīstību un plašo pieejamību mūsdienās, kļuvis grūti noteikt robežu tam, cik jaudīga aparatūra var būt pieejama personām, kuras ieinteresētas piekļūt tai vai citai šifrētai informācijai. Tas noteic vien nepieciešamību arī IS drošības jautājumus pastāvīgi pilnveidot.

[70] OECD Guidelines for the Security of Information systems.

[71] http://www.scramdisk.clara.net/pgpfaq.html#SubKeysize ; http://en.wikipedia.org/wiki/Key_size ; http://www.ecrypt.eu.org/

[72] http://www.rsasecurity.com/rsalabs/node.asp?id=2176

lietotāja kontam, turklāt lietotājs nedrīkst zināt paroli šā datora administratora kontam – lai vienkāršam lietotājam nebūtu tehniskas iespējas datorā instalēt programmatūru (t.sk. kaitīgas programmas bez viņa ziņas) un izdarīt nevēlamas izmaiņas tā konfigurācijā.

Katram informācijas sistēmas lietotājam IS pārzinis piešķir unikālu lietotāja vārdu un paroli, ar ko šī persona autentificējas un autorizējas piekļuvei IS resursiem. Izņēmums var būt vienīgi tās personas, kuras – kā viesi – saņem anonīmiem IS lietotājiem paredzētos pakalpojumus. Piešķirot lietotāja vārdu un paroli, lietotājs tiek brīdināts par atbildību, ja nepareizi glabā paroli un tā nonāk citu personu rīcībā.

Vienlaikus IS pārzinis nosaka arī attiecīgam lietotājam pilnvaras IS informācijas un tehnisko resursu lietošanā (tas jānodrošina arī programmātiski). Katram lietotājam jāpiešķir vienīgi tik lielas pilnvaras, cik viņam nepieciešams tiešo darba pienākumu pildīšanai vai pakalpojumu saņemšanai.

Parole drīkst būt zināma vienīgi IS lietotājam (izņemot pirmo paroli, ko lietotājs saņem no IS pārziņa). Pirmā parole lietotājam, īstenojot programmātiskos uzstādījumus, jānomaina tad, kad pirmo reizi autentificējas sistēmā, un visas nākamās paroles IS sistēmā jau jābūt uzglabātām šifrētā veidā ar pietiekami drošu šifrēšanas metodi, lai pat IS pārzinis tās nezinātu. Turpmāk lietotājam sava parole regulāri jānomaina uz jaunu paroli. Paroles nomaiņa tehniski jānoteic ar programmātiskiem uzstādījumiem IS, ko lietotājs nevar neizpildīt. Paroles maiņas biežums atkarīgs no IS apstrādātās informācijas vērtības un konfidencialitātes pakāpes; to vajadzētu darīt ne pārāk bieži, lai lietotājiem neveidotos ieradums paroles pierakstīt, nevis iegaumēt, un arī ne pārāk reti, lai mazinātos iespējas, ka lietotāji tās kaut kādu ērtību labad, piemēram, aizvietošanai atvaļinājuma vai komandējuma laikā, ir izpauduši kolēģiem. Optimāla var būt paroles nomaiņa divas līdz četras reizes gadā.

Vispārējos gadījumos minimālais paroles garums ir vismaz 8 simboli, un ir izmantoti gan burti, rakstot tos dažādos reģistros, gan skaitļi un speciālās zīmes. Lai lietotājam būtu vieglāk atcerēties paroli, lietderīgi ieteikt tiem veidot noteiktu frāzi.

Ja noskaidrojies, ka lietotājam piešķirtais lietotāja vārds un parole nonākusi citas personas rīcībā, IS pārzinis šo paroli nekavējoties anulē, piešķirot lietotājam citu. Turpmāk steidzamības kārtībā IS pārzinis vai drošības speciālists noskaidro šāda notikuma iemeslus, kā arī veic riska analīzi attiecībā uz iespējami jau citas personas izdarītu patvaļīgu piekļuvi IS.

Vispārīgi izplatītākās metodes piekļuvei parolēm ir šādas: visu iespējamo zīmju kombināciju izmēģināšana *(brute force)*, t.sk. mēģinājumi uzminēt paroli, izmēģinot vienkāršas taustiņu kombinācijas, kā arī pēc vārdiem, kas atbilst konkrētā cilvēka interesēm, dzīves apstākļiem u.c, mēģinājumi uzminēt pēc vārdnīcas *(dictionary attack)*; paroles pārtveršana ar lokālajā datortīklā strādājošu speciālu programmatūru *(sniffer);* paroļu meklēšana failos, kur tie var paviršības dēļ atrasties nešifrētā veidā, ja uzbrucējs ieguvis iespējas aplūkot failus resursdatorā; paroļu meklēšana failos, kur tās atrodas šifrētā veidā, cenšoties dešifrēt tos; paroles fiksēšana no apstrādājamiem

datiem datorā, tajā skaitā no taustiņu kombinācijām, kādus lietotājs nospiež uz tastatūras, šim nolūkam sistēmā slēpti ielādējot speciālu *Trojas zirga* jeb *System Monitors* tipa kaitīgu programmu *(key logger);* paroles fiksēšana vizuāli, vērojot lietotāja nospiestos tastatūras taustiņus ar slēpti izvietotu videokameru, vai arī paroles ievadīšanas brīdī klātesot kādam citam cilvēkam; paroļu meklēšana, pārskatot papīra lapiņas šī lietotāja darba vietā, arī piezīmju bloknotu u.c.; paroles uzzināšana no paša lietotāja uz uzticēšanās pamata (piemēram, parole var būt izpausta labam vai it kā labam paziņam, vai arī personai, kura apsolījusi palīdzēt veikt darbu, ko pats lietotājs neprot, vai pat persona apzināti par maksu paziņojis to kādam, lai tas iegūtu iespēju piekļūt viņa uzņēmuma IS); paroles uzzināšana no paša lietotāja, mudinot to atklāt maldinošā kādas interneta mājaslapas (piemēram, bankas, e-komercijas veikala, telekomunikācijas pakalpojuma sniedzēja) veidlapā, uz kuru lietotāja datora pārlūkprogramma ar viltu pāradresēta; paroles uzzināšana no paša lietotāja, zvanot pa telefonu un nosaucot maldinošu ieganstu *(social engineering*).

Te var piebilst, ka ir arī gadījumi, kad lietotājs vispār nelieto paroli piekļuvei kaut kādiem IS resursiem, ja tas nav pieprasīts, un netiek lietoti arī citādi autentifikācijas un autorizācijas līdzekļi.

Ja datorā ir informācija ar konfidencialitātes vai vērtības pakāpi, IS lietotājam, pārtraucot darbu kaut uz īsu brīdi, dators jāatstāj tādā stāvoklī, lai darbu varētu atsākt tikai pēc IS lietotāja autentificēšanas.

Kriptogrāfiskās metodes jāizmanto arī lietotāja identitātes un pilnvaru pārbaudei, ja pieeja komercnoslēpumu saturošai vai vērtīgai informācijai tiek dota ar datu pārraides tīkla starpniecību. Par pietiekami drošu var uzskatīt tikai divpakāpju aizsardzības metožu pielietošanu, piemēram, autentificētu lietotāju piekļuvi ar VPN (*virtual private network*) pieslēgumu.

Var uzstādīt arī nosacījumus, ka gadījumos, ja IS lietotāja autentificēšana no interneta pieslēguma vairākas reizes pēc kārtas ir neveiksmīga, piekļūšana IS no šā lietotāja izmantotās IP adreses tiek bloķēta, piemēram, ne mazāk kā 5 minūtes. Šāda metode var apgrūtināt pieslēguma patvaļīgu veidošanu ar automatizētu (programmas veiktu) lietotājvārda un paroles uzminēšanas metodi, līdz ar to padarot to mazāk efektīgu. Tomēr jāpiebilst, ka tādā veidā var rasties arī nevēlama situācija, kad tiek bloķēta IP adrese kāda datortīkla segmenta *proxy* serverim, līdz ar to bloķējot arī citus lietotājus šajā segmentā.

Ja lokālajā datortīklā tiek apstrādāta informācija ar konfidencialitātes vai vērtības pakāpi, to pieslēdz ārējam datortīklam (Internetam) tikai caur ugunsmūri, nodrošinot lokālā datortīkla loģisko aizsardzību. Resursdators, kas veic ugunsmūra funkcijas, būtu jāizmanto tikai šim nolūkam. Uz šā datora lieto pret patvaļīgu piekļuvi un citiem IS apdraudējuma veidiem pietiekami drošu un pareizi konfigurētu operētājsistēmu, kā arī IDS programmatūru (kuru var savienot arī ar *honeypots / honeynet* sistēmu).[73]

[73] http://www.tracking-hackers.com/papers/honeypots.html

Ugunsmūris nodrošina šādas funkcijas:

1. Veic datu pakešu filtrāciju pēc konfigurētiem nosacījumiem un pieļauj savienojumu veidošanu starp ārējo tīklu un lokālo datortīklu tikai ar atļautajiem tīkla protokoliem, portiem un programmām;
2. Liedz informācijas iegūšanu no ārējā datortīkla par izmantoto operētājsistēmu, serveru un resursdatoru atvērtajiem portiem, IS lietotājiem un informācijas resursiem;
3. Nodrošina *proxy* servera funkcijas, neļaujot veidot tiešu savienojumu ar lokālā datortīkla apakštīkla segmenta IP adresēm;
4. Var nodrošināt lokālā datortīkla skenēšanas, patvaļīgu savienojumu veidošanas, paaugstināta daudzuma datu pakešu sūtīšanas, ciklisku procesu izraisīšanas vai citādas neparastas aktivitātes konstatēšanu, to pārtraukšanu, kā arī dokumentēšanu un arī brīdinājumu nosūtīšana IS pārzinim par to;
5. Var nodrošināt apdraudoša rakstura pieslēguma avota konstatēšanu datortīklā, cik tas tehniski iespējams;
6. Nodrošina visu ārējo savienojumu un jebkādu IS apdraudējumu pazīmju auditācijas pierakstu veidošanu un saglabāšanu (vēlams vismaz vienu mēnesi);[74]
7. Var būt arī noteikta funkcija pārbaudīt elektroniskā pasta sūtījumus (arī pielikumu failus), vai tajos nav kaitīgu programmu pazīmes, u.c.

Ja kaut kādi datori tiek pieslēgti gan nepastarpināti ārējam datortīklam (piemēram, portatīvais dators tiek lietots mājās), gan arī lokālajam tīklam, vai arī pārrakstāms informācijas nesējs tiek ievietots arī citā datorā (piemēram, USB atmiņas ierīce vai pat fotoaparāta atmiņas karte, ko ievieto fotoaparātā, kuru savieno ar mājas datoru), tad visiem uzņēmuma datoriem jābūt apgādātiem ar atjauninātu efektīvu[75] antivīrusu programmu, kas konfigurēta tā, lai reāllaika režīmā pārbaudītu visus lietotāja failus, kas nonāk vai tiek apstrādāti šajā datorā, tajā skaitā arī īslaicīgas lietošanas mapēs un operatīvajā atmiņā. (Izņemot vienīgi, ja visos datoros tiek lietota tikai *Unix* bāzēta operētājsistēma, piemēram kāda GNU/Linux distribūcija, BSD saimes OS, Solaris vai tml. – tādā gadījumā antivīrusa programma, kā likums, nav vajadzīga vispār.)

No IS drošības viedokļa nav pieļaujams uzglabāt komercnoslēpumu, informācijas šifrēšanai / atšifrēšanai nepieciešamās atslēgas vai jebkādu citu konfidenciālu informāciju, ja datora savienojumu ar datortīklu vai ar jebkādu pārnēsājamu informācijas nesēju kaut jel vienā gadījumā neaizsargā pareizi konfigurēts ugunsmūris un lietotāja pilnvaru ierobežošana, un – *Windows* operētājsistēmām – arī efektīva antivīrusa programma, turklāt visa tajos lietotā programmatūra ir

[74] Te var piebilst, ka elektronisko sakaru komersantiem, saskaņā ar *Elektronisko sakaru likuma* 19.p. (1) d. 11) punkta un 71.[1] panta, un to Pārejas noteikumu 2.[8] panta nosacījumiem, ir noteikts pienākums saglabāt šī likuma 1.pantā un 2.pielikumā definētos saglabājamos datus 18 mēnešus.

[75] Jāteic gan, ka atrast pietiekami efektīvu antivīrusu var nebūt viegli. Piemēram, metamorfie vīrusi var būt veidoti tā, ka to kods tiek atšifrēts operatīvajā atmiņā pa daļām, secīgi arī izpildot attiecīgās koda daļas, pēc kā tās atkal tiek šifrētas ar mainīgu atslēgu, līdz ar ko operatīvajā atmiņā nekad nav viss tās kods un tas nav arī vienoti šifrēts.

atjaunināta un pareizi konfigurēta, atbilstīgi augstākajām prasībām nepieciešamās drošības un darbības stabilitātes nodrošināšanai, tajā skaitā ieslēgta *Data Execution Prevention* funkcija utt. Uzņēmuma vadītājam jāapzinās, ka daudzi lietotāji to nepratīs un arī nevēlēsies patstāvīgi nodrošināt. Tāpēc par to atbildība jāuzņemas IS drošības pārzinim. Un tas pilnībā attiecas arī uz paša vadītāja lietotajiem datoriem.

Auditācijas pierakstos programmātiski reģistrē visus IS darbībai un drošībai nozīmīgos notikumus un iespējamu IS apdraudējumu pazīmes, tajā skaitā aktivitāti lokālajā datortīklā, lietotāja veiksmīgos un neveiksmīgos piekļūšanas mēģinājumus IS, kā arī unikālo lietotāja vārdu un paroli, datumu un laiku, kad noticis katrs piekļuves mēģinājums.

Auditācijas pierakstus aizsargā ar loģiskās aizsardzības līdzekļiem un uzglabā, optimāli ne mazāk kā vienu mēnesi. Reizi mēnesī IS pārzinis vai viņa uzdevumā cita pietiekami kvalificēta persona veic auditācijas pierakstu izskatīšanu.

IS drošības noteikumos jānosaka arī vērtīgas informācijas, kā arī programmatūras **rezerves kopiju** *(backups)* veidošanas un uzglabāšanas kārtība, tajā skaitā norādot: a) uz kādiem datu nesējiem tās veido; b) kādi loģiskās un fiziskās aizsardzības līdzekļi tam tiek lietoti; c) kādos gadījumos rezerves kopijās uzglabāto informāciju šifrē; d) rezerves kopiju veidošanas biežumu; e) informācijas nesēju rotācijas principa ievērošanu un kā to īsteno; f) rezerves kopiju skaitu un glabāšanas ilgumu.

Vispārīgos gadījumos, ja nenotiek intensīva informācijas aktualizēšana, uzņēmuma vērtīgai informācijai rezerves kopijas var būt lietderīgi veidot ne retāk kā divas reizes gadā un katru reizi ne mazāk kā divos eksemplāros.

Ja arī tiek veidotas vērtīgas informācijas rezerves kopijas uz atsevišķiem nesējiem, vēl lietderīgi IS datu bāžu serveriem nodrošināt datu spoguļattēlu pastāvīgu veidošanu reāllaikā *(data mirroring)* ar *RAID (Redundant Arrays of Inexpensive Disks)* tehniku, kas iekļauj arī kļūdu pārbaudi un automatizētu datu atjaunošanu nepieciešamības gadījumā.

IS pārzinim jānodrošina, ka ar rezerves kopijām var atjaunot informāciju un programmatūru. Tāpēc lietderīgi veikt atbilstīgas tehniskas pārbaudes.

Informācijas resursu rezerves kopijas uzglabā fiziski dažādās vietās, kas izvēlētas tā, lai ārkārtas apstākļos (ugunsgrēks, applūšana, zādzība u.tml.) praktiski nebūtu iespējams vienlaikus sabojāt visas informācijas resursu rezerves kopijas.

Informācijas rezerves kopijas uzglabā tik ilgi, lai informācijas atjaunošana no tām vienmēr būtu iespējama bez pārtraukuma. Tas nozīmē, ka katras jaunas rezerves kopijas veidošanas laikā tiek uzglabāti šās informācijas citas rezerves kopijas. Arī rezerves kopijās klasificētu informāciju šifrē un kriprogrāfiski aizsargā ar pietiekami drošu metodi.

ISDN jānoteic **tehnisko resursu aizsardzība**, tajā skaitā: a) pasākumus, kas veicami

informācijas un tehnisko resursu aizsardzībai pret ugunsgrēku, plūdiem un citiem ārkārtas apstākļiem; b) tehnisko resursu tehniskajiem noteikumiem atbilstīgas gaisa temperatūras un mitruma nodrošināšanas līdzekļus telpās, kur tie atrodas; c) kādus tehniskos resursus apgādā ar iekārtām, kas uz noteiktu laiku uztur to darbību, ja zūd spriegums elektroenerģijas padeves tīklā, norādot arī, cik ilgu laiku jāuztur tehnisko resursu darbība; d) ar kādiem līdzekļiem nodrošina tehniskos resursus pret patvaļīgu fizisku piekļuvi, tīšu bojāšanu un zādzību; e) kā jāglabā pārnēsājamie datu nesēji un kā tie jāiznīcina.

Visās telpās, kur atrodas serveri vai resursdatori, pastāvīgi jānodrošina tāda temperatūra un mitruma līmenis, kāds paredzēts šo iekārtu lietošanai, kā arī jānovērš putekļu, vibrācijas, piedūmotības, tiešu saules staru, spēcīga ārēja elektromagnētiskā starojuma kaitīgā ietekme. Šajās telpās jāierīko ugunsdrošības automatizētie sensori un signalizācija – turot tos apsargājamās telpās.

Serveriem un resursdatoriem, kur tiek uzglabāta un apstrādāta vērtīga informācija, jānodrošina nepārtrauktās elektroenerģijas padeves avots UPS (*Uninterruptible Power Supply*), kas izlīdzina sprieguma svārstības elektronereģijas tīklā un tās zuduma gadījumā turpina elektroenerģijas padevi no neatkarīga avota vai, vismaz, spēj nodrošināt ar elektroenerģiju tik ilgi, kamēr tiek droši pārtraukta datora darbība. Vēlams izveidot iespēju, ka elektroenerģijas zuduma gadījumā serveriem, kuros apstrādā vērtīgu informāciju, automatizēti tiek nosūtīts trauksmes signāls (piemēram, uz IS pārziņa mobilo telefonu īsziņas veidā).

Saistībā ar portatīvajiem datoriem noteikti jāapzinās risks, ka var būt nozagts vai nolaupīts pats dators. Tāpēc vismaz jānodrošina visas tajā uzglabātās svarīgās informācijas šifrēšana, kā arī rezerves kopēšana uz citiem informācijas nesējiem. Bez tam jānovērš personas nokļūšana riskantās situācijās, kad to apjukumā var aizmirst, uz brīdi var atstāt nepieskatītu, kāds var to atņemt utt.

Gadījumos, kad tiek norakstītas vai citiem uzdevumiem nodotas trešajām personām tādas atmiņas ierīces, uz kurām iepriekš jebkad ticis uzglabāts komercnoslēpums vai cita aizsargājama informācija, jāveic visu uz tām saglabājušos datu (t.sk. it kā izdzēstas informācijas) pareiza pilnīga iznīcināšana, lai novērstu tās atjaunošanas iespējas.

Lietderīgi apsvērt iespēju ekranēt telpas, kur darbojas serveri un datori, kā arī izvietotas perifērijas ierīces, t.sk. uzmanību pievēršot arī kabeļiem, lai novērstu informācijas iegūšanu no datoru un to perifērijas iekārtu izstarotā elektromagnētiskā starojumu (TEMPEST). Nedrīkst pieļaut, ka nepiederošas personas, ja tās spējušas iekļūt dienesta telpās, var rast fizisku piekļuvi datortīkla iekārtām.

Ja tiek lietots **bezvadu tīkls** (piemēram, *WiFi, WiMax, Bluetooth),* tad lietderīgi lietot speciālus līdzekļus un metodes, lai novērstu informācijas iegūšanu no tā. Tomēr vislabāk vispār izvairīties bezvadu tīklos pārraidīt svarīgu informāciju (piemēram, finanšu norēķinu informāciju), jo bezvadu tīklu drošība vēl aizvien ir nepietiekama. Jāapzinās arī, ka mūsdienās aizvien vairāk

dažādas ierīces tiek aprīkotas ar bezvadu tīkla piekļuves tehnoloģiju, ne tikai portatīvie datori, tāpēc zemāk minētie drošības aspekti jāattiecina uz visiem organizācijas / uzņēmuma darbiniekiem, ja iekšējā tīkla resursiem ir bezvadu tīkla piekļuve. Arī *Bluetooth* u.c. veida bezvadu tīkli jāuztver kā nepietiekami droši pret apdraudējumu.

Bezvadu tīkla *WiFi* (*IEEE 802.11* standarts) pamatelements – bezvadu maršrutētājs – nodrošina *NAT* ugunsmūri (kas var nodrošināt konekcijas tikai no noteiktām statiskām IP adresēm), kā arī šifrēšanu vai nu ar novecojušo *WEP (Wireless Equivalent Privacy)* vai modernāko *WPA (Wi-Fi Protected Access)* tehnoloģiju, un arī bezvada tīkla karšu *MAC ID* jeb numuru filtrēšanu, ar ko maršrutētājs var noteikt piekļuvi tā, lai atļautu pievienoties tīklam tikai tām ierīcēm, kuru *MAC* numuri ir iekļauti iepriekš definētā sarakstā. *Wi-Fi* tīklos var uzlabot drošību, lietojot jaunākas iekārtas ar *IEEE 802.11i* standartu, kurā iekļauta papildus šifrēšana un piekļuves kontrole *WPA2 (Wi-Fi Protected Access 2)*. Bezvada tīklā arī var izveidot *Virtual private network* datu pārraidi – ar tiem lietotājiem, kuriem paredzētas konekcijas šajā tīklā, tomēr tas var nenodrošināt pietiekamu aizsardzību (tieši bezvadu tīkla datu pārraides īpatnību dēļ).
Jauniem *Wi-Fi* maršrutētājiem pēc noklusējuma jānomaina ražotāja uzstādītā parole. Bezvadu tīklā legāli lietotajos portatīvajos datoros ar Windows operētājsistēmu jāatslēdz iespēja veidot *ad hoc*[76] savienojumus, jo caur tiem var būt izveidota konekcija ar citiem šī tīkla datoriem, ja ir konfigurēta tāda iespēja (kas gan ir maz ticams, ka tā kāds darīs) vai ja datoriem ir resursi ar koplietošanas piekļuvi, turklāt *ad hoc* savienojumi notiek vispār bez šifrēšanas.
Kaut arī informācijas šifrēšana var palēlināt datu pārraides ātrumu bezvadu tīklā, tomēr to ļoti vēlams aktivēt. Ja netiek nodrošināta jebkāda aizsardzība, tad bezvadu datortīklā pārraida gan paroles, gan e-pasta ziņojumus un citu informāciju tādā formā, ka katrs, kurš uztveršanas zonā redz šo tīklu[77] un var tam pieslēgties, var pārtvert tajā arī citu lietotāju pārraidītos datus, lietojot kādu *sniffer* programmu datu analīzei un pielietojot *MAC spoofing* metodi. Uzbrucējs savu portatīvo datoru ar noteiktām programmām var konfigurēt tā, ka citu šī bezvada tīklu lietotāju konekcijas šajā tīklā tiek novirzītas caur uzbrucēja datoru (*man-in-the-middle* metode) vai pat pielietot šajā tīklā *DNS spoofing* uzbrukumu. Noteiktos gadījumos, ja sekmīgi izmanto to vai citu metodi neaizsargāta tīkla apdraudējumam, uzbrucējs var iegūt pat pilnīgu piekļuvi visiem tīklā lietoto datoru resursiem. Uzbrucējs var arī mērķtiecīgi traucēt neaizsargāta tīkla darbību. Tāpat pastāv arī iespēja, ka uzbrucējs ievieto kaitīgu programmu šāda neaizsargāta tīkla datorā, kas – nepareizas konfigurācijas dēļ – var būt pārnests arī uz citu, labāk aizsargātu tīklu.
Kā viena no drošākajām (kaut arī prasa papildus izmaksas) metodēm bezvadu tīklu aizsardzībai ir speciālu viedkaršu vai USB ierīču lietošana, kuras, ievietojot portatīvajā datorā un autentificējoties ar PIN kodu, ar speciālu programmatūru veido šifrētu savienojumu ar serveri, katrai konekcijas sesijai ģenerējot jaunu šifra atslēgu. Bez tam, var būt lietota arī iekārta ar speciālu programmatūru bezvadu tīkla ielaušanās atklāšanai, kas veic radio spektra monitoringu, lai konstatētu neautorizēta piekļuves punkta aktivitāti un novērstu cita veida apdraudējumus.[78] Tāpat arī telpu ekranējums var ierobežot bezvada tīkla piekļuves teritoriju.
Noslēdzot šo nelielo atkāpi par bezvadu tīklu drošību, var piebilst, ka dažkārt pat tiek apsvērta iespēja noteikt sodu par tīkla atstāšanu brīvai piekļuvei bez paroles.[79]

Turpinot aplūkot ISDN, vēl tajos jānoteic: a) vai un kā uzņēmums dod atļauju darbam lietot darbinieku īpašumā esošos datorus; b) vai darbinieki drīkst lietot uzņēmuma datoru personiskām vajadzībām; c) vai un kā uzņēmumam piederošu datoru darbinieks var lietot mājās.

IS drošības noteikumos tāpat jānoteic, kā jāveic informācijas un tehnisko resursu modernizācija, tajā skaitā paredzot arī: a) kā tiek novērtēta izmaiņu ietekme uz IS drošību; b) kā tiek veidots izmaiņu reģistrācijas žurnāls; c) kā pirms izmaiņu izdarīšanas tiek sagatavotas visu informācijas resursu rezerves kopijas.

IS drošības noteikumos jānosaka darbinieku apmācība, tajā skaitā lietderīgi apmācīt arī par informācijas aizsardzību un kaitīgo programmu profilakses, atklāšanas un likvidēšanas kārtību viņu personīgajos datoros.

Jāuzsver, ka, neatkarīgi no tā, kāda operētājsistēma un IS informācijas un tehniskie resursi

---

[76] http://jamus.co.nz/techthought/2009/07/18/wireless-ad-hoc-networking/

[77] Tomēr *SSID broadcasting* atslēgšana var mazināt vienīgi nelietpratēju apdraudējumu, jo ar speciālām programmām var redzēt šo tīklu arī tad, ja bezvadu tīkla identifikators *SSID* netiek atklāts.

[78] http://en.wikipedia.org/wiki/Wireless_Intrusion_Prevention_System

[79] http://drosiba.pudele.com/2010/05/german-court-orders-wireless-passwords/

tiek lietoti, vājākais posms IS drošībā vienmēr ir ***cilvēka faktors*** (ar to saistītas arī izplatītās maldināšanas metodes *social engineering).* Jebkādās IS informācijas aizsardzību var nodrošināt ar programmātiski pietiekami drošām kriptogrāfiskām metodēm, taču jebkuru IS apkalpo cilvēki ar visām tiem piemītošām vājībām.[80] IS drošība 90% ir atkarīga no sistēmas administratora darba, no sistēmas lietotāju darbības, no drošības politikas IS veidošanā, uzturēšanā un lietošanā, tāpēc IS drošība jāuztver kā komplekss problēmu loks, kam vajadzīga daudzpusīga izvērtēšana un risināšana.

Šādu uzskatu desmitajā ikgadējā *«Annual IT Security Summit»* konferencē izteica arī kompānijas *Gartner* informācijas drošības direktors Moguls *(Rich Mogull)*:[81] «Jebkurš nopietns uzbrukums sākās ar izsekošanu. Ļaunprātis var vienkārši atnākt uz firmas telpām un nofotografēt svarīgus dokumentus ar mobilā telefona vai kompaktas fotokameras palīdzību, vai pat pārrakstīt tos no datora, izmantojot USB atmiņas ierīci. Un šajā gadījumā nepalīdzēs neviena, pat ne vislabākā aizsardzības sistēma, kas aizsargā pret ielaušanos no Inerneta. Tāpat, lai uzzinātu paroles piekļuvei korporatīvajiem informācijas resursiem, nereti nav vajadzības uzlauzt datu bāzes. Bieži pietiek piezvanīt darbiniekam un, uzdodoties par tehniskā atbalsta dienesta darbinieku, pajautāt paroli. Šajā gadījumā nav nepieciešams tērēt resursus ievainojamību meklēšanai IS, paroļu piemeklēšanai utt.»

IS drošības nodrošināšanai lietderīgi maksimāli ierobežot informācijas sistēmā veicamos servisus un procesus, pieļaujot vienīgi tos, kas vajadzīgi IS funkciju izpildei stabili un droši.

Bez tam, darba vajadzībām parasti nav nepieciešams lietot vienādrangu tīklus *P2P, Skype,* arī *IRC, Instant Messaging,*[82] sociālos tīklus un iepazīšanās portālus *(draugiem.lv, one.lv, oho.lv, face.lv facebook.com,*[83]*odnoklassniki.ru*, *sekoman.lv, twitter.com*[84] u.tml.),[85] *virtuālās pasaules* servisus, t.sk. tiešsaites daudzlietotāju spēles, kā arī portālus ar pornogrāfisku saturu, tāpēc IS administratoram lietderīgi attiecīgi ierobežot interneta lietošanu.[86]

Papildus te vēl var pieminēt atsevišķus pamatieteikumus, kas tiek sniegti plašam personu lokam šajā jomā. Apvienotās Karalistes Tirdzniecības un rūpniecības departamenta atbalstītajā

---

[80] Firmas *Reed Exibirtions* konferences *«Infosecurity Europe 2004»* laikā veiktajā pētījumā konstatēts, ka 34% no 172 aptaujātajiem datora lietotājiem ar prieku atklāja datora paroli apmaiņā pret šokolādes tāfelīti, bet 37% vispār nevajadzēja pierunāt – viņi tāpat uzreiz atbildēja, kāda ir to parole. 40% paziņoja, ka zina savu kolēģu paroles. Pētījums tāpat liecināja, ka lielākā daļa darbinieku, pāriedami citā darbā, sev līdzi paķer konfidenciālu informāciju par darba devēju, ja vien viņiem ir tai pieeja.

[81] http://bdim.ru/arts.php?1634

[82] Publiskos *Instant Messaging* tīklos kaitīgas programmas var izplatīties visā pasaulē ārkārtīgi lielā ātrumā, jo tām nav jāmeklē viegli ievainojami datori. Piemēram, 30 līdz 40 sekundēs var inficēt pusmiljonu datoru. http://antivirus.lv/news.asp?l=lv&d=22.06.2004&n=2&w=l

[83] Kā piemēru var minēt gadījumu, kad Interpol ģenerālsekretārs Roberts Noble 2010.gada septembrī konstatēja, ka sociālajā tīklā facebook.com ir viltots viņa profils, lai piekļūtu sarakstei, ko viņš šajā tīklā veic par darba jautājumiem, tajā skaitā par Interpol plānotajām starptautiskajām operācijām smagu noziegumu apkarošanai.

[84] Jāpiebilst gan, ka IS drošības aspektā risku var radīt informācijas izplatīšana, nevis vienīgi tās saņemšana ar *twitter.com* u.tml. tehnoloģijām.

[85] Kaut arī sociālie tīkli tiek raksturoti kā Web 2.0 tehnoloģijas elements, tomēr to negatīvie sociālie aspekti būtiski nomāc pozitīvos. Piemēram, sk.: http://rodzhers.com/2008/03/08/13-socialo-tiklu-ipatnibas/

[86] Parasti izvēlas vai nu *black list* principu – ar aizliegto IP adrešu un domēna vārdu sarakstu vai arī *white list* principu – ar vienīgo atļauto IP adrešu un domēna vārdu sarakstu, kā arī sistēmā slēdz neizmantojamos portus. Bez tam liedz lietotājiem pilnvaras pašiem instalēt jebkādas programmas, izmainīt darba datora konfigurāciju utt.

«Informācijas drošības pārkāpumu pētījumā 2004», ko veica *PricewaterhouseCoopers*,[87] sniegti šādi ieteikumi:

1. Izmantot speciālistu zināšanas katru konkrēto uzņēmumu apdraudošo risku apzināšanai un iespējamo to mazināšanas veidu izvērtēšanai. Lieliem uzņēmumiem parasti ir iespēja algot pastāvīgus IS drošības speciālistus, mazākām organizācijām var būt lietderīgāk piesaistīt ārējos konsultantus.
2. Integrēt drošības prasības biznesa procesos. Absolūtais vairākums incidentu rodas uzņēmuma iekšienē, tāpēc visaptverošas drošības politikas izstrādei un ieviešanai, kā arī lietotāju apmācībai var būt izšķirīga loma uzņēmuma informācijas resursu aizsardzībai.
3. Veikt pietiekamus ieguldījumus drošības kontrolēs (lai mazinātu pastāvošos riskus) vai apdrošināšanā (lai nodotu riskus trešajai pusei).
4. Regulāri pārbaudīt drošības aizsardzības elementus, piemēram, OS drošības atjauninājumus, informācijas rezerves kopēšanas programmu, ugunsmūra konfigurāciju utt.
5. Efektīvi reaģēt uz drošības incidentiem, lai minimizētu normālas darbības traucējumus.
6. Veikt preventīvus drošības pasākumus, negaidot, kamēr notiks reāli incidenti.

Interneta drošības asociācijas internet *Security Alliance* dokumentā[88] kā 12 svarīgākie ieteikumi vidējiem un maziem uzņēmumiem informācijas aizsardzībai internetā ietverti šādi:

1. Drošu paroļu lietošana un to regulāra nomainīšana.
2. Tādas e-pasta programmas un interneta pārlūkprogrammas lietošana, kas nodrošina aizsardzību pret e-pasta vēstuļu pielikumos un interneta mājaslapu kodā ietvertām kaitīgām programmām.
3. Antivīrusu programmu lietošana un regulāra atjaunošana.
4. Ugunsmūra programmas lietošana.
5. Nevajadzīgu programmu un nevajadzīgu lietotāja kontu izdzēšana no IS; jebkādas informācijas izdzēšana no pārvietojamiem datu nesējiem.
6. Fiziskas piekļuves kontrole jebkurai datortehnikai.
7. Svarīgas informācijas un programmatūras rezerves kopiju veidošana.
8. Programmatūras pastāvīga atjaunināšana *(update)*.
9. Piekļuves kontrole datortīkla resursiem.
10. Piekļuves ierobežošana vērtīgai un konfidenciālai informācijai.
11. Finansiāla riska drošības pārvaldības plāna izstrāde un īstenošana; adekvāta risku apdrošināšana.
12. Drošības auditu veikšana un speciālistu konsultācijas.

---

[87] http://www.security-survey.gov.uk; http://www.pwc.com/Extweb/ncsurvres.nsf/docid/845A49566045759E80256B9D003A4773

[88] Woody C, Clinton L. Common Sense Guide to Cyber Security for Small Business. / Recommended Actions for Informations Security. 1st ed. – Arlington, Virginia, U.S.: internet Security Alliance, 2004. – 37 p. – http://www.isalliance.org

IS administratoram vai drošības pārzinim lietderīgi arī pastāvīgi sekot līdzi notikumiem pasaulē, kas saistīti ar IS drošības jautājumiem, tajā skaitā arī paziņojumiem par kaitīgu programmu izplatību, kā arī par jaunākajiem programmatūras atjauninājumiem. Šajā sakarā var pieminēt, ka ASV Drošības departaments *(Department of Homeland Security)* izveidojis **agrīno brīdinājumu sistēmu** *(National Cyber Alert System),* kas pastāvīgi un nekavējoties informē par konstatētiem jauniem apdraudējumiem IS. Šo sistēmu uztur ASV institūcija *US-CERT,* kura informāciju iegūst no dažādiem avotiem, pirmkārt, IT drošības uzņēmumiem. Sistēmas galvenais uzdevums – informācijas vākšana un tūlītēja izplatīšana divās mērķauditorijās: IT profesionāļiem (lielu datortīklu administratori, drošības speciālisti u.c.) un parastiem lietotājiem.[89]

Pabeidzot šo metodisko aspektu izskatīšanu, vēlreiz jānorāda, ka šeit tie aplūkoti tikai vispārīgi, jo konkrētā uzņēmumā šajā jomā jāņem vērā jau konkrētās IS darbības un lietošanas īpatnības un uzņēmuma kopējā drošības politika.

Operētājsistēmu drošības problemātika

Runājot par IS drošību, atsevišķi nedaudz uzmanību var veltīt arī operētājsistēmu (OS) drošības aspektiem, ievērojot, ka dažkārt sabiedrībā vai pat datorspeciālistu vidū izvēršas diskusijas par šo tematu, piemēram, par brīvi izplatītās atvērtā pirmkoda (*open source*) programmatūras[90] priekšrocībām salīdzinājumā ar personālo datoru tirgū mūsdienās dominējošo uzņēmuma Microsoft programmatūru, ko nereti reducē uz OS salīdzinājumu.[91] Šis jautājums gan ir ļoti plašs un tam nepieciešama tehnisko aspektu padziļināta izpratne, tāpēc te autors tikai nedaudz tam pieskarsies, kā disputam par šās jomas problemātiku. Lai saīsinātu šī jautājuma apskatu, autors arī pievērsīs uzmanību vienīgi personālo datoru operētājsistēmām, bet sīkāk neaplūkos mobilajos telefonos, web serveros, lieldatoros, tīkla iekārtās, spēļu konsolēs, dažādu tehnoloģisku iekārtu vadības ierīcēs un iegultajās sistēmās lietotās operētājsistēmas.

Iesākumā var paskaidort, ka jēdzienu *atvērtā pirmkoda programmatūra* raksturo daudzi aspekti, starp kuriem ir nozīmīgas īpatnības gan programmatūras licences noteikumos, gan programmatūras izstrādes, izplatīšanas un uzturēšanas praksē, tomēr īsumā šis jēdziens nozīmē, ka ikviens cilvēks var brīvi iepazīties ar programmatūras, tajā skaitā tās kodola *(kernel)* kodu, jo programmas kods ir pilnībā dokumentēts saprotamā formā, kamēr ar t.s. *slēgtā pirmkoda programmatūras* kodu lielākā daļa lietotāju nevar iepazīties, jo tas ir speciāli aizsargāts pret to, kompilējot tikai mašīnlasāmā formā.

Vispirms jānorāda, ka dažādu operētājsistēmu ir ļoti daudz un dažādas, tāpēc OS

[89] Jebkura persona var pierakstīties ziņojumu saņemšanai: www.us-cert.gov

[90] http://www.opensource.org/docs/osd

[91] Neapšaubāmi, Microsoft operētājsistēmas mūsdienās dominē personālo datoru tirgus nišā, kamēr web serveru, tīkla iekārtu un lieldatoru nišās dominē atvērtā pirmkoda programmatūra (galvenokārt, uz *Unix* standarta bāzētās OS).

salīdzinājumu nevar uzskatīt par korektu, ja salīdzina, piemēram, tikai *GNU/Linux*[92] distribūcijas ar *Windows* OS. Turklāt dažādas programmas un programmu skripti, kas var darboties tādā vai citādā OS vidē, ir tikpat kā bezgalīgi daudz. Tomēr diskusija par *GNU/Linux* (un citu uz *Unix* bāzēto OS) priekšrocībām attiecībā pret *Windows* OS Latvijā ir bijušas, tajā skaitā arī par IS drošības aspektiem, un droši vien būs arī nākotnē. Dažkārt šādu diskusiju iemesls tiek norādīts priekšstats, ka uzņēmums Microsoft, izmantojot gan dažādas mārketinga metodes, gan patentu likumu normas, gan lobijus, cenšas mazināt personālo datoru lietotāju, uzņēmumu un valsts institūciju pāriešanu uz atvērtā pirmkoda operētājsistēmām, tajā skaitā arī pasūta pētījumus, kuros izdarīti secinājumi, ka *Windows* operētājsistēmas ir salīdzinoši drošākas,[93] kam gan daļa IT speciālistu nepiekrīt, teikdami, ka Microsoft izstrādāto OS drošības līmenis nav vis augstāks, kā citām OS.

Netieši šādai kritikai piekrīt arī Microsoft, vienlaikus gan mēģinot novērst atbildību no sevis kā programmatūras izstrādāja uz lietotājiem un pakalpojumu sniedzējiem. Piemēram, Microsoft publiskoja ierosinājumu ieviest tādu globālu «kolektīvās drošības sistēmu» cīņā pret kaitīgo programmatūru, botu tīkliem u.tml., kad interneta pakalpojumu sniedzējiem jeb provaideriem, būdami tam attiecīgi tiesiski pilnvaroti, būtu pienākums atslēgt no interneta inficētos datorus, līdz problēmas novēršanai. Vairāki datorspeciālisti gan ir publiskojuši arī skeptisku viedokli par šo iniciatīvu, norādot, ka visbiežāk inficēti jau ir tieši datori ar *Windows* operētājsistēmu, internet *Explorer* pārlūku, *Microsoft Office* lietojumprogrammām un *.Net Framework* programmatūru satvaru, tāpēc būtu vērtīgāk, ja Microsoft vairāk pūles veltītu savas programmatūras drošības uzlabošanai, nevis centieniem izmainīt tiesisko kārtību globālā mērogā, kas turklāt ir iluzors risinājums, ievērojot interneta decentralizēto struktūru. Un tāda veida ierosinājumus novedot līdz absurdam, tikpat var ierosināt globālā mērogā aizliegt pārdot tādas operētājsistēmas, kurām praksē ir visvairāk drošības problēmu... Ja Microsoft pat savā web vietnē kā pamatieteikumu lietotājiem uzsver ne vien programmatūras atjaunināšanu un ugunsmūra lietošanu, bet arī antivīrusa programmatūras lietošanu, brīdinot par vīrusu ievērojamo apdraudējumu, tad *Unix* bāzētās operētājsistēmās šāda problēma, vismaz līdz šim, vispār nav aktuāla.

Vispirms gan jāuzsvers, ka nevienas operētājsistēmas lietošana pati par sevi negarantē drošību. IS drošības nodrošinājumam, kā jau iepriekš izklāstīts, vajadzīga kompleksa sistēmiska pieeja. IS drošības firmas *Counterpane internet Security, Inc.* dibinātājs Šneijers *(Bruce Schneier)* pārskatā par IS drošības problēmām trāpīgi norādīja: «IS drošība nav produkts, bet gan process.»[94] Tāpēc nav pareizi paļauties uz to vai citu programmatūru, pat ja tā tiek raksturota kā drošāka, jo vienalga pastāvīgi būs dažādi apdraudējumi, kuru mazināšana iespējama vien tad, ja IS pārzinis pastāvīgi seko līdzi IS darbībai un konfigurācijai un pastāvīgi strādā pie drošības aspektu

[92] Korekti ir lietot terminu *GNU/Linux*, kas norāda gan uz šo OS koda tehniskajiem aspektiem, gan to licences aspektiem. Tomēr dažreiz šīs OS mēdz saīsināti saukt *Linux*.

[93] http://www.betanews.com/article/Microsoft-Vista-Most-Secure-OS-Ever/1150366131

[94] http://schneier.com/crypto-gram-9912.html

pilnveidošanas attiecībā uz visiem IS informācijas un tehniskajiem resursiem.

IT drošības speciālisti, veicot OS salīdzinājumu, kā drošākās un stabilākās nosauc uz *Unix* standarta izstrādātās (‘*Unix-like*’) operētājsistēmas, tajā skaitā *BSD (Berkeley Software Design)* saimes OS, pirmkārt jau *OpenBSD*,[95] no kuras īpaši neatpaliek *FreeBSD* apakšprojekts *TrustedBSD*, kā arī vairākas *GNU/Linux* distribūcijas, tajā skaitā *Security-Enhanced Linux*[96] modifikācijas, piemēram, *Ubuntu* distribūcijai. Dažreiz nosauc arī *Mac OS X*,[97] kaut gan šo OS arī kritizē.[98] Arī vairākas kompilētā pirmkoda operētājsistēmas ir izstrādātas[99] un / vai novērtētas[100] pēc augstiem formālajiem drošības un stabilitātes standartiem, piemēram, *Trusted Solaris*,[101] *HP-UX*,[102] *LynxOS-178 RTOS* [103] u.c. Šis salīdzinājums gan laika gaitā tiek rediģēts, piemēram, informācija par savulaik līderi šajā aspektā *GEMSOS* [104] vairākus gadus vairs netiek aktualizēta.

Operētājsistēmas darbības drošības novērtēšanai (noteiktā IS konfigurācijā), savienojot dažādu valstu standartus, kopš XX gs. deviņdesmitajiem gadiem mēdz piemērot vienotu starptautisku metodisku pieeju, kuru 1999.gadā pieņēma kā Starptautiskās standartu organizācijas ISO standartu – ISO 15408 «Informācijas sistēmu drošības novērtējuma kritēriji». Saskaņā ar ASV Aizsardzības departamenta 1985.gada «Oranžo grāmatu»,[105] šis standarts atbilst t.s. «vienotajam kritērijam» *(Common Criteria).*

Common Criteria standarts sadalīts trīs daļās: «Ievads un vispārējais modelis. Drošības funkcionālās prasības. Drošības garantēšanas prasības.» Atbilstība drošības funkcionālajām prasībām tiek noteikta pēc «klasēm» *(Classes),* kur katra klase ietver daudzpusīgu novērtējumu identifikācijai un autentifikācijai informācijas sistēmā, datu aizsardzībai, drošības menedžmentam, komunikāciju drošībai un auditam, savukārt atbilstība drošības garantēšanas un kontroles prasībām attiecīgās klasēs tiek novērtēta ar «novērtēšanas garantijas līmeni» – *EAL (Evaluation Assurance Level).* Kopumā ir septiņi *EAL* līmeņi, no kuriem *EAL7* šajā drošības standartā ir visaugstākais. Tie atbilst noteiktām klasēm. Kā piemēru var minēt, ka ASV Aizsardzības departamentā noteikts, ka neklasificētu IS drošībai jāatbilst *Class C2* jeb *EAL3* līmenim. Šis līmenis tiek definēts kā «metodiski testēts un pārbaudīts» un tas ir pieņemams, kad nepieciešams vidējs drošības līmenis.

Tajā pašā laikā daudzi IT drošības speciālisti kritizē šo standartu kā nepietiekami piemērotu vispusīgai un objektīvai dažādu sistēmu novērtēšanai. Līdz ar ko mūsdienās programmatūras, t.sk.

---

95 http://wiki.answers.com/Q/What_is_the_most_secure_operating_system
Jāpiemin gan 2010.gada decembrī publiskotā skandalozā informācija, ka ASV FIB ar piesegorganizācijas palīdzību panācis slēptas piekļuves rīku iekļaušanu OpenBSD IPSEC-stekā, ko lieto VPN kriptogrāfiskai aizsardzībai.

96 http://www.nsa.gov/research/selinux/index.shtml

97 *Mac OS X ir* izstrādāta uz *FreeBSD* kodola un *Mach* mikorkerneļa (kas arī ir *Unix* standarts) bāzes.

98 http://news.techworld.com/security/1798/mac-os-x-security-myth-exposed/

99 http://en.wikipedia.org/wiki/Security_focused_operating_system

100 http://en.wikipedia.org/wiki/Security-evaluated_operating_system

101 http://www.sun.com/software/solaris/trustedsolaris/index.xml

102 http://en.wikipedia.org/wiki/Trusted_operating_system

103 http://www.lynuxworks.com/rtos/lynxos-178.php3

104 http://www.aesec.com/

105 http://csrc.nist.gov/publications/secpubs/rainbow/

operētājsistēmu testēšana tiek veikta ar daudzpusīgāku metodisko pieeju.[106]

Viens no programmatūras testēšanas etapiem ir drošības testēšana, kurā nosaka sešu pamataspektu nodrošinājumu: konfidencialitāte (informācijas atklāšanas nepilnvarotām personām novēršana), integritāte (informācijas neizmainīts veselums, par ko lietotājs var pārliecināties), autentificēšana (lietotāja identitātes konstatēšanas process), autorizēšana (pilnvaru – piekļuvei noteiktiem IS resursiem vai īstenot funkciju – konstatēšanas process), pieejamība (IS informācijas resursu un komunikācijas kanālu lietošanas gatavība paredzētajos apstākļos) un ne-atteicamība (pakalpojuma atteices, ja tiek īstenots kaut kāds apdraudējums, novēršana).

Nenoliedzami, dažādu programmatūru un OS drošības aspektu novērtēšanas metodiskās pieejas precizitāte un ticamība (*validity*) un procedūras drošība (*reliability*) paliek speciālistu kompetences lokā, bet nespeciālistiem atliek vien paļauties uz publiskotajiem pētījumu ziņojumiem, pat ja tie mēdz atšķirties secinājumos, kam iemesls var būt arī pētījuma pasūtītāja selektīvi izvēlētie kritēriji, līdz ar to radot neobjektīvu rezultātu.

Neraugoties uz minēto, nevar tomēr nepamanīt arī vairākus vispārīgus argumentus, ko izvirza atsevišķi atvērtā pirmkoda programmatūras entuziasti. Tajā skaitā to, ka uz *Unix* standarta bāzētajās operētājsistēmās jau kodola līmenī var noteikt, kas un kādā veidā vispār var pieslēgties konkrētam datoram un cik lielā mērā var būt veiktas konkrētas programmātiskas funkcijas. *BSD, GNU*/*Linux, Solaris* u.c. t.s. **nix* operētājsistēmās jau kodola līmenī iebūvēti vairāki drošības risinājumi, tajā skaitā IP adresācija ugunsmūrim *(iptables),* lietotāju autorizācija, atbalsts kriptēšanai tīkla protokolu līmenī, aizsardzība pret *buffer overflow* apdraudējumu (ko mēdz veikt *DoS* jeb *Denial of Service* uzbrukumos), sistēmas stabilitātes nodrošināšana ar resursu dalīšanu laiksakritīgiem procesu pavedieniem *(threads),* atbilstība IT atvērtajiem standartiem u.c. Šo OS lietotāji (tātad arī neautorizēti procesi, kas sistēmā darbojas ar lietotāja pilnvarām) pēc noklusējuma neiegūst administratora (*root*) pilnvaras, kas dotu iespējas veikt darbības, kuras būtiski ietekmē OS drošību.

Piemēram var raksturot datortārpu *Koobface*, kas tiek izplatīts sociālajos tīklos kā vēstule ar intriģējošu nosaukumu, pēc kuras atvēršanas pārvirza pārlūkprogrammu uz citu web vietni ar it kā interesējošo video filmiņu, kur jau piedāvā datorā instalēt it kā programmatūras atjauninājumu, kas faktiski gan ir kaitīga programma un inficē datorus, kuros ir instalēta neatjaunota *Java* platforma, pēc kā veic kaitīgas funkcijas, t.sk. iegūst no datora sensitīvu lietotāja informāciju, ko lieto finanšu norēķinu sistēmās u.c., kā arī pieslēdz datoru botu tīklam, lai īstenotu DDoS uzbrukumus un izsūtītu mēstules, un vienlaikus arī (ar šajā kaitīgajā programmā iekļautu DNS filtru) liedz datora piekļuvi antivīrusu resursu vietnēm internetā. Šī ir viena no ārkārtīgi daudzajām – vairāki desmiti miljoni – kaitīgajām programmām, kādas apdraud Windows OS, turklāt apdraudējums tām ir pavisam reāls. Un tā ir viena no tikai dažām kaitīgajām programmām, kas vispār radītas arī *Mac OS X* un *Linux*

[106] http://en.wikipedia.org/wiki/Software_testing

OS, tomēr arī tad apdraudējums ir vien teorētisks – jo šajās OS tas spēj izplatīties vien lietotāja kontā, kam pēc noklusējuma ir ļoti ierobežotas pilnvaras, un pēc datora pārstartēšanas šī kaitīgā programma nespēj atjaunot savu darbību. Turklāt *Linux* OS pēc noklusējuma *Java* platforma netiek iekļauta vispār. Tāpēc pat šādu atsevišķu kaitīgu programmu radīšana vienalga *Unix* standarta operētājsistēmu lietotājiem nerada nepieciešamību pēc antivīrusa programmas.

Kaut arī *Windows* jaunākajās operētājsistēmās, t.sk. *Windows 7* ir būtiski uzlaboti drošības risinājumi, tomēr vēl aizvien atrodas iemesls kritikai, jo *Windows* un *Unix* arhitektūra veidota ar atšķirīgiem pamatprincipiem, tajā skaitā *Windows* OS izstrādātas tā, lai lietotāja programmatūrai piešķirtu lielāku funkcionalitāti un to dziļi integrētu sistēmas kodolā (sākotnēji *Windows* OS vispār nebija izstrādāta lietošanai tīklam pieslēgtā datorā, kuru jānodrošina pret ārējiem apdraudējumiem), savukārt uz *Unix* standarta veidotās sistēmas izstrādātas tā, lai skaidri nodalītu sistēmas darbības lauku no lietotāja darbības lauka. Tāpēc kaitīgas programmas un *hakeri* var izmantot tehniski daudzus veidus, ko dod *Windows* programmatūrai piešķirtā funkcionalitāte, ietekmējot sistēmas darbību, savukārt *Unix* standarta sistēmās tādas iespējas ir minimālas vai nav vispār pašas sistēmas arhitektūras dēļ.[107] Piemēram, viens no retajiem *Linux* OS radītajiem vīrusiem *Bliss* spēja inficēt datoru tikai, ja lietotājs pats apzināti instalēja šo programmu, un tikai tās lietojumprogrammas, kuras lietotājam bija pilnvaras izmainīt, līdz ar ko faktiski šis vīruss bija nekaitīgs. Vīruss *Bliss* nespēja izplatīties plašāk un tā arī palika vien IT drošības pētnieku eksperimentāls produkts. Tajā pašā laikā daudzi miljoni *Windows* OS radīti vīrusi spēj inficēt datoru pilnībā bez lietotāja ziņas un pat sistēmas kodola līmenī. Iemesls tam ir tieši minētās atšķirības operētājsistēmu arhitektūrā.

Jaunākajās Microsoft operētājsistēmās – *Windows Vista* un *Windows 7* jau ir iekļauta tehnoloģija lietotāja pilnvaru nošķiršanai pēc noklusējuma (*User Account Control*) un citas drošības metodes, kādas vienmēr bijušas *Unix* sistēmās, tāpēc šīs *Windows* OS noteikti var novērtēt kā drošākas par iepriekšējām. Tomēr, kā jau norādīts, tas nedod pamatu apgalvot, ka tās kļuvušas drošākas par visām pārējām OS. Faktiski tās tikai tuvojas *Unix* standarta OS drošības līmenim.

Attiecībā uz IS drošību nozīme ir arī programmatūras atjauninājumu izlaišanai. Atšķirībā no atvērtā pirmkoda programmatūras izstrādātājiem, Microsoft negribīgi nodrošina atjauninājumus vecākām operētājsistēmas versijām, mudinot lietotājus iegādāties aizvien jaunu programmatūru.

Vēl viens aspekts attiecībā uz drošību ir arī programmatūru licencēšanas īpatnības. Atvērtā pirmkoda programmatūras licences, t.sk. *GNU GPL, BSD, MIT* u.c.[108] ļauj visplašākajam personu lokam iepazīties ar programmatūras kodu, izvērtēt, pārbaudīt to un savām vajadzībām arī izmainīt (pirms programmatūras noslēguma versijas izplatīšanas to pilnībā pārbauda kvalificēti eksperti, pielietojot arī īpašu drošības procedūru). Avērtā pirmkoda programmās viss kods ir pilnībā dokumentēts un pieejams, lai izslēgtu situācija, ka programmas izstrādātājs atstāj programmā

[107] http://www.itworld.com/security/75601/why-windows-security-awful
[108] http://opensource.org/licenses

nozīmīgas nepilnības, kuras lietotājam nebūtu iespējas uzzināt, vai pat atstāt programmā patvaļīgas piekļuves iespējas *(backdoors)*. Savukārt Microsoft licences ierobežo tādu iespēju. Tādēļ Microsoft programmatūras drošības aspektus dažkārt raksturo ar frāzi: «Drošība dēļ neziņas» (*mūsdienās gan šī situācija ir uzlabota, skat. tālāk*).

IS drošība ietver ne tikai aizsardzību pret patvaļīgu piekļuvi un kaitīgām programmām, bet arī datoru darbības stabilitāti (kā jau minēts, IS drošība nozīmē arī IS resursu pieejamību). Šā aspekta dēļ serveru un superdatoru nišā izvēlas *Unix* standarta operētājsistēmas.[109] Daudzas valstis[110] pievērsušās atvērtā pirmkoda programmatūras, t.sk. *GNU/Linux* OS ieviešanai dažādu valsts pārvaldes iestāžu vai valstiski nozīmīgu uzņēmumu IS. Atvērtā pirmkoda programmatūru savās IS lieto arī starptautiskas organizācijas, piemēram, ANO, ES, UNESCO, NATO, Pasaules Banka u.c.

Minētās tendences dēļ Microsoft 2002.gadā pieņēma lēmumu atklāt savu operētājsistēmu kodu valstu valdībām un to institūcijām, Šo iniciatīvu sauc «Valdības drošības programma», jo piekļuve OS kodam dod iespēju valstu valdībām pārliecināties, vai viņu izmantotajā programmatūrā nav ietvertas kaut kādas nedefinētas jeb *backdoors* funkcijas. Microsoft paziņoja arī par vairāku *Windows* OS koda atklāšanu privātpersonām – Microsoft sabiedrības *Most Valuable Professionals* biedriem, kas tiek veikts programmas *Shared Source Initiative* ietvaros.[111]

Tas, ka programmatūras kods ir jebkuram brīvi pieejams, turklāt to arī izvērtē ļoti daudzi programmētāji *(*kā tas ir *open source community)* gan entuziasti, gan profesionāļi, dod iespēju, ka jebkurš uzņēmums ar kvalificētu speciālistu palīdzību var pats pārliecināties, ka noteiktā programmatūrā nav kaut kādas nevēlamas nepilnības. Tādu argumentu minēja arī ASV Nacionālā aeronautikas un kosmosa aģentūra NASA pētnieks Morans (*Patrick Moran*), komentējot NASA noslēgto vienošanos ar atvērtā pirmkoda programmatūras iniciatīvas grupu *(Open Source Initiative):* «Lielāks skaits programmētāju, kuri pārskata programmas pirmkodu, var efektīvāk atrast nepilnības un potenciālas problēmas».

Piemēram, 2003.gadā *Linux* jaunākā kodola versijas *beta* testēšanas stadijā uz servera *BitKeeper* kāda persona (testēšanas laikā jebkurš var brīvi piekļūt *beta* versijai) bija mēģinājusi šīs OS kodolā ievietot *Trojas zirgu*, kas ļautu patvaļīgi piekļūt datoriem ar šo OS. Taču šis mēģinājums beidzās neveiksmīgi, pirms tika pabeigts – jau tuvāko 24 stundu laikā testēšanas procesā obligātajā salīdzināšanā ar OS koda kriptogrāfisko kontrolsummu, ko veic drošības programma, tika pamanītas izmaiņas kodā un drošības programma sacēla trauksmi, pēc kā jau tūlītāji tika konstatēts šo kaitīgo darbību mēģinājums, līdz ar ko kaitīgās funkcijas tā arī nenonāca līdz noslēguma

[109] http://en.wikipedia.org/wiki/Usage_share_of_operating_systems

[110] http://www.netc.org/openoptions/pros_cons/world.html#government
http://www.openia.com/resources/open-source/governments/

[111] http://www.microsoft.com/resources/sharedsource/default.mspx
Jāpiebilst gan, ka IT speciālisti par šo Microsoft iniciatīvu dažkārt izsaka arī kritiku, norādīdami, ka OS koda daļēja atklāšana daudz neko nemaina, jo neatkarīgi speciālisti nevar testēt programmas kodu noteiktos apstākļos – Microsoft pieļauj vienīgi aplūkot kodu, taču nepieļauj veikt jekbādas darbības ar to.

(release) versijai.

Salīdzināšanai var minēt, ka Microsoft programmatūras kļūdas tiek atklātas daudz un bieži, taču tās dažkārt ir palikušas nenovērstas vairākus mēnešus un pat vairākus gadus. Turklāt nereti tās atklāj nevis Microsoft testētāji, bet gan neatkarīgi IT drošības speciālisti vai *hakeri,* daļa no kuriem nekautrējas arī tās ļaunprātīgi izmantot.

Te gan jāpiebilst – lai gan atvērtā pirmkoda programmatūras novērtēšana teorētiski ir pieejama ikvienam, tomēr praktiski tā nav ikvienam pa spēkam. Operētājsistēmu individuāla novērtēšana ir nosacīta iespēja, jo to kods ir ļoti liela apjoma, to algoritma un iekšējās struktūras, kā arī visu koda rindiņu detalizēta analīze prasa milzīgu laika ieguldījumu, kuru, turklāt, spēj īstenot vienīgi speciālists, un tādam darbam nepieciešama arī pietiekama motivācija. Motivācija var būt vai nu maksa par šo darbu vai arī personas entuziasms. Iespēja, ka t.s. *atvērtā koda sabiedrībā* vienmēr atradīsies pietiekams daudzums entuziastu, lai savlaicīgi notestētu visu atvērtā koda programmatūru, faktiski pastāv un šāda prake arī tiek veicināta, tomēr tā nav garantēta. Tāpat kā nav garantijas arī, ka komerciāli izplatītā kompilētā koda programmatūrā nav tīši vai aiz neuzmanības atstātas tādas funkcijas, kas var radīt kaitējumu lietotāja interesēm. Līdz ar to šāda veida riska faktors gan atvērtā koda, gan kompilētā koda programmatūras lietošanā kaut kādā ziņā līdzsvarojas.

Jānorāda, ka programmatūras pārbaudē var pielietot ne tikai iekšējās struktūras analīzi, bet arī t.s. «melnās kastes» testēšanas metodi – izpētot attiecīgās programmas funkcionalitāti dažādos noteiktos apstākļos un pēc noteiktiem kritērijiem, līdz ar ko testētājam programmas kodu un iekšējo struktūru nav nepieciešamības zināt. Vispārīgi tas nozīmē, ka tiek specifiski noteikti ieejošie dati informācijas sistēmā, kurā dažādos apstākļos ar dažādām metodēm tiek testēta attiecīgā programmatūra, un tiek novērtēti izejošie dati no šīs sistēmas un programmatūras funkcijas.

Noslēdzot šo vispārīgo disputu, skaidrs, ka speciālistu vidū dažādu operētājsistēmu priekšrocības un trūkumi tiek skatīti ļoti daudzpusīgi. Tāpēc katras organizācijas / uzņēmuma vadītājam un IS pārzinim vajadzētu atbildīgi paredzēto funkciju izpildei gan izvēlēties, gan konfigurēt noteiktu programmatūru, izvērtējot speciālistu atzinumus arī par drošības aspektiem.

Elektronisku finanšu darījumu drošības pamataspekti

Papildus aplūkotajiem jautājumiem var vēl atsevišķi īsumā pievērsties jautājumam, kas bieži ir individuālu lietotāju uzmanības centrā saistībā ar IS drošību – kā nosargāt savu naudu, veicot elektroniskus norēķinus internetā. Nenoliedzami, ikvienam individuālam datorlietotājam īpaši uzmanīgam un piesardzīgam jābūt darījumos ar maksājuma kartēm, jo finanšu informācija ir lielākās daļas apdraudējumu mērķis, turklāt elektroniski finanšu norēķini kļūst aizvien izplatītāki, bet šādos gadījumos par savas naudas drošību jārūpējas katram pašam (atšķirībā no uzņēmuma vai

valsts organizācijas, kur, piemēram, komercnoslēpuma vai ar likumu aizsargātas informācijas aizsardzību nodrošina IS drošības pārzinis).

Diemžēl, individuālie datorlietotāji dažkārt mēdz būt neapdomīgi attiecībā uz informācijas drošību, kas var radīt arī būtiskus finansiālus zaudējumus, piemēram, ja *datorkrāpnieki* piekļūst bankas kontam. Te var minēt firmas *Fittkau&Maaß* 2004.gada pētījuma datus, ka tikai katrs otrais individuālais interneta lietotājs Vācijā bija uzstādījis kaut kādu antivīrusu programmu (kaut arī daudzas firmas privātiem lietotājiem šo pakalpojumu piedāvā pat bez maksas). Vēl retāk individuālie lietotāji izmanto ugunsmūra programmatūru (ko arī var iegūt bez maksas). Vairākās aptaujās konstatēts, ka cilvēki neaizsargā savu datoru nevis dēļ nezināšanas vai finansiālu apstākļu dēļ, bet faktiski tikai dēļ slinkuma.

Šajā publikācijā gan nav mērķis sniegt plašas rekomendācijas drošības aspektos, jo šī publikācija pamatā veidota kā juridisko un metodisko jautājumu analīze. Turklāt praktiskas rekomendācijas šajā jomā ir atrodamas daudzos avotos internetā u.c. Tāpēc te nosaukti tikai atsevišķi ieteikumi, kas ir attiecināmi uz šīs publikācijas sagatavošanas situāciju – 2010.gadu.

Elektroniskiem finanšu darījumiem var apsvērt tos vai citus no šādiem ieteikumiem:

1. Ievērot maksimālu piesardzību attiecībā uz kredītkartēm ar iebūvētu RFID[112] tehnoloģiju, kas gan padara maksājumus ērtākus, tomēr arī dod iespēju no neliela attāluma slēpti nolasīt tajā iekļautos datus.[113]
2. Vēlams neuzglabāt lielas naudas summas tajā bankas kontā, kuram piesaistīta maksājuma karte, ja ar to veic darījumus internetā, bet gan ieskaitīt attiecīgajā kontā tikai noteiktam paredzētajam maksājumam nepieciešamo summu brīdi pirms konkrētā finanšu darījuma.
3. Vēlams lietot tikai tādas bankas pakalpojumus, kura nodrošina divpakāpju autentifikāciju piekļuvei bankas kontam (piemēram, bez lietotājvārda un paroles piekļuvei, katram darījumam vēl arī jāievada kods no kodu kartes vai kodu kalkulatora, vai tml.).
4. Maksājuma kartei, ko lieto pirkumiem internetā, izmantot starptautisko papildus autentificēšanas sistēmu (*Verified by VISA* vai *MasterCard Secure code*).
5. Vēlams neveikt jebkādas darbības internetā ar maksājuma karti no datora, kurā startēta [ikdienā lietotā] *Windows* operētājsistēma, bet tā vietā datoru startēt no LiveCD[114] ar *Linux* OS – tādā veidā nodrošinot, ka arī inficēta datora gadījumā nav tomēr draudi, ka kaut kāda kaitīga programma varētu pārtvert finanšu norēķiniem lietoto informāciju – jo kaitīgās programmas, pat ja ir inficējušas datoru, vispār nedarbojas, ja dators tiek startēts ar tādu operētājsistēmu no

[112] Radio Frequency Identification. OECD Policy Guidance. A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives. Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy. OECD Ministerial Meeting on the Future of the internet Economy, Seoul, Korea, 17-18 June 2008. – http://www.oecd.org/dataoecd/19/42/40892347.pdf

[113] http://www.wreg.com/news/wreg-electronic-pickpocketing-story,0,5636726,full.story

[114] http://www.livecdlist.com/

LiveCD (piemēram, *Ubuntu* OS).

6. Pēc iespējas izvairīties veikt jebkādus finanšu darījumus, īpaši jau ievadīt maksājuma kartes informāciju tādos datoros, kuriem ir citu personu piekļuve, piemēram, interneta kafejnīcās, viesnīcās u.tml. kā arī ar bezvadu tīklu, t.sk. *WiFi* starpniecību (ja vien tas nav privāts, uzticami un droši konfigurēts, lietojot protokolu *IEEE 802.11i*). Novērst iespēju pie sava datora piekļūt nepiederošām personām.
7. Īpaši pievērst uzmanību pārnēsājamām USB atmiņas ierīcēm, ja tā tiek pieslēgta pie kāda cita datora (tajā skaitā inficēts var būt arī fotosalonā lietotais dators, kuram pieslēdz fotoaparāta atmiņas karti, lai izdrukātu fotoattēlus, vienlaikus bez personas ziņas inficējot arī šo atmiņas karti, no kuras vīruss vēlāk caur kabeli var nonākt personālajā datorā).
8. Tāpat pievērst vērību aizsardzībai pret vīrusiem, veicot maksājumus ar mobilo telefonu, kurā lieto 'mobilo banku'. Pievērst uzmanību, lai šāds mobilais telefons pat uz neilgu laiku nenonāk citu personu rīcībā, kā arī gan mobilajā telefonā, gan arī datorā neinstalēt programmas ar neskaidru izcelsmi vai pirātiskas programmas.
9. Datora un mobilā telefona lietošanā nepaļauties tikai uz antivīrus programmu, īpaši ja tā nav lietpratīga speciālista rūpīgi nokonfigurēta.
10. Pievērst uzmanību, vai finanšu norēķinu laikā tiek lietots drošs datu pārraides kanāls,[115] vismaz novērtējot to, vai attiecīgās interneta vietnes apmeklēšanas laikā pārlūkprogrammas apakšējā rīkjoslā ir parādījusies atslēgas ikona.
11. Saglabāt [piemēram, izdrukātā formā] priekš sevis visu informāciju par veiktajiem pirkumiem un izdarītajiem maksājumiem internetā, lai varētu kontrolēt, vai ar maksājuma karti vēlāk nenotiek kaut kādi citu personu veikti darījumi. Pastāvīgi sekot līdzi savas bankas pārskatiem par veiktajiem darījumiem ar kontu.
12. Finanšu darījuma laikā aizvērt visas pārējās cilnes interneta pārlūkprogrammā, bet pēc darījuma pilnībā izdzēst interneta pārlūkprogrammas saglabātos datus un aizvērt šo programmu. Pēc norēķiniem nepieciešamās informācijas pārsūtīšanas un saņemtā darījuma apstiprinājuma saglabāšanas (gadījumam, ja nāksies apliecināt konkrēto maksājumu vai pārbaudīt visu maksājumu vēsturi) nekavējoties neatjaunojami izdzēst darījuma gaitā pārsūtīto informāciju no tīklam pieslēgtā datora, t.sk. no failiem, ko veido pārlūkprogrammā uz laiku – *Temporary internet files; Cache* un no 'atkritumu kastes'. Nekad neuzglabāt maksājuma kartes datus datorā, īpaši jau nešifrētu pierakstu formā.
13. Piekļuvei web vietnēs, kur izmanto elektronisko finanšu norēķinu sistēmas, nelietot tādas pašas paroles, kādas lieto sociālajos tīklos vai citiem resursiem, turklāt paroles veidot kā diezgan garu,

[115] Interneta URL adreses sākumā prefiksa http:// vietā tad jābūt https://, kas nozīmē, ka elektroniskai datu pārraidei [vismaz uz konkrēto adresi] tiek lietots šifrēta kanāla protokols *SSL – Secure Socket Layer* vai *TLS – Transport Layer Security.* Vēl gan jānovērtē arī tam lietotā drošības sertifikāta autentiskums. Tomēr jāapzinās, ka šis aspekts pats par sevi nav pietiekams drošības garantēšanai, jo to iespējams ļaunprātīgi apiet.

tomēr personīgi viegli iegaumējamu (lai nevajadzētu pierakstīt) frāzi, tajā iekļaujot arī lielos burtus, ciparus un speciālās zīmes.

14. Piesardzīgi attiekties pret vilinošiem ātrā kredīta, tiešsaites loterijas u.tml. piedāvājumiem, kuriem var pieteikties ar mobilo telefonu. Tāpat arī nedot citām nepazīstamām personām savu mobilo telefonu kaut kādu pakalpojumu pieteikšanai, jo tā var būt krāpnieciski pieteikts kredīts, kuru nāksies atmaksāt, kamēr naudu saņem krāpnieks, kurš norādījis savu bankas konta numuru.
15. Pirms ieplānotā darījuma pārbaudīt arī atsauksmes par to interneta firmu, kas piedāvā interesi izraisījušo tiešsaites maksas pakalpojumu vai preci, vai kas izsaka vēlmi veikt piedāvāto pirkumu. Apdomīgi apsvērt konkrētā piedāvājuma īstenošanas loģiku, kā arī visu pieejamo informāciju par piedāvātāju, lai novērtētu, vai tajā neizpaužas kaut kādas maldināšanas pazīmes (jāņem vērā, mūsdienās dažādas Nigērijas krāpšanas shēmas[116] pielieto arī no citām valstīm). Nekad nepirkt internetā tādus pakalpojumus, kas nāk no acīmredzami apšaubāmiem avotiem, piemēram, pornogrāfiju.
16. Rūpīgi iepazīties ar visu pārdevēja / pakalpojuma sniedzēja sniegto informāciju par to, kā tiks pārsūtītas, uzglabātas un izmantotas klienta sniegtās ziņas. Uzmanīgi izlasīt visus pakalpojuma vai preces piegādes, lietošanas un apmaiņas noteikumus; pievērst uzmanību slēptajām izmaksām, kas var parādīties preču komplektācijas, piegādes vai lietošanas laikā; pievērst uzmanību garantijas un darījuma atsaukšanas nosacījumiem, t.sk. kā tas var būt īstenots no otras puses. Salīdzināt apzināto informāciju par šo interneta firmu ar citu šajā jomā darbojošos firmu sniegto informāciju. Nesteigties ar darījuma noslēgšanu.
17. Nekavējoties vērsties savā bankā ar lūgumu bloķēt maksājumu karti (īpaši, ja kredītkartei ir piešķirts kredītlimits), ja tā ir pazudusi, ja noticis acīmredzami citas personas darījums, piemēram, no citas valsts vai tamlīdzīgi. Šim nolūkam vienmēr vajag zināt, uz kādu telefona numuru zvanīt, lai noskaidrotu savas bankas kontaktinformāciju kartes bloķēšanai.
18. Nekad nesniegt sava bankas konta un savus datus, un / vai maksājuma kartes informāciju, ja saņemts tāds informācijas lūgums / pieprasījums ar e-pastu vai kādā interneta lapā izvietotā veidlapā (kas var būt arī vizuāli identiska ar pazīstamu lapu, jo uz to lietotājs var būt maldinoši pāradresēts ar DNS *spoofing* metodi *phishing* vai *pharming*). Neviena banka vai cita legāla institūcija nepieprasa šādu informāciju tamlīdzīgā veidā, tāpēc tā vienmēr ir datorkrāpšana.
19. Vēlams izvairīties no situācijām, kad maksājuma karte zūd no redzesloka, kad oficiante vai bārmenis to paņem, lai veiktu maksājumu ar POS termināli. Ja tā tomēr notiek, tad saglabāt kartes izdruku un čeku vēlākai darījuma informācijas pārbaudei.
20. Novērst iespēju veikala rindā blakusesošai personai [ar mobilo telefonu] nofotografēt rokās atrodošās maksājumu kartes abas puses – informācija uz kartes tiek lietota, kad veic pirkumus ar

[116] http://en.wikipedia.org/wiki/Advance-fee_fraud

karti internetā). Nedot citām personām savu maksājuma karti un neatstāt to bez uzraudzības arī šķietami drošos apstākļos.

21. Nu un, protams, izvairīties no tā, ka cita persona var redzēt ievadīšanas laikā pie bankomāta (vai citādi uzzināt) PIN kodu autentifikācijai maksājuma terminālī vai bankomātā, kā arī katru reizi pievērst uzmanību, vai bankomātam nav pievienotas kaut kādas aizdomīgas ārējas ierīces,[117] utt.

Lietderīgi arī patstāvīgi iepazīties ar šiem jautājumiem, piemēram, banku un viedkaršu ražotāju publiskotajiem padomiem.[118]

Tomēr jānorāda, ka pilnīga drošība šajā aspektā var būt vienīgi tad, ja vispār netiek lietoti elektroniski norēķini internetā, bet tas mūsdienās tiek uzskatīts par pārmērību un faktiski jau skar sociālpsiholoģisku aspektu, tāpēc iziet ārpus šī temata.

Kā paskaidrojošu piemēru piesardzības nepieciešamībai var norādīt vienu no pēdējā laikā izplatītajām datorkrāpšanas *pharming* metodēm: izmantojot nepietiekamu IS drošības līmeni interneta pakalpojumu sniedzēja DNS serverim, *datorkrāpnieks* ar speciālām uzlaušanas metodēm (*TCP Hijacking*)[119] var patvaļīgi piekļūt tajā uzglabātiem *domēna* vārdu ierakstiem (tie ir svarīgi, jo pēc DNS ierakstiem lietotāji atrod interneta adreses – tādas kā e-komercijas portāla adresi). Ja *datorkrāpniekam* tas izdevies, tad DNS serverī *datorkrāpnieks* var izmainīt noteikta *domēna* vārdam piesaistīto IP adresi. Līdz ar to e-komercijas portāla lietotāji izmainīto DNS ierakstu dēļ tiek pāradresēti uz *datorkrāpnieka* kontrolēto datoru, kur viņš izveidojis atbilstīgās lapas vizuāli identisku kopiju, ar to maldinot lietotājus par to, kādā interneta vietnē viņi atrodas. Atsevišķos gadījumos šādus pieslēgumus *datorkrāpnieks* var nodrošināt arī ar šifrētu datu pārraides protokolu, izmantojot viltotu drošības sertifikātu. Lai papildus maldinātu lietotājus, *datorkrāpnieks* var nodrošināt visas lietotāja sūtītās informācijas faktisku pārsūtīšanu uz īsto web vietni. Vienīgā informācija, kuru *datorkrāpnieks* nepārsūta uz īsto bankas mājaslapu, ir informācija par pieprasījumu iziet no tās. Līdz ar to *datorkrāpnieks* galarezultātā ir ieguvis visu informāciju, kuru lietotāji pārsūta, lai pārvaldītu savu kontu e-komercijas portālā (līdzīgi arī bankas vai citā portālā). Pēc tam, kad lietotājs ir beidzis darboties ar savu kontu, *datorkrāpniekam* paliek iespējas pārvaldīt šo lietotāja kontu, piemēram, veikt pirkumus ar viņa datiem, ja tam nav prasīta papildus autentifikācija.

Citas datorkrāpšanas metodes saistītas ar vēstuļu nosūtīšanu ļoti daudziem lietotājiem, kuras veic iepriekš minētā veida maldinošu pāradresāciju, vai ar kaut kādas mājaslapas kodā iekļautiem *skriptiem,* kas izsauc *uznirstošos logus* ar maldinošu pāradresāciju. Šajā nolūkā *datorkrāpnieki* izplata arī interneta *tārpus,* kas uz lietotāju datoriem slēpti instalē kaitīgu programmatūru (*Trojas zirgu)* ar aprakstītajām funkcijām.

---

[117] Tomēr jāņem vērā, ka bankomātam var būt pievienoti tādi *skimeri*, kas nemaz nav vizuāli pamanāmi.
[118] http://www.smartcardbasics.com/smart-card-security.html
[119] http://www.microsoft.com/technet/technetmag/issues/2005/01/SessionHijacking/default.aspx

Dažādas datorkrāpšanas metodes aizvien turpina attīstīties. Īpaši šādi riski būs aktuāli, ja nākotnē tiks savienotas personas autentifikācijas, dažādu pakalpojumu autorizācijas (tādas kā sabiedriskā transporta lietošana, mikrokreditēšana veikalos, veselības aprūpes pakalpojumu saņemšana u.tml.) un finanšu norēķinu tehnoloģijas, piemēram, vienā viedkartē, jo, kā likums, jaunu tehnoloģiju pieejamība visos uzņēmumos un valstīs nenotiek vienlaikus, tāpēc līdztekus drošākiem pakalpojumiem pastāv arī mazāk droši, par ko gan lietotāji var nebūt pietiekami informēti.

Normatīvo aktu un literatūras saraksts

1. Eiropas Parlamenta un Padomes direktīva COM(2010) 517. Par uzbrukumiem informācijas sistēmām, un ar ko atceļ Padomes Pamatlēmumu 2005/222/TI. / Pieņemta Briselē, 4.10.2010.
2. Elektronisko sakaru likums. / Pieņemts Saeimā 28.10.2004., stājās spēkā 1.12.2004., ar grozījumiem uz 1.01.2011. Latvijas Vēstnesis Nr. 183, 17.11.2004.
3. Fizisko personu datu aizsardzības likums. / Pieņemts Saeimā 23.03.2000., spēkā ar 20.04.2000., ar grozījumiem uz 2.06.2010. Latvijas Vēstnesis Nr.123/124, 6.04.2000.
4. Informācijas tehnoloģiju drošības likums. / Pieņemts Saeimā 28.10.2010., stājās spēkā 1.02.2011. Latvijas Vēstnesis Nr. 178, 10.11.2010.
5. Likums „Par valsts noslēpumu". / Pieņemts Saeimā 17.10.1996., stājās spēkā 1.01.1997., ar grozījumiem uz 13.01.2010; Latvijas Vēstnesis Nr.181, 29.06.1996.
6. Valsts informācijas sistēmu likums. / Pieņemts Saeimā 2.05.2002., stājās spēkā 5.06.2002., ar grozījumiem uz 1.01.2011. Latvijas Vēstnesis Nr.76, 22.05.2002.
7. Informācijas sistēmu drošības noteikumi. / Ministru kabineta noteikumi Nr.106. Pieņemti 21.03.2000., stājās spēkā 1.07.2000., zaudēja spēku 1.11.2002. Latvijas Vēstnesis Nr.109/110, 24.03.2000.
8. Kārtība, kādā aizsargājama informācija dienesta vajadzībām. / Ministru kabineta noteikumi Nr.280. Pieņemti 26.04.2005., stājās spēkā 30.04.2005., ar grozījumiem uz 5.11.2005. Latvijas Vēstnesis Nr.68, 29.04.2005.
9. Kritisku valsts informācijas sistēmu un valsts informācijas sistēmu savietotāju aizsardzības prasības. / Ministru kabineta noteikumi Nr.1445. Pieņemti 15.12.2009., stājās spēkā 01.01.2010. Latvijas Vēstnesis Nr. 200, 21.12.2009.
10. Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības. / Ministru kabineta Noteikumi Nr.40. Pieņemti 30.01.2001., stājās spēkā 3.02.2001., ar grozījumiem uz 1.09.2007. Latvijas Vēstnesis Nr. 19, 2.02.2001.
11. Valsts informācijas sistēmu vispārējās drošības prasības. / Ministru kabineta noteikumi Nr.765. Pieņemti 11.10.2005., stājās spēkā 15.10.2005., ar grozījumiem uz 4.02.2011. Latvijas Vēstnesis Nr.164, 14.10.2005.
12. Valsts informācijas sistēmu vispārējās tehniskās prasības. / Ministru kabineta noteikumi Nr.764. Pieņemti 11.10.2005., stājās spēkā 15.10.2005., ar grozījumiem uz 3.06.2009. Latvijas Vēstnesis Nr.164, 14.10.2005.
13. Valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu institūciju klasificētās informācijas aizsardzības noteikumi. / Ministru kabineta noteikumi Nr.21. Pieņemti 6.01.2004., stājās spēkā 4.02.2004., ar grozījumiem uz 1.10.2008. Latvijas Vēstnesis Nr.17, 3.02.2004.
14. Valsts pārvaldes funkciju izpildi apdraudošu kiberuzbrukumu noteikšanas instrukcija. / Ministru kabineta instrukcija Nr.20. Pieņemta 22.12.2009., stājās spēkā 29.12.2009., zaudēja spēku 4.02.2011. Latvijas

Vēstnesis Nr. 203, 28.12.2009.

15. Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi. / Finanšu un kapitāla tirgus komisijas normatīvie noteikumi Nr.278. Pieņemti 8.10.2010.; stājās spēkā 01.01.2011. Latvijas Vēstnesis Nr.162, 13.10.2010.
16. Latvijas Republikas Nacionālās drošības koncepcija. – http://polsis.mk.gov.lv/LoadAtt/file55886.doc
17. ISO/IEC 17799 «Informācijas tehnoloģija: Prakses kodekss informācijas drošības pārvaldībai.»
18. ISO/IEC 15408 «Informācijas tehnoloģija. Drošības metodes. Kritēriji informācijas tehnoloģiju drošības novērtēšanai: Ievads un vispārējais modelis; Drošības funkcionālās prasības; Drošības garantēšanas prasības.» – [*Common Criteria for Information Technology Security Evaluation*]
19. ISO/IEC TR 13335 «Informācijas tehnoloģija. Vadlīnijas informācijas tehnoloģijas pārvaldīšanai: Informācijas tehnoloģiju drošības koncepcija un modeļi; Informācijas tehnoloģiju drošības pārvaldīšana un plānošana; Aizsardzības līdzekļu izvēle; Tīklu drošības pārvaldīšanas ieteikumi.»
20. Personas datu apstrādes sistēmu audita rokasgrāmata. – http://www.dvi.gov.lv/fpda/files/fpda_audita_rokasgramata.pdf
21. Charles C. Wood. Information Security Policies Made Easy. A Comprehension Set of Information Security Policies. (Version 9). – Baseline Software, 2002. – 730 p.
22. Control Objectives for Information and related Technology. – http://www.isaca.org/cobit.htm
23. Cyber Security Strategy / Cyber Security Strategy, Ministry of Defence, Estonia, Tallinn, 2008. – 36 p.
24. Governing the internet : Freedom and Regulation in the OSCE Region. Organization for Security and Co-operation in Europe. The Representative on Freedom of the Media, 2007. – http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf
25. International Cyber Incidents: Legal Consideration. / By Eniken Tikk, Kadri Kaska, Liis Vihul. Cooperative Cyber Defence Centre of Excellence. – Tallinn: www.ccdcoe.org, 2010. – 130 p.
26. OECD Guidelines for the Security of Information systems. Explanatory Memorandum to Accompany the Guidelines for the Security of Information Systems / Accepted 26 November, 1992.; Latest update 1 July, 1997. Replaced by the 2002 OECD Guidelines. – http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_119820_1_1_1,00.html
27. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. / Adopted as a Recommendation of the OECD Council at its 1037 Session on 25 July, 2002. – http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
28. Radio Frequency Identification. OECD Policy Guidance. A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives. Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy. OECD Ministerial Meeting on the Future of the internet Economy, Seoul, Korea, 17-18 June 2008. – http://www.oecd.org/dataoecd/19/42/40892347.pdf
29. The North Atlantic Treaty / Washington D.C., 4 April, 1949.

http://www.nato.int/cps/en/natolive/official_texts_17120.htm

30. The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. Organisation for Economic Co-operation and Development. Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy. DSTI/ICCP/REG(2005)1/FINAL. 16th December 2005. – http://www.oecd.org/dataoecd/16/27/35884541.pdf
31. Woody C, Clinton L. Common Sense Guide to Cyber Security for Small Business. / Recommended Actions for Informations Security. 1st ed. – Arlington, Virginia, U.S.: internet Security Alliance, 2004. – 37 p. – http://www.isalliance.org
32. World Intellectual Property Organization. Methods and device for increasing security during data transfer (WO/2007/035149). – http://www.wipo.int/pctdb/en/wo.jsp?IA=SE2006001044&DISPLAY=DESC

Summary

In the article «Information systems security» there are considered main juridical and methodical as well as some practical aspects of the security of information systems in international, governmental, business as well as individual area nowadays (according to situation in the autumn of 2010)..

Аннотация

В статье «Безопасность информационных систем» рассмотрены главные практические, методические и некоторые практические аспекты безопасности информационных систем на международном, правительственном, бизнес, а также индивидуальном уровне в наше время (учитывая ситуяцию осенъю 2010 года).