LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

ILZE MURĀNE

INFORMĀCIJAS DROŠĪBAS APZINĀŠANĀS SISTĒMA IKDIENAS DATORLIETOTĀJAM

Promocijas darbs
datorzinātņu doktora (Dr. sc. comp.) zinātniskā grāda iegūšanai

Nozare: datorzinātnes
Apakšnozare: datu apstrādes sistēmas un datortīkli

Zinātniskais vadītājs:
profesors, Dr. habil. sc. comp.
JURIS BORZOVS

R ī g a - 2015

ANOTĀCIJA

Promocijas darbs ir veltīts risinājuma izveidei, lai veicinātu informācijas drošības apzināšanos mājsaimniecībās, kur aizvien biežāk tiek izmantotas informācijas tehnoloģijas. Tā kā darba vide vairs nav pilnībā atdalīta no personīgās, darbā apskatīti informācijas drošības pārvaldības standarti un uzņēmējdarbības vides labā prakse, īpašu uzmanību pievēršot darbinieku informācijas drošības apzināšanās veicināšanai. Izstrādāta pieeja, kuras pamatā ir informācijas drošības pārvaldības modelis mājsaimniecībai, un kas ietver metodi un e-rīku informācijas drošības risku novērtēšanai mājsaimniecībā. Tā nodrošina iespēju ikdienas datorlietotājam apzināties un novērtēt riskus rīcībā ar elektronisko informāciju, kā arī saņemt padomu drošības uzlabošanai.

Atslēgas vārdi: informācijas drošība, apzināšanās, risku novērtēšana, kiberdrošība, ikdienas datorlietotājs

ABSTRACT

The thesis outlines a solution for raising households' information security awareness when they become more frequent users of information technologies. Since borders between the business and private environments have become blurred, the paper researches corporate information security management standards and best corporate practices by focussing on raising information security awareness of employees. An approach based on the information security management model for households is developed, including method and an e-tool for information security risk assessment. It provides the everyday computer user an opportunity to recognize and assess risks to electronic information handling, as well as receive advice on improving security.

Keywords: information security, awareness, risk evaluation, cybersecurity, everyday computer user

SATURS

TABULU SARAKSTS

ATTĒLU SARAKSTS

TERMINI UN SAĪSINĀJUMI

CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CSP	Centrālā statistikas pārvalde
DF	Datorikas fakultāte
DNS	Ģenētiskās informācijas glabātuve – dezoksiribonukleīnskābe
drošības vadīkla	angl. *security control* – rīks vai pasākums, lai novērstu vai mazinātu drošības riskus
ENISA	European Network and Information Security Agency; Eiropas Tīkla un informācijas drošības aģentūra
ES	Eiropas Savienība
IDRE	Informācijas drošības risku eksperts
ISACA	Information Systems Audit and Control Association – provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems
ISF	Information Security Forum – an independent, not-for-profit organisation that supplies authoritative opinion and guidance on all aspects of information security
ISO	International Organization for Standardization
IT	Informācijas tehnoloģijas
LU	Latvijas Universitāte
LZA TK	Latvijas Zinātņu akadēmijas Terminoloģijas komisija
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
RFID	radiofrekvenciālā identificēšana
ROSI	return-on-security-investment
SASHE	Security Aware Smart Household Employee
USB	universālā secīgā kopne, pieslēgvieta dažādām ierīcēm
WiFi	bezvadu datortīkls

IEVADS

Informācijas tehnoloģijas aizvien vairāk ienāk katra cilvēka dzīvē, ikdienā, mājās. Šo tehnoloģiju progress šobrīd ir straujāks nekā jebkad agrāk. Tīmekļa pārlūkošanas iespējas radušās tikai apmēram pirms 20 gadiem, bet pašlaik gandrīz katru gadu internetā rodas jauns rīks, kas kļūst populārs visā pasaulē. Seminārā *Workshop on the Economics of Information Security* [WEIS09] izskanēja apgalvojums, ka šobrīd mazie un vidējie uzņēmumi ieguvuši iespēju izmantot tehnoloģijas, kas pirms 10 gadiem bija pieejamas tikai lielām korporācijām. Tehnoloģiju izmantošana aizvien pieaug. Pēc Centrālās statistikas pārvaldes apsekojuma datiem 2014. gadā Latvijā internetu izmantoja vairāk nekā 95% no uzņēmumiem ar mazāk nekā 50 darbiniekiem un vairāk nekā 71% iedzīvotāju, bet 2009. gadā attiecīgi – 84% un 60% [CSP1]. Nereti mājās tiek izmantotas ātrākas un daudzveidīgākas ierīces nekā birojos.

Attīstoties tehnoloģiju izmantošanai, attīstās arī dažādi apdraudējumi. Laikā, kad nozīmīgi informācijas tehnoloģiju resursi bija pieejami tikai lieliem uzņēmumiem, saskaroties ar apdraudējumiem, attīstība notika arī aizsargāšanās pusē jeb informācijas drošības pārvaldībā [OECD02, NIST, ISF]. Tomēr viens no svarīgākajiem aspektiem ir domāšanas jeb uztveres maiņa. Ir pētījumi, kā to vajadzētu veikt uzņēmējdarbības vidē, piemēram, apmācot pirmā līmeņa vadītājus, rādīt drošas uzvedības paraugu un veicināt atbilstošu informācijas drošības kultūru [JOH07].

Arī ikdienas dzīvē ārpus darba vides informācijas drošības kultūras attīstība ir nepieciešama. Ikdienas datorlietotāji saskaras ar iemīļotu fotogrāfiju kolekcijas zaudējumu, jo nav zinājuši, ka datora cietais disks var sabojāties, kā arī nav dzirdējuši par nepieciešamību veidot rezerves kopijas. Cilvēki neapzinās, ka reiz internetā publiskota informācija vairs nav padarāma privāta, un tā var tikt dažādi, t.sk. nepatīkami, izmantota.

Otrs aspekts, kas nereti apgrūtina risinājuma atrašanu atbilstošai informācijas drošības pārvaldībai, ir grūtības saprasties tehnoloģiju speciālistiem un tehnoloģiju lietotājiem. Tehnoloģiju speciālistiem ir zināšanas, tiek apkopoti un publicēti padomi, bet tie rakstīti, izmantojot specifisku profesionālo valodu.

Trešais aspekts saistīts ar nepieciešamību informācijas drošību pārvaldīt nepārtraukti. Pat tad, ja datora pārdevējs ir datoru aprīkojis ar vislabākajiem aizsardzības rīkiem, datora lietotājs nevar paļauties, ka praktiskajā lietošanā tas būs drošs arī turpmāk.

Pirmkārt, katras atsevišķas ierīces pārdevējs nezina, ar kādām citām ierīcēm un kādā veidā tā tiks savienota. Otrkārt, jauni apdraudējumi rodas gandrīz katru dienu, tāpēc jāseko līdzi atbilstošu aizsardzības rīku attīstībai. Treškārt, tikai katrs informācijas īpašnieks un tehnoloģiju ierīces lietotājs pats zina, cik svarīga viņam ir konkrētā informācija un līdz ar to – cik daudz resursu tās aizsardzībai viņš ir gatavs tērēt.

Tēmas aktualitāte un novitāte

Aizvien vairāk cilvēku dažādu informāciju meklē internetā ar mērķi kaut ko iemācīties. Latvijā 2010. gadā to darīja vismaz trešā daļa iedzīvotāju (38.7%), kas ir vairāk nekā puse (58.4%) no tiem, kas lieto internetu. Savukārt, 2008. gadā šie skaitļi bija tikai 13.4% un 22.1% [CSP1]. Atsevišķi tehnoloģiju uzņēmumi nodrošina padomus savu produktu lietotājiem. Ir pieejamas grāmatas ar daudzveidīgu padomu apkopojumiem. Bet šie materiāli ir jāsaprot un jāpielieto katram pašam, un tas ir sarežģīts uzdevums tehnoloģijas ne pārāk labi pārzinošam lietotājam.

Pēdējos 10 gadus aizvien vairāk tiek runāts par informācijas sabiedrības veidošanos [ISAP06, ISAP14], taču ir jāpalīdz sabiedrībai orientēties arī šīs vides apdraudējumos un drošā lietošanā. Dažas valstis ir izstrādājušas plānus, kā uzlabot drošību tehnoloģiju vidē, t.sk. izglītojot patērētājus [AUS10, SE09]. Latvijas Republikas Saeima 2011. gada 10. martā apstiprināja Nacionālās drošības koncepciju, kurā noteikti valsts apdraudējuma novēršanas stratēģiskie pamatprincipi, prioritātes un pasākumi nākamajiem četriem gadiem. Pirmo reizi koncepcijā iekļauti arī informācijas tehnoloģiju drošības jautājumus, t. sk. noteikta nepieciešamība izglītot lietotājus [NDK11]. Konkrēti pasākumi šī uzdevuma veikšanai tiek plānoti, dažu īstenošana jau ir uzsākta. Savukārt 2014. gada 21. janvārī Latvijas Republikas Ministru kabinets apstiprināja Latvijas kiberdrošības stratēģiju 2014.–2018. gadam, kas cita starpā ietver rīcības virzienus sabiedrības izglītošanai informācijas tehnoloģiju drošības jomā [KDS14].

Promocijas darbs ir veltīts risinājuma meklējumiem, lai palīdzētu nodrošināt katram ikdienas datorlietotājam iespējas pašam pārvaldīt savas informācijas drošību elektroniskajā vidē.

[HOW12] autori atzīst, ka mājas jeb ikdienas datorlietotāja jēdzienam nav vispāratzītas definīcijas, jo to ir apgrūtinoši noteikt. Pieaugušais mājās datoru var lietot vienkāršām vajadzībām, piemēram, ziņu lasīšanai vai darbībām internetbankā, bet mājās datoru var izmantot arī bērni un jaunieši, kas savu ikdienu bez tā nevar iedomāties. Darba

autore piekrīt šiem novērojumiem. Ikdienas datorlietotājs šī darba ietvaros tiek definēts kā persona, kas savā ikdienā, privātām vajadzībām izmanto datoru vai planšetdatoru un interneta iespējas, bet, kuriem nav formālas izglītības vai ilgstošas pieredzes IT vai līdzīgā jomā. Ikdienas datorlietotājs pats ir pilnībā atbildīgs par izmantojamo datoru vai planšetdatoru un rīcību ar to.

Datorlietotāju apskata kā vājāko posmu informācijas drošības procesā [GLI10, KAP10]. [HOW12] autori pēta tieši mājas datorlietotāju drošības paradumus un secina, ka tad, ja lietotājs apzinās apdraudējumu iespējamību, viņš vairāk rūpējas par drošības jautājumiem.

Informācijas drošības pārvaldībai uzņēmumā pieejami standarti, apkopota labā prakse, kā arī iespējams izmantot speciālistu palīdzību. Katram ikdienas datorlietotājam savs konsultants ne vienmēr ir pieejams.

Promocijas darba mērķis un uzdevumi

Pētījuma priekšmets ir ikdienas datorlietotāja elektroniskās informācijas aizsardzība personīgajā datorā[1] un izmantojot internetu. Darba rezultātu mērķauditorija ir ikdienas datorlietotāji un mājsaimniecības, kas vēlas sistemātiski pārvaldīt elektroniskās informācijas drošību.

Promocijas darba galvenais mērķis ir izstrādāt pieeju, kā veicināt informācijas drošības apzināšanos privātā vidē[2], informācijas drošības risku novērtēšanas metodi un sistēmas prototipu (rīku), kas palīdz uzņemties atbildību un īstenot drošības pārvaldību, sniedzot praktiskus padomus, kas pielāgoti konkrēta ikdienas datorlietotāja vajadzībām.

Promocijas darbam izvirzīti šādi **uzdevumi**:

- analizēt pētījumus par saistītām tēmām;
- izpētīt uzņēmējdarbības vides pieredzi informācijas drošības pārvaldībā un informācijas drošības apzināšanās veicināšanā;
- izpētīt informācijas drošības standartus;
- balstoties uz uzņēmējdarbības vidē populāru standartu, izveidot formalizētu modeli informācijas drošības pārvaldībai uzņēmumā;

[1] Datora jēdziens iekļauj galddatoru, klēpjdatoru, planšetdatoru, viedtālruni.

[2] Promocijas darba ietvaros jēdziens 'privāta vide' aptver mājsaimniecību un ikdienas datorlietotāja privāto telpu.

- izveidot formalizētu modeli un vadlīnijas informācijas drošības pārvaldībai mājsaimniecībā;
- izmantojot statistikas datus par tehnoloģiju pielietošanu, izpētīt ikdienas datorlietotāju vajadzības;
- apzināt informācijas tehnoloģiju apdraudējumus, kas ir būtiski privātā vidē;
- izstrādāt metodi informācijas drošības risku pārvaldībai mājsaimniecībā;
- aprobēt metodi, izstrādājot praktiski izmantojamu sistēmas prototipu (rīku).

Psiholoģiskie cilvēka rīcības aspekti nav iekļauti šī darba tvērumā.

Pētījumā izvirzītās tēzes

Promocijas darba ietvaros ir izvirzītas šādas pamata tēzes:

Ir nepieciešams un, balstoties uz uzņēmējdarbības vides pieredzi, ir izveidojams risinājums, lai pilnveidotu informācijas drošības pārvaldības procesu mājsaimniecībā;

Ikdienas datorlietotāja informācijas drošības apzināšanos iespējams uzlabot, izmantojot informācijas risku novērtēšanas metodi, kas realizēta kā praktiski izmantojama tīmekļa lietojumprogramma.

Izmantotās metodes

Darbā pielietotas gan teorētiskas analīzes, gan praktiskas pielietojuma metodes.

Teorētiskie pētījumi balstīti uz literatūras avotu konceptuālu analīzi, apkopošanu, sistematizēšanu, lai novērtētu iespējas izmantot ikdienas datorlietotāja vajadzībām uzņēmējdarbības vidē uzkrāto informācijas drošības pārvaldības pieredzi.

Darbā izmantota modelēšana – izstrādāti formalizēti modeļi, kas tiek aprakstīti ar UML diagrammu palīdzību.

Izstrādāta informācijas drošības novērtēšanas metode ikdienas datorlietotājam, tā aprobēta kā tīmekļa lietojumprogramma (rīks IDRE).

Rīka IDRE novērtēšanai izmantotas aptaujas metodes. Ikdienas datorlietotāju aptauja veikta ar anketēšanas paņēmienu, aptaujā piedalījās 65 respondenti. Papildu anketēšanai izmantotas intervijas ar ekspertiem.

Galvenie rezultāti

Darba galvenais rezultāts ir jauna pieeja ikdienas datorlietotāja elektroniskās informācijas drošības apzināšanās veicināšanai un pārvaldībai, kas sastāv no

- informācijas drošības pārvaldības formalizēta modeļa un vadlīnijām mājsaimniecībai, ko var izmantot drošības apzināšanās pasākumu plānošanai un izpratnes veicināšanai,
- informācijas drošības risku novērtēšanas metodes, kas aprobēta kā tīmekļa lietojumprogrammas prototips (rīks), ar ko katrs ikdienas datorlietotājs var novērtēt riskus savas elektroniskās informācijas drošībai un saņemt drošības pilnveidošanas ieteikumus.

Darbam ir gan teorētiska, gan praktiska nozīme. Darba novitāte ir risku novērtēšanas metodes pielietošana ikdienas datorlietotāja informācijas drošības pārvaldībai.

Promocijas darba saturs parāda, ka formulētie uzdevumi izpildīti un izvirzītais darba mērķis ir sasniegts.

Rezultātu aprobācija

Promocijas darba atziņas un secinājumi publicēti piecos zinātniskos rakstos [IM08, IM09, IM10, IM11a, IM11b]. Publikācija "Raising awareness in information security: Everyone should participate" [IM08] indeksēta datubāzē *Scopus*, publikācija "Information security management method for households " [IM11a] – datubāzēs *Scopus* un *Web of Science*. Rezultāti referēti piecās starptautiskās zinātniskās konferencēs:

- The 2008 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2008 International Conference on Security and Management, Lasvegas, USA, July 14-17, 2008
- The 2009 World Congress in Computer Science, Computer Engineering, and Applied Computing, The 2009 International Conference on Security and Management, Lasvegas, USA, July 13-16, 2009
- The 9th International Baltic Conference on Databases and Information Systems (Baltic DB&IS'2010), Riga, Latvia, July 5-7, 2010
- The 1st Security Conference – Europe, Örebro, Sweden, August 15-17, 2010
- The 2011 European Security Conference, Örebro, Sweden, June 13-14, 2011

Pētāmā problēma apskatīta arī referātā "G.Bārzdiņš, I.Murāne Jauno tehnoloģiju ēnas puses" Latvijas Universitātes 65. konferences plenārsēdē "Drošība – neatkarības garants", 02.02.2007., referāts publicēts [BAR07].

Vairākas darba atziņas autore izklāstījusi referātos Latvijas Universitātes zinātnisko konferenču informācijas tehnoloģiju sekcijā:

- "Informācijas sistēmas lietotājs - drošības ķēdes vājais posms? ", 66. konference, 2008., Rīga, Latvija
- "Informācijas drošības procesa elementi", 67. konference, 2009., Rīga, Latvija
- "Informācijas drošības politika mājsaimniecībai", 68. konference, 2010., Rīga, Latvija

Pieredzes papildināšanai autore ir uzstājusies ar referātiem vairākās konferencēs, kur pārsvarā pulcējas nozares praktiķi, t.sk.:

- From IT Security to Business Continuity, Information Security Forum Annual Congress, Washington DC, 12.11.2006
- Reviewing Information Security Standards that can Help Improve Protection, Electronic Crime Prevention Tactics, Geneva 09.11.2007
- Who is responsible for information security awareness education (children and grown-ups)?, workshop: Security − Internet and Information Systems, Baltic IT&T 2008 Forum, Riga, 09.04.2008
- Information Security Awareness Raising – CIO responsibility?, CIO Session: Information Systems Security, Baltic IT&T 2010 Forum, Riga, 21.04.2010
- Optimising information security awareness, IT Governance for Central Banks, Cambridge, 09.09.2010
- Beyond the firewall: information security awareness, IT Governance for Central Banks, Cambridge, 22.09.2011
- Mani dati – kā tos pasargāt?, diskusija ES mājā, Rīga, 28.01.2014.
- 2nd ENISA National Cyber Security Strategies workshop, Riga, 13.05.2015.

- Workshop "Building Trust and Confidence Online", Digital Assembly 2015, June 18, 2015, Riga

Darba vispārīgs raksturojums

Promocijas darba pamatā ir autores vairāk nekā piecpadsmit gadu pieredze datorlietotāju izglītošanā informācijas drošībā. Pieredze uzkrāta, gan trīspadsmit gadus nodrošinot konkrēta uzņēmuma darbinieku izglītošanu, gan konsultējot citu uzņēmumu un valsts iestāžu darbiniekus. Uzņēmuma darbinieki tiek izglītoti gan par aizsardzību pret vispārējiem apdraudējumiem, gan par uzņēmumam specifiskiem informācijas drošības jautājumiem.

Darbs izstrādāts Latvijas Universitātes Datorikas fakultātē (LU DF) kā darba autores patstāvīgi veikts pētījums. Atsevišķu praktisku uzdevumu veikšanā piedalījās minētās fakultātes studenti. Par promocijas darba tematiku LU DF izstrādāti vairāki kursa darbi un trīs bakalaura darbi (M. Kaļķis, 2006., A. Pavlova, 2009., Z. Purene, 2010.). Vairākus gadus autore vada Informācijas sistēmu drošības studiju kursu LU DF, kā arī ir piedalījusies skolēnu izglītošanā dažādu projektu ietvaros. Promocijas darba izstrādes laikā ir arī sagatavoti materiāli un veikta praktiska lietotāju izglītošana dažādos semināros.

Promocijas darbs izklāstīts 164 lapaspusēs. Darbs satur 25 attēlus, 16 tabulas, ievadu, četras pamata nodaļas, nobeigumu, literatūras avotu sarakstu un sešus pielikumus.

Darba pirmajā nodaļā aprakstīts informācijas tehnoloģiju pielietojums privātā vidē, apdraudējumi informācijas drošībai un pētāmā problēma. Tajā analizēti informācijas drošības jēdziena dažādi skaidrojumi un informācijas privātuma jēdziens, kā arī šī darba tvērumam aprakstīti jēdzieni ikdienas datorlietotājs un mājsaimniecība. Nodaļā sniegts ieskats informācijas drošības pārvaldībā un saistītos pētījumos un aprakstīta uzņēmējdarbības labā prakse informācijas drošības pārvaldībā.

Informācijas drošības pārvaldības populārākie modeļi ir informācijas drošības standarti, kas apskatīti darba otrajā nodaļā. Balstoties uz vienu no šiem standartiem, izveidots informācijas drošības pārvaldības konceptuāls modelis uzņēmumam. Veicot analīzi, modelis transformēts, izveidojot informācijas drošības pārvaldības konceptuālu modeli mājsaimniecībai. Izveidotas mājsaimniecības informācijas drošības pārvaldības vadlīnijas.

Informācijas drošības apzināšanās ir promocijas darba vadošā tēma, un šī informācijas drošības pārvaldības aspekta elementi aprakstīti darba trešajā nodaļā.

Analizēti dažādu autoru pētījumi šajā jomā, kā arī pētīta informācijas drošības apzināšanās labā prakse gan pasaulē, gan Latvijā. Otrajā nodaļā aprakstītais mājsaimniecības informācijas drošības pārvaldības modelis un vadlīnijas un ceturtajā nodaļā aprakstītā risku novērtēšanas metode un rīks izmantojami ikdienas datorlietotāja drošības apzināšanās veicināšanai.

Darba ceturtā nodaļa veltīta informācijas drošības risku novērtēšanas metodei un promocijas darba praktiskajam rezultātam – informācijas drošības risku novērtēšanas sistēmas prototipam. Nodaļā apskatītas autores vadībā studentu veiktas izpētes par internetā pieejamiem informatīviem un apmācību risinājumiem aizsardzībai pret apdraudējumiem. Risku novērtēšanas metode ietver informācijas sagatavošanas daļu, kur būtiska loma ir nozares ekspertiem, kā arī praktiskās pielietošanas daļu, ko izmanto ikdienas datorlietotājs. Metodes praktiskajā pielietošanā ir vairāki soļi, t.sk. elektroniskās vides apzināšana, risku identificēšana un novērtēšana, padomu sniegšana drošības vadīklu (*security control*) izvēlē. Metode aprobēta, izmantojot tīmekļa lietojumprogrammas prototipu – rīku IDRE (Informācijas Drošības Risku Eksperts). To pozitīvi novērtējuši gan tās lietotāji, gan dažādu jomu eksperti.

Pateicības

Liels paldies katram un visiem, kas sniedza atbalstu un palīdzēja promocijas darba tapšanā!

ESF
EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA

LATVIJAS UNIVERSITĀTE
ANNO 1919

IEGULDĪJUMS TAVĀ NĀKOTNĒ

Promocijas darbs izstrādāts ar Eiropas Sociālā fonda atbalstu projektā "Atbalsts doktora studijām Latvijas Universitātē".

1. INFORMĀCIJAS DROŠĪBAS PĀRVALDĪBA MĀJSAIMNIECĪBĀ

1.1. Nodaļas mērķi

Nodaļā aprakstīta pētāmā problēma, izpētot statistikas datus par informācijas tehnoloģiju pielietojumu privātā vidē un apdraudējumus informācijas drošībai. Apskatīti informācijas drošības un informācijas privātuma jēdzieni. Šī darba tvērumam aprakstīti jēdzieni ikdienas datorlietotājs un mājsaimniecība. Aprakstīti labās prakses piemēri uzņēmējdarbības vides pieredzē informācijas drošības pārvaldībā un informācijas drošības apzināšanās veicināšanā, kā arī pētījumi par informācijas drošības pārvaldību mājsaimniecībās.

1.2. Informācijas drošība un privātums

Informācijas drošība

Informācijas drošības jēdziens ir pazīstams jau sen. Konkrētākas aprises tas ieguva līdz ar rakstības apgūšanu. Lai pasargātu informāciju no svešām acīm, rakstītu informāciju šifrē, dokumentus glabā seifos. Attīstoties informācijas apstrādei un glabāšanai datorizētā vidē, arī drošības aspekts mainās un paplašinās. Dažādos avotos tiek minēta datoru drošība, datu drošība, informācijas sistēmu drošība, informācijas tehnoloģiju drošība, informācijas drošība [NISTTerm, ISO27002, Term]. Jēdzieni 'informācijas sistēmu drošība' un 'informācijas drošība' nereti tiek lietoti, lai aprakstītu vienu un to pašu. Jēdziens parasti iekļauj vārdu 'sistēma' situācijās, kad tiek runāts par tehnoloģijām.

Informācijas sistēmu drošības visbiežāk lietotā definīcija balstīta uz trim pamatjēdzieniem informācijas konfidencialitāte, integritāte un pieejamība: "Informācijas un informācijas sistēmas aizsardzība no neatļautas piekļuves, lietošanas, izpaušanas, sabojāšanas, izmaiņām vai sagraušanas ar mērķi nodrošināt konfidencialitāti, integritāti un pieejamību." [NISTTerm, ISO27002]. Nereti tiek izmantota abreviatūra CIA, kas veidota no minēto jēdzienu nosaukumu pirmajiem burtiem angļu valodā (*confidentiality*, *integrity*, *availability*).

Viens no bieži lietotiem avotiem - Standartu un tehnoloģiju institūts pat vienā materiālā [NISTCS] ar vienu nozīmi lieto gan jēdzienu 'datoru drošība', gan 'informācijas tehnoloģiju drošība', gan drošība kā sistēmas īpašība: "Informācijas tehnoloģiju drošība ir sistēmas īpašība". Savukārt informācijas tehnoloģiju drošības mērķis ir sekmēt

organizācijas spēju sasniegt darbības mērķus, izmantojot sistēmas un ņemot vērā informācijas tehnoloģiju riskus. Šo mērķi var sasniegt, nodrošinot konfidencialitāti, integritāti, pieejamību, uzskaitāmību un pārliecību (*assurance*).

Konfidencialitāte ir sistēmas īpašība, kas nodrošina piekļuvi informācijai tikai pilnvarotiem lietotājiem. Konfidencialitātes aizsardzība attiecas gan uz datu glabāšanu, gan apstrādi, gan pārsūtīšanu. Integritāte ietver gan datu integritāti jeb īpašību, kas nodrošina, ka dati netiek bez pilnvarojuma grozīti, gan sistēmas integritāti jeb īpašību, ka sistēmas veiktās darbības ir ar paredzamu rezultātu. Pieejamība ir sistēmas īpašība, kas nodrošina piekļuvi pilnvarotiem lietotājiem katrā laikā, kad tas nepieciešams, un aizsargā no neatļautas datu izdzēšanas. Atkarībā no informācijas sistēmas darbības mērķiem minētajām trim īpašībām var būt dažāda svarīguma pakāpe.

Uzskaitāmība (*accountability*) ir prasība nodrošināt pierakstu saglabāšanu par sistēmā veiktajām darbībām.

Pārliecība ir apliecinājums, ka sistēmai vajadzīgajā apjomā piemīt visas iepriekš minētās četras īpašības. Pārliecība ir svarīgs elements, tā jāskata kā nepārtraukts process.

Standarts "Informācijas tehnoloģija. Drošības metodika. Prakses kodekss informācijas drošības pārvaldībai" [ISO27002] min tādas papildus īpašības, kā autentiskums (*authenticity*), uzskaitāmība (*accountability*), nenoliegšana (*non-repudiation*) un uzticamība (*reliability*), kas var tikt apskatītas informācijas drošības ietvaros.

Vairāki informācijas drošības analītiķi uzskata, ka ar klasisko triādi CIA (konfidencialitāte, integritāte, pieejamība) nav pietiekami [BOS02, Chapter 5]. Ir nepieciešams jauns ietvars, kas plašāk apraksta, kā informācijas īpašniekam labāk pasargāt to no dažādiem ienaidniekiem. Lielākā daļa līdzšinējo datorsistēmu drošības skatījumu fokusējas uz datoriem un datortīkliem, t.i. elementiem, ko tehnoloģiju speciālisti pazīst labāk. Bet dzīvē primārais izaicinājums drošībai ir cilvēka rīcība, kas neprasmīgi vai neatbilstoši rīkojas ar informāciju, ne vienmēr informācija tiek apstrādāta ar datoru vai pārsūtīta tīklā. Datoru drošības rokasgrāmatas [BOS02] autori ierosina apskatīt ietvaru, kurā ir seši drošības pamatelementi – pieejamība, derīgums (*utility*), integritāte, pareizība (*authenticity*), konfidencialitāte un valdījums (*possesion*). Ietvarā tiek uzskaitīti minēto pamatelementu drošības zaudēšanas veidi un avoti, aizsardzības rīki un paņēmieni, kā arī informācijas drošības mērķi. Minētie mērķi ir izvairīšanās no pienākuma nepildīšanas, sakārtota un aizsargāta sabiedrība, likumu un noteikumu ievērošana, ētiska uzvedība, sekmīga tirdzniecība, privātums. Šis ietvars ir balstīts uz mērķi sasniegt īpašnieku

vajadzības pasargāt vēlamos informācijas drošības elementus no tīšas un nejaušas lietošanas, kas var radīt zaudējumus. Šo uzdevumu risina, pielietojot aizsardzības rīkus un metodes, kas izvēlēti, balstoties uz standartiem un konkrētām vajadzībām. Lai pamatotu visu sešu elementu nepieciešamību, tiek izmantoti iespējamo zaudējumu scenāriji, kur katrs apdraud tieši vienu informācijas drošības elementu. Ja svītrotu kādu no sešiem elementiem, būtu jāatzīst, ka tam piekārtotais scenārijs nav iespējams, bet aprakstītie scenāriji balstīti uz reāliem notikumiem.

Pieejamības apdraudējumam atbilstošais scenārijs apraksta izbrāķēta programmētāja apzinātas sabotāžas rīcību, nomainot svarīgu failu nosaukumus, ko līdz ar to sistēma vairs nemāk atrast.

Derīgums (*utility*) var tikt ietekmēts, ja informācija tiek nošifrēta, bet šifrēšanas atslēga nejauši izdzēsta. Klasiskajā CIA modelī šādu situāciju apskatītu kā pieejamības zaudējumu, bet šeit tiek skaidrots, ka informācija ir pieejama, tikai nelietojamā formātā. Konfidencialitāte ir būtiski uzlabota, citi elementi nav ietekmēti.

Programmatūras izplatītājs iegādājās programmu no mazpazīstama izstrādātāja, izdzēsa tā vārdu no datu nesēja, tādējādi izjaucot sākotnējās informācijas integritāti, jo nebija norādīts izstrādātājs. Tālāk izplatot un lietojot šo produktu, pārējie drošības elementi netika ietekmēti. Pieķeršanas gadījumā tiktu piemērota atbildība saskaņā ar autortiesību aizsardzības likumdošanu. Līdzīgā scenārijā, ja izplatītājs nevis dzēstu, bet aizstātu izstrādātāja vārdu ar populārāku vārdu, tiktu ietekmēts autentiskums (*authenticity*). Abi minētie scenāriji apraksta no tehnoloģiskā viedokļa ļoti līdzīgas situācijas. Atšķirības ir juridiskās un finansiālās niansēs.

Ļaundaris ar tehniskiem palīglīdzekļiem aprīkoja bankomātu, lai iegūtu tā lietotāju PIN kodus, tādējādi ietekmējot konfidencialitāti. Konfidencialitāte bieži var tikt ietekmēta, tikai noskatoties informāciju.

Sestajā scenārijā aprakstīta zādzība, kurā zaglis aiznes serveri ar pamatdatiem un rezerves kopijas, lai vēlāk pieprasītu izpirkšanas maksu par to atdošanu, tādējādi ietekmējot valdījuma (*possesion*) elementu. CIA modelī šis būtu pieejamības zaudējuma scenārijs, bet autors norāda, ka pieejamība tomēr nav ietekmēta, jo par samaksu datus var atgūt nesabojātus. Turklāt zaglim nav mērķa datus analizēt un līdz ar to ietekmēt konfidencialitāti.

Kopumā ietvars ir interesants, tas piedāvā uz informācijas drošību skatīties plašāk nekā tikai tehnoloģiskā līmenī. Tomēr trīs papildus drošības elementus var uzskatīt arī kā

klasiskā CIA modeļa elementu atvasinājumus. Arī pats [BOS02] piedāvā elementus apvienot pa pāriem, kur katrā pārī ir kāds no klasiskā CIA.

[BOS02] ietvars piedāvā paplašināt arī klasisko drošības funkciju klāstu. Triju funkciju – profilakse (*prevention*), atklāšana (*detection*) un atjaunošana (*recovery*) – vietā apskatītas tiek septiņas drošības funkcijas. Tāda detalizācija sniedz skaidrību atsevišķos aspektos, tomēr praktiskajā pielietošanā rada grūtības, tā vietā, lai veiktu funkciju, vispirms jāveic ne visai lietderīga analīze, kura funkcija tā īsti ir. Tomēr viena no piedāvātajām funkcijām - Spēju attīstīšana (*education*) - klasiskajā modelī tiek apskatīta sadrumstaloti un mūsdienās nepietiekamā apjomā. Šīs funkcijas uzdevums ir nodrošināt, ka visi iesaistītie mācās no pieredzes, gan attīstot savas zināšanas informācijas drošībā, gan nododot šīs zināšanas citiem.

Latvijas Zinātņu akadēmijas Terminoloģijas komisijas (LZA TK) apstiprinātā informācijas drošības definīcija arī iekļauj vārdu 'sistēmas': "Informācijas sistēmas aizsargātība pret neatļautu piekļuvi informācijai un tās maiņu gan glabātuvē, gan apstrādes vai pārraides procesā, kā arī izsargāšanās no pakalpojumu sniegšanas nepilnvarotiem lietotājiem un tās nenodrošināšanas pilnvarotiem lietotājiem." [Term]. Turpat atrodama arī vecāka informācijas sistēmas drošības definīcija, kas pēc būtības neatšķiras: "Informācijas sistēmas aizsardzība pret nepilnvarotu piekļuvi informācijai un tās modificēšanu atmiņā, apstrādes vai pārsūtīšanas procesā. Šajā nodrošinājumā ietverti līdzekļi draudu atklāšanai, dokumentēšanai un novēršanai.".

Viens no iemesliem jēdzienu daudzveidībai ir vārda 'sistēma' dažādās nozīmes. Šis jēdziens var tikt lietots, gan apzīmējot ļoti šaurus tehnoloģiskus elementus, gan papildus iekļaujot tajā lietojumprogrammas, kā arī pat lietotājus un pārvaldības procesus [AND04, 11. lpp]. Ņemot vērā gan straujo izplatību, gan dažādo ar datora vārdu apzīmēto vai saistīto ierīču klāstu, gan šo ierīču lietotāju dažādās zināšanas un pieredzi, jēga, ko katrs saprot ar jēdzienu 'informācijas drošība', ir atšķirīga.

Visas definīcijas pamatā vērstas uz uzņēmumu informācijas drošību. Privātu informāciju kā definētu vērtību neiekļauj neviena no populārām definīcijām. Tomēr visas definīcijas tādā vai citādā veidā iekļauj mērķi, piemēram, "informācijas drošība ir stāvoklis" vai "informācijas riski ir atbilstoši pārvaldīti" un apdraudējumus vai sargājamos elementus, piemēram, "novēršot nepilnvarotu piekļuvi" vai "jāsargā konfidencialitāte".

Vairākās jomās, t.sk. valsts pārvaldē izmanto arī jēdzienu 'kiberdrošība', ko definē kā "instrumentu, politikas, drošības konceptu un vadlīniju, risku vadības, rīcības,

apmācības, pieredzes un tehnoloģiju kopums, kuru var izmantot elektroniskās vides, tās organizācijas un lietotāju aktīvu aizsardzībai" [KDS14]. Kiberdrošības jēdzienam ir gan līdzības ar informācijas drošību, gan jaunas iezīmes saistībā ar pārmaiņām elektroniskajā vidē [KIL14].

Informācijas privātums

Informācijas apstrāde elektroniskā vidē nenoliedzami ietekmē indivīdu privāto dzīvi. Ikdienā norēķinoties ar maksājumu karti, lietotājs vispirms sajūt ērtības. Iespēja nenēsāt lielu skaidras naudas daudzumu sniedz arī papildus drošību. Arī iespēja datorā (internetbankā) pārlūkot veiktos maksājumus vispirms tiek uzlūkota kā ērtība. Bet informāciju par veiktajiem pirkumiem var izmantot arī indivīda paradumu un interešu analīzei. Privātumu cilvēki uztver ļoti dažādi, turklāt atšķiras vērtējums par privātumu apdraudošām tehnoloģijām atkarībā no to izmantošanas mērķa. Pētījumā [WES10] iegūti secinājumi, ka 92% aptaujāto pilnībā akceptē videonovērošanu, gandrīz 90% neuztrauc radiofrekvenciālās identificēšanas (RFID) tehnoloģija, ja tā tiek izmantota autobusa biļetē, bet attieksme pret ģenētiskās informācijas dezoksiribonukleīnskābes (DNS) datu reģistriem atkarīga no mērķa (cilvēki parasti uzskata, ka par noziedzniekiem šādus datus jāuzkrāj). Interesanti, ka jaunieši ir noraidošāki pret šīm tehnoloģijām. Autore piedalījās konferencē, kur šo pētījumu prezentēja, un diskusijā tika izvirzīta hipotēze, ka tas ir tāpēc, ka jaunie labāk saprot tehnoloģiju riskus. Arī [PIR08] apskata atšķirības drošības un privātuma uztverei fiziskajā pasaulē un datoru vidē.

Lai mazinātu iespējamību, ka maksājumu dati tiek izmantoti ļaunos nolūkos, bankām un citām institūcijām, kas tos uzkrāj un apstrādā savu uzdevumu veikšanai, jāievēro dažādi noteikumi par datu aizsardzību. Šāda veida noteikumu kopuma piemērošanas mērķis ir privātuma un personas datu aizsardzība.

Privātuma jēdziens sākotnēji lielā mērā bija saistīts ar cilvēktiesībām. Izpratne par cilvēktiesībām dažādās valstīs un reģionos atšķiras, ir izstrādāti dažādi dokumenti, kas jomu apraksta [SMI05]. No datorzinātnes skatupunkta privātuma tēma plaši aplūkota [JAC04, JAC08], analizējot riskus, kas apdraud privātumu internetā.

LZA TK privātumu definē kā "fiziskas personas vai organizācijas tiesības kontrolēt vai noteikt, kādu informāciju par to drīkst uzkrāt un saglabāt un kam šo informāciju ir atļauts izmantot" [Term].

Latvijā fizisko personu datu aizsardzību regulē Fizisko personu datu aizsardzības likums [FPDAL], kura mērķis ir aizsargāt fizisko personu pamattiesības un brīvības, it īpaši privātās dzīves neaizskaramību, attiecībā uz fiziskās personas datu apstrādi. [FPDAL] definēts personas datu jēdziens, un noteikti pienākumi katram, kas veic personas datu apstrādi. Mājsaimniecībām prasības nav stingri noteiktas, tomēr ir ierobežojumi attiecībā uz šādu datu izpaušanu trešajām personām [FPDAL, 3. panta 3. daļa]. Tomēr katra paša interesēs ir arī privātā vidē apzināties, kā vajadzētu sargāt savu privāto informāciju, un, kā – citu personu informāciju. Bez saskaņošanas ar attēlos redzamajām personām, piemēram, nedrīkstētu sociālajos tīklos publicēt mājas ballītēs tapušas bildes. Ne vienmēr personas dati, kas tādi ir saskaņā ar [FPDAL], tiek uztverti kā sargājama privāta informācija. Populārākais piemērs Latvijā ir personas kods, kas ir personas dati pēc likuma, bet plašās izmantojamības dēļ tikai retais šo informāciju uzskata par privātu. Par šo jautājumu nereti diskutē arī tiesību zinātņu eksperti un jomas speciālisti [PK].

Kamēr datora lietotājs nav saskāries ar drošības problēmām elektroniskajā vidē, tikmēr lietošanas ērtums ir svarīgākā īpašība. Un piesardzība tiek aizmirsta. Pat tik lielā mērā, ka esot pārliecinātam par vispasaules tīmekļa anonimitāti, *YouTube* tiek publicēti paša publicētāja noziedzīgu nodarījumu videoieraksti. Šo informāciju policija nekavējas izmantot. Savukārt, sociālajos tīklos, piemēram, *Facebook* publicēto informāciju aizvien vairāk izmanto darba devēji. Jaunā māmiņa, kas lepojas ar savu pirmdzimto un publicē viņa dzīves gājumu no dzimšanas brīža, neaizdomājas, ka šī rīcība var ietekmēt jaunā cilvēka tālāko dzīvi. Tehnoloģijas nepārzinošam cilvēkam ir grūti aptvert, ka internetā publicētu informāciju vairs nevar padarīt par nebijušu. Kaut kur tās kopijas saglabāsies, un nav zināms, kas un kad to izmantos.

Jauniešiem un bērniem kā aktīvākajiem tiešsaistes resursu lietotājiem arī biežāk jāsaskaras ar apdraudējumiem. Sociālie tīkli ir "īsā laika periodā radījuši nozīmīgu kulturālu rezonansi amerikāņu pusaudžu vidū" [BOY07]. Izglītošana šajā sabiedrības daļā ir ļoti nozīmīga, būtu labi, ja lietotāji apzinātos potenciālās sekas viņu pašu publicētās informācijas izmantošanai [BRY09].

Līdzīgi kā 100% drošība, arī 100% privātums nav iespējams. Lai izmantotu informācijas tehnoloģiju sniegtās ērtības, daļa privātuma ir jāziedo. Tomēr katram privātas informācijas elementam ir atšķirīga ietekme, ja tas tiek nepareizi izmantots. Turklāt informācijas nozīme mainās laikā, piemēram, bērna vienu reizi internetā publicēta ziņa "šobrīd pieaugušie nav mājās" kopā ar citu informāciju var radīt apdraudējumu, bet jau pēc

laika, kad situācija būs mainījusies, minētajam privātās informācijas fragmentam būs daudz mazāka nozīme.

Informācijas privātumu jeb vērtību pašai personai nav vienkārši novērtēt. Viens no mēģinājumiem ir izmantot ekonomikas teorijas par vērtību izmaiņām laikā. [BER09] secināts, ka personas datiem pašiem par sevi ir tikai aptuveni nosakāma informatīvā nozīme (apdraudējums privātumam). Vērtība rodas, šos datus izmantojot gan labiem, gan arī sliktiem mērķiem. Turklāt laikam ejot, privātuma vērtība personas datiem var gan pieaugt, gan – samazināties. Arī privātumu, tāpat kā drošību, ir jāpārvalda nepārtraukti. Jo vairāk zināšanu tiek uzkrāts, jo labāk apbruņoti ir ikdienas datorlietotāji, un piemērotāku rīcību izvēlas [JAC08, 260. lpp].

1.3. Problēmas nostādne

1.3.1. Informācijas tehnoloģiju pielietojums

Datorus un datortīklus aizvien vairāk izmanto gan uzņēmējdarbībā, gan mājsaimniecībās. Nereti ikdienā lietotas ierīces, piemēram, mobilie telefoni, fotokameras utml. pēc savas skaitļošanas jaudas un iespējām pārsniedz ierasto vecākas paaudzes personālo datoru iespējas.

21. gadsimta pirmajā dekādē informācijas drošība ir viens no tematiem, bez kā apspriešanas neiztiek ne uzņēmumi, ne valsts pārvalde [BJO05, KRU08, MEE09, ISF, ENISAAR, SInt, NetS, AUS10]. Lieliem uzņēmumiem un daļai valstu ir pieejami gan naudas līdzekļi, gan atbilstoši izglītoti speciālisti, lai pieņemamā līmenī pārvaldītu ar jaunajām tehnoloģijām saistītos riskus, apzinātu sargājamos resursus un izveidotu aizsardzības risinājumus. Taču jaunās tehnoloģijas ienāk arī katra cilvēka dzīvē un mājās, bet pieredze elektroniskas informācijas pārvaldībā ir tikai retajam [SZE09, YOU09, TAL10].

Daudzi ikdienas datorlietotāji lieto tīmekļa programmas rēķinu apmaksai, turklāt nereti tās ir atšķirīgas dažādiem pakalpojumu sniedzējiem. Dažādi e-veselības projekti vedina domāt, ka nav tālu laiks, līdz cilvēkiem būs iespēja tiešsaistē sekot līdzi saviem medicīnas dokumentiem. Apsardzes sistēmas uzkrāj datus par tās lietošanas paradumiem, daļa mājokļu jau izmanto elektroniskas atslēgas. Informācijas tehnoloģijas mājsaimniecībā vairs neaprobežojas ar galddatoru vai piezīmjdatoru.

Tuvākajās desmitgadēs minēto un līdzīgu sistēmu skaits pieaugs aizvien ātrāk. Bet nepieciešamās pārvaldības prasmes nav pietiekami izplatītas. Sistēmu izstrādātājiem ir jāņem vērā drošības prasības un jāveido pēc iespējas labāki un drošāki risinājumi [AND04]. Tomēr katram posmam drošības pārvaldībā ir jāpilnveidojas, un nedrīkst atpalikt arī datorlietotāju prasmju attīstība.

Informācijas tehnoloģijas, kas gūst popularitāti iedzīvotāju vidū, attīstās nepārtraukti. Meklēšanas rīks *Google* izveidots pirms nedaudz vairāk nekā 10 gadiem [GMst]. Kopš 2003. gada darbojas un aizvien populārāks kļūst *Skype*, kas dod iespēju miljoniem cilvēku sazināties savā starpā gan ar rakstītu tekstu, gan balss sarunāt, gan videoattēliem. Portāls *Facebook*, kura mērķis ir dot iespēju cilvēkiem apmainīties ar privātu informāciju, dzimis 2004. gadā. 2006./2007. gadā darbību uzsāka *Twitter*, kas ir reālā laika īsu ziņu apmaiņas serviss. Šobrīd gan radio, gan televīzijas skatītāji tiek aicināti izteikt viedokļus tieši *Twitter*.

Protams, tehnoloģijas dod priekšrocības. Publicēt informāciju kļuvis tik vienkārši, ka ir iespējas radoši izpausties katram, kas to vēlas. Interneta iespējas novērtē arī vecmāmiņas, kas sazinās ar ārzemēs studējošiem mazbērniem, un mazi bērni, kas vispirms iemācās rakstīt ar datoru.

Uzņēmumos apdraudējumus saistībā ar datora izmantošanu nereti palīdz pārvaldīt atbilstoši speciālisti. Bet datoru izmantošana mājās notiek biežāk nekā darba vietā vairāk nekā pusei interneta lietotāju, turklāt datoru lietošana mājās aizvien pieaug, 2013. gadā jau vairāk nekā 90% no personām, kas lietojušas internetu pēdējo 3 mēnešu laikā, to darījušas mājās (1. tabula, [CSP1]).

1. tabula Iedzīvotāju interneta izmantošanas vietas gada sākumā

	Mājās	Darbavietā	Izglītības iestādē	Citur
2008	81.8	36.9	17.1	30.1
2010	85.3	31.0	14.9	40.0
2011	89.2	36.3	15.1	37.8
2013	92.7	34.4	11.6	28.8

Latvijā šobrīd mājsaimniecībām ir pieejamas pašas modernākās tehnoloģijas. Daudzdzīvokļu mājās Rīgā un vēl vairākās pilsētās Latvijā katram dzīvoklim ir iespējams izmantot interneta pieslēgumu ar ātrumu, kas šobrīd ikdienas lietotājam ir daudz vairāk,

nekā viņš spēj izmantot. Platjoslas interneta pieslēgums ir 85.9% no mājsaimniecībām ar interneta pieslēgumu (2. tabula, [CSP1]).

2. tabula Interneta pieslēgumu veidi mājsaimniecībās 2014. gada sākumā

Platjoslas interneta pieslēgums	
% no mājsaimniecību kopskaita	**% no mājsaimniecībām ar interneta pieslēgumu**
63.1	85.9

2014. gadā jau 71.8% Latvijas iedzīvotāju lieto internetu regulāri (vismaz reizi nedēļā), un no tiem 92.7% internets ir pieejams mājās [CSP1]. Datora un it īpaši interneta lietošana daudzās Latvijas mājsaimniecībās pamazām kļūst par neatņemamu dzīves sastāvdaļu – ar to palīdzību notiek norēķinu veikšana, preču iegāde, informācijas meklēšana un nu jau ar interneta starpniecību cilvēki veic arī sev tik nepieciešamo socializēšanos. Papildus jāņem vērā arī cilvēciskas vājības un tieksme pēc jaunām "rotaļlietām", kas nereti nozīmē, ka mājās ir jaunāki un jaudīgāki datori nekā uzņēmumā, kam jārēķina ekonomiskais izdevīgums.

Savukārt, ja mājsaimniecībā ir bērni, internetu lieto vairāk nekā 90% aptaujāto (% no mājsaimniecību kopskaita attiecīgajā grupā) (3. tabula, [CSP1]).

3. tabula Interneta pieejamība dažāda tipa mājsaimniecībās gada sākumā

	2014
	Internets
Kopā visās mājsaimniecībās	**73.4**
1 pieaugušais ar bērniem	93.9
2 pieaugušie ar bērniem	94.6
3 un vairāk pieaugušie ar bērniem	**94.2**

2014. gadā iedzīvotāji visvairāk internetu izmanto e-pasta sūtīšanai (84.3% no interneta lietotājiem jeb 63.9% no visiem iedzīvotājiem) un informācijas iegūšanai (vairāk nekā 70% no interneta lietotājiem) (4. tabula, [CSP1]). Nozīmīga daļa interneta lietotāju (69.5%) izmanto to, lai darbotos sociālajos tīklos. Desmit gadu laikā no 2004. līdz 2014. gadam vairāk nekā piecas reizes pieaudzis to iedzīvotāju skaits, kas izmanto internetbankas iespējas. Paša izveidota satura augšupielādēšana par statistiski nozīmīgu darbību kļuvusi beidzamo gadu laikā.

4. tabula Iedzīvotāju interneta izmantošanas mērķi gada sākumā (%)

	2004		2008		2014	
	No iedzīvotāju kopskaita	No interneta lietotājiem	No iedzīvotāju kopskaita	No interneta lietotājiem	No iedzīvotāju kopskaita	No interneta lietotājiem
E-pasta nosūtīšana vai saņemšana	**24.6**	74.2	49.5	81.6	**63.9**	84.3
Telefona sarunas, izmantojot internetu vai video zvani …	**2.9**	8.7	24.3	40.1	**43.2**	57.0
Ziņojumu izvietošana 'čatošanas' lapās, blogos, …	**13.4**	40.6	30.5	50.3	**…**	…
Informācijas meklēšana par precēm un pakalpojumiem	18.8	56.9	48.6	80.1	52.6	69.4
Radio klausīšanās vai televīzijas skatīšanās internetā	9.5	28.6	23.6	38.9	19.6	25.9
Spēļu, attēlu, filmu vai mūzikas spēlēšana vai lejuplāde	15.5	46.9	...	...	39.1	51.5
Iesaistīšanās sociālajos tīklos	...	...	…	…	52.7	69.5
Interneta banka	**11.7**	35.4	38.6	63.7	**56.8**	**74.9**
Sadarbība ar valsts un sabiedriskajām iestādēm	13.4	40.6	15.5	25.6	31.2	47.1
Informācijas meklēšana internetā, lai kaut ko iemācītos …	...	...	**13.4**	**22.1**	**38.7**	**58.4**
Pašizveidota satura … augšupielādēšana jebkurā tīmekļa vietnē	...	...	**19.3**	31.9	**28.9**	**38.1**

Daudz tiek lietotas arī digitālās foto un video kameras. Pašu veidotas fotogrāfijas un filmas tiek uzkrātas datorā. Attīstās mobilo telefonu iespējas glabāt datus aizvien lielākos apjomos. Mājas dators vai mobilais telefons ir kļuvis vienlaicīgi par ģimenes fotoalbumu un piekļuves rīku naudas uzkrājumiem.

1.3.2. Apdraudējumi informācijas drošībai

Uzņēmumu vajadzībām tiek apkopoti un publicēti dažādi apdraudējumu pārskati [CSR11, CSR13a, CSR13b, CSR13c, CSR15]. Aizvien vairāk lietotāju saņem brīdinājumu no sava interneta pakalpojuma sniedzēja vai arī viņiem tiem slēgta iespēja lietot internetu. Īpašniekam nezinot, viņa dators kļūst par mēstuļu izsūtīšanas avotu vai pakalpojuma atteikuma (DoS) uzbrukuma elementu. Interneta vidē nav atšķirības starp lielām un mazām valstīm. Lietotāji ir apdraudēti jebkur. Organizācija *Gartner* savā 2006. gada septembra informācijas tehnoloģiju konferencē iepazīstināja ar pieciem galvenajiem apdraudējumiem. Minēti tika mērķtiecīgi apdraudējumi, identitātes zādzība, spiegošanas programmatūra,

sociālā inženierija un, joprojām, vīrusi [Gar06]. Aģentūra *Federal Office for Information Security (BSI)*, kas veicina IT drošību Vācijā, ir publicējusi apdraudējumu katalogu, kas ietver 46 apdraudējumu uzskaitījumu un īsu aprakstu [ThrCat]. Daļa no katalogā minētajiem apdraudējumiem raksturoti veidā, kas tieši saistāms ar biznesa vidi, piemēram, rūpnieciskā spiegošana, vides aizsardzība, personāla vai citu resursu nepietiekamība. Daļa, piemēram, ugunsnelaime, iekārtu zādzība, var būt aktuāli arī privātā vidē, tomēr šajā vidē tos nav lietderīgi iekļaut informācijas drošības pārvaldības tvērumā. Aktuāli privātai videi ir šādi, tieši ar datora un interneta izmantošanu saistīti apdraudējumi:

- datu nesēju zudums vai zādzība;
- datorā esošas informācijas zaudēšana;
- jutīgas informācijas izpaušana;
- svarīgas informācijas integritātes zudums;
- personas datu neatļauta izmantošana;
- identitātes zādzība;
- datora aizmuguriska, neatļauta izmantošana;
- datora nepareiza darbība;
- programmatūras ievainojamība;
- interneta nepieejamība;
- ļaundabīga programmatūra;
- pakalpojumatteices uzbrukums;
- speciālista zināšanu vai pakalpojuma nepieejamība;
- sociālā inženierija.

Daudzveidīgi sociālās inženierijas rīki tiek lietoti ar mērķi izvilināt dažādu informāciju. Sociālā inženierija tiek dažādi definēta: viens no variantiem, ka tā ir māksla un māka likt cilvēkiem izpildīt jūsu vēlēšanās [SocE]. Šī "māksla" jau ir sena, tomēr tieši beidzamajā laikā daudz tiek pielietota informācijas tehnoloģiju jomā, tāpēc, ka nezinošu un nobijušos cilvēku nedrošā vidē ir vieglāk ietekmēt.

Patiešām globālu izplatību sasnieguši dažādi zombētu datoru tīkli. Nesenā pagātnē populārs ir uzbrukums *Storm Worm* [SW], kas izplatās ar datortārpu palīdzību. Tiek izmantotas sociālās inženierijas metodes, lietotājs saņem e-pasta vēstuli ar saiti uz kādu populāru interneta vietni, piemēram, *Youtube* vai *Facebook* ar vilinošu filmu vai attēlu. Mēģinot to skatīties, jau pēc viena peles klikšķa lietotāja nepilnīgi aizsargātais dators tiek

inficēts. Tā kā *Storm* tīkla robežas nav stingri noteiktas, tad dažādi statistiskie dati par tā izplatību atšķiras. Tomēr jebkuri skaitļi ir iespaidīgi. Miljardos skaitāmas e-pasta vēstules, kas satur vīrusu, desmitiem tūkstošu reāli inficētu datoru, kas tiek lietoti DoS uzbrukumos. Atsevišķi speciālisti izteikuši minējumus, ka kiberkarš Igaunijā ir lielā mērā veikts tieši no *Storm Worm* tīkla [StWorm]. Aizvien pieaugošais nevēlamā e-pasta apjoms lielā mērā ir rezultāts zombētu datoru tīklu izplatības pieaugumam. Kaut arī ir pilnīgi iespējams, ka lielu datortīklu turētāji pārdot tā jaudu nevēlamā e-pasta izplatītājiem, tomēr mēstuļu izplatītāji meklē lētākos variantus, tāpēc plaši izmanto tieši nezinošu vai neuzmanīgu lietotāju datorus.

Savukārt nozagtu datu patiesos apjomus aprēķināt ir gandrīz neiespējami. Vispirms jau tāds fakts ir jākonstatē, jo atšķirībā no fiziskas mantas informācijas zudums (nokopēšana) var nebūt pamanāms. Priekšstatu sniedz pētījums *The 2008 Data Breach Investigations Report* [Ver08], kura ietvaros tika analizēti vairāk, nekā 500 četru gadu laikā pēc dažādu uzņēmumu pasūtījuma izmeklēti gadījumi, kas saistīti ar informācijas nepilnvarotu izmantošanu. Pētījuma veicēji ir atzinuši, ka līdzīgu pētījumu par informācijas apdraudējumiem privātiem datoriem ir gandrīz neiespējami paveikt.

2010. gada janvāra sākumā uz daudzām stundām tika bloķēta piekļuve internetam desmitiem tūkstošu tā lietotāju [Vispa]. Cietušais interneta pakalpojuma sniedzējs Vispa izsekojis uzbrukuma ceļu, kas izrādījušies slepus svešiem "saimniekiem" pakļauti jeb "zombēti" Latvijas datori jeb botu tīkls. Patiesie uzbrucēji varēja būt no jebkuras pasaules malas, t.sk. cietušā kaimiņi. Botu tīkli rodas neaizsargātos vai slikti aizsargātos datoros, iesūtot tajos speciālas programmas, kas darbojas īstajam saimniekam nezinot. Lielākā daļa uzbrukumā izmantoto datoru īpašnieku droši vien nemaz nezina, ka viņu dators ticis izmantots uzbrukumā. Turklāt interneta piekļuves iespējas un kvalitāte Latvijā ir starp labākajām pasaulē [INT13], kas veicina interesi par mūsu ne pārāk labi aizsargātajiem datoriem.

Attīstās arī datoru un informācijas drošības joma. Pirms dažiem desmitiem gadu uzmanības centrā bija lieldatori ar galvenajiem uzsvariem uz tehniskiem drošības aspektiem pamatā saistībā ar pieejamību, ātrdarbību. Vēlāk aizvien nozīmīgāku lomu ieguva personālie datori, ko bieži apdraudēja dažādi vīrusi, kas izplatījās ar disketēm. Beidzamo 15 gadu laikā, interneta iespējām kļūstot plaši lietojamām, mainās arī drošības uzsvari. Vīrusi joprojām ir starp būtiskākajiem apdraudējumiem, bet apdraudējumu klāsts kļuvis daudz plašāks. Turklāt daudz plašāks kļuvis arī apdraudēto loks. Šobrīd datorizētas

informācijas drošības jautājumi ir kļuvuši svarīgi bezmaz katrā cilvēka dzīves aktivitātē. Rokasgrāmatas jomas pārvaldīšanai kļūst aizvien biezākas un aptver ļoti daudzveidīgu apdraudējumu un risinājumu loku, apskatot gan to attīstības vēsturi, gan uzbūvi un pielietošanu [BOS02].

Darāmā drošības līmeņa paaugstināšanā jāattīsta nepārtraukti. Ieviešot jebkuru aizsardzības mehānismu, nav nekādas garantijas, ka jau vistuvākajā laikā netiks izgudrots atkal jauns apdraudējuma paveids. Ar nepārtraukta darba režīmu 24/7/365 un globālu izplatību pat uz salīdzinoši neattīstītām teritorijām, gan ieguvumi, gan drošības apdraudējumi pieaugs aizvien ātrāk [BOS02].

Starp biežākajiem apdraudējumiem, kas būtiski privātā vidē, jāmin gan tehnoloģiski apdraudējumi, gan krāpnieciskas darbības, gan arī tieši likumpārkāpumi. Tehnoloģiskie apdraudējumi ietver, piemēram, vīrusus u.c. kaitīgus rīkus, mēstules, spiegprogrammatūru un arī datorspēles. Krāpnieciskie apdraudējumi ir nepatiesa informācija, mānīšanās, ķēdes vēstules, "kļūsti ātri bagāts" shēmas, tiešsaistes izsoles un tiešsaistes azartspēles. Likumpārkāpumi atkarībā no dažādu valstu likumdošanas var būt gan zagtas programmatūras, gan zagta mūzikas un filmu izmantošana, gan arī plaģiāts.

Reputācijas apdraudējumus internetā tradicionāli saista ar uzņēmuma reputāciju, tomēr arī ikdienas datorlietotāja reputācija var tikt apdraudēta. Šodien publicējot ne visai solīdas bildes no kādas ballītes, pēc gadiem tās var kalpot kā potenciālā darbinieka novērtēšanas kritērijs. Mājas datortīkla apdraudējumu loks ir plašāks nekā tikai tārpi, vīrusi vai trojas zirgi. Līdzās tehnoloģiskiem apdraudējumiem jāņem vērā arī sociālie un juridiskie apdraudējumi, kā arī datu glabāšanas apdraudējumi.

Labākie drošības risinājumu uzņēmumi regulāri piedāvā svaigāko apdraudējumu apskatus [TEx]. Informācijas drošības speciālistiem šī ir noderīga informācija (1. attēlā).

Threats

Severity	Name	Type	Protected*
	Trojan.Wensal	Trojan	02/10/2015
	Backdoor.Wensal	Trojan	02/10/2015
	Exp.CVE-2015-0310	Trojan	02/10/2015
	Trojan.Mangzamel	Trojan	02/09/2015
	Linux.Xorddos!gen1	Trojan	02/09/2015
	Trojan.Ransomlock!g83	Trojan	02/10/2015
	Backdoor.Korplug!gen8	Trojan	02/10/2015
	Infostealer.Steamfishi	Trojan	02/08/2015
	Trojan.Cryptlock.G!gm	Trojan	02/06/2015
	Trojan.Swifi!gen2	Trojan	02/07/2015
	Backdoor.Mivast	Trojan	02/07/2015

1. attēls Apdraudējumi (*Symantec*)

Galvenie tehnoloģiskie apdraudējumi ir saistīti ar mājas datora pieslēgumu internetam un lietotāju darbībām tajā. Iespējami, protams, ir arī aparatūras bojājumi. Internetā mājās datoru lietotāju galvenais tehnoloģiskais apdraudējums ir dažādu veidu ļaunprātīga programmatūra, kuras darbības sekas var būt gan vieglas, piemēram, apnicīgi reklāmas paziņojumi, gan arī ļoti nopietnas, piemēram, ar spiegprogrammatūras palīdzību nozagti interneta bankas dati. Šobrīd populārākie ir sekojoši ļaunprātīgas programmatūras veidi: datorvīrusi, datortārpi, trojas zirgi, reklāmprogrammatūra un spiegprogrammatūra [VW10].

SANS (*SysAdmin*, *Audit*, *Network*, *Security*) institūta publicēts kiberdrošības risku indekss kā svarīgāko apdraudējumu avotu norāda klienta programmatūru, kurā savlaicīgi nav novērstas programmatūras ievainojamības jeb uzstādīti ielāpi. Mērķēti uzbrukumi var tikt vērsti pret dažādām populārām lietojumprogrammām, piemēram, biroja programmatūra, e-pasta klientu programmatūra, multivides atskaņotāji un tūlītēja ziņojumapmaiņa. Protams, šie uzbrukumi ir iespējami tikai tad, ja dators ir pieslēgts internetam, bet tādu ir lielākā daļa [SANS].

Sociālie draudi internetā ir līdzīgi kā jebkur citur – uz ielas, veikalā, nepazīstamā vietā. Taču, lietojot internetu, cilvēkiem trūkst pieredzes. Biežāk sastopamie sociālie apdraudējumi internetā ir personas datu izvilināšana, kiberiebiedēšana un datorspēles un azartspēles. Katrs no šiem sociālajiem riskiem ir ar savu bīstamības pakāpi, taču visnopietnākie riski ir identitātes zādzība internetā, jo tā var radīt lielus finansiālus zaudējumus un juridiskus sarežģījumus, kā arī riski, kas skar bērnus un pusaudžus, piemēram, vardarbība [Re08]. Turklāt internets rada iespēju "satikt" sociāli nelabvēlīgas personas biežāk nekā citā vidē.

Juridiskie apdraudējumi mājās var būt saistīti ar autortiesību aizsardzības pārkāpumiem. Latvijas Republikas teritorijā autortiesības sargā Autortiesību likums, un primārais uzdevums ir aizsargāt autora darbu pret tā neatļautu lietošanu. Šajā kategorijā ietilpst arī datorprogrammu pirātisms.

Personas datus Latvijā sargā Fizisko personu datu aizsardzības likums [FPDAL], kas nosaka pienākumus organizācijām, kas apstrādā personas datus. Pašai personai ir tiesības ar saviem datiem rīkoties pēc saviem ieskatiem. Tomēr ikdienā nereti neaizdomājas, ka, piemēram, mājas ballītē fotografētas bildes var saturēt citu personu personas datus, pret ko būtu jāizturas saskaņā ar likumā noteikto.

Atbildību par vairākiem pārkāpumu veidiem saistībā ar datu apstrādes sistēmām Latvijā nosaka Krimināllikums. Sodāma ir patvaļīga piekļūšana automatizētai datu apstrādes sistēmai, tās darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju. Nepilnīgi aizsargāta datora, kas ticis izmantots uzbrukumā citām datorsistēmām, īpašnieku sargā izmeklētāju pieredzes trūkums, ne pārāk ātrā izmeklēšanas sadarbība starp valstīm utml. iemesli. Savākt juridiski saistošus pierādījumus interneta vidē pagaidām vēl ir ļoti dārgi. Tomēr tas nedrīkstētu būt par iemeslu bezatbildībai par katra internetam pieslēgta datora drošības pārvaldību.

Attiecībā uz failiem, kas tiek glabāti personīgajā datorā, izdalāmas divas datu apdraudējuma kategorijas. Pirmkārt, nesankcionēta pieeja, piemēram, personīgajos datoros var tikt glabāta bankas pieejas kodu informācija, kas ļauj autentificēties internetbankā, tātad šādu datu noplūšana var radīt nopietnus finansiālus zaudējumus, tāpat tie var būt arī dažādi, dziļi personīgi dati, kas satur sensitīvu informāciju. Sliktā ziņa šai apdraudējumu grupai ir tāda, ka nesankcionēta datu nokopēšana ir ļoti grūti konstatējama. Mājās, kur visbiežāk nav uzstādīta attiecīga kontroles programmatūra, datu nokopēšanu varēs konstatēt tikai tad, kad tie tiks izmantoti, t.i., jau nodarīts kaitējums datu īpašniekam.

Papildus riskus šāda tipa apdraudējumam rada personu aktīva darbošanās vienranga (*peer-to-peer*) tīklos. Daudzi cilvēki ir kļuvuši par identitātes zādzības upuriem, jo neuzmanīgi darbojušies vienranga tīklos. Papildus problēmu rada fakts, ka šādas zādzības vietu ir gandrīz nepiespējami precīzi noteikt. Tā kā droša šo tīklu lietošana gandrīz nav iespējama, jo tā mērķu sasniegšanai pēc būtības ir nepieciešams atvērt jebkuram tīkla dalībniekam piekļuvi savam datoram. Vienīgais risinājums, kas pasargā no apdraudējumiem vienranga tīklos, ir nelietot šos tīklus vispār [JOH08]. Tomēr daļai datoru lietotāju minēto padomu negribas ievērot, tāpēc ir svarīgi katram pašam saprast, cik lietu riska līmeni viņš ir gatavs uzņemties.

Ne mazāk būtiska datu apdraudējuma kategorija, ir datu zaudēšana, jo pat, lietojot visuzticamāko šobrīd pieejamo datortehniku un programmatūru, 100% garantijas pret datu zudumiem nav. Visbiežākie iemesli datu zaudēšanai tiek minēti: cilvēciskās kļūdas, piemēram, nejauša datu dzēšana, cietā diska sabojāšanās, piemēram, nolietošanās, kā arī datora vai ārējo datu nesēju zādzība vai pazaudēšana.

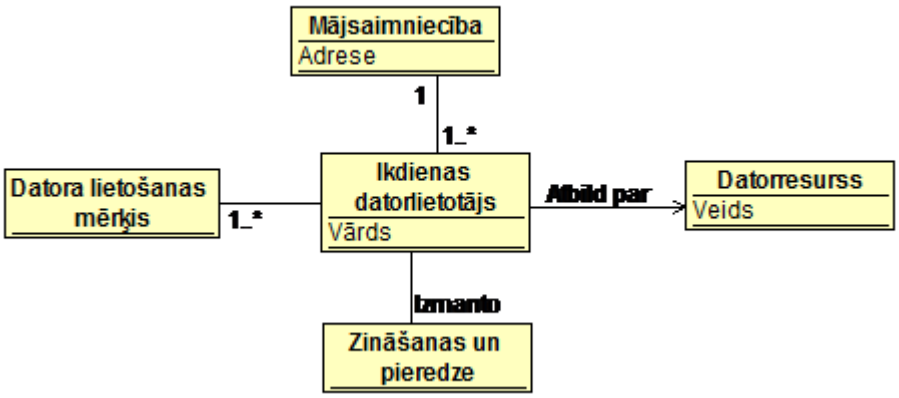
Neveicot attiecīgus drošības pasākumus, dati noteikti tiks zaudēti, jo nav tādu elektronisku datu nesēju, kas būtu mūžīgi. Pēc tiešsaistes rezerves kopiju nodrošināšanas servisa kompānijas "Kabooza" aptaujas (aptaujāti 4257 lietotāji), 66% aptaujāto ir kādreiz

zaudējuši savus datus, pietam 44% gadījumu, pēdējā gada laikā. Kā jau viegli var iedomāties, regulāru datu rezerves kopiju veidošana tiek veikta reti – 18% [Kab09].

Minētais apdraudējumu uzskaitījums nav galīgs, diemžēl to skaits un daudzveidība nemitīgi palielinās. Citu starpā iespējami arī psiholoģiski apdraudējumi, neadekvāta anonīmu interneta komentāru uztvere un daudz citu.

1.3.3. Ikdienas datorlietotājs mājsaimniecībā

Ikdienas datorlietotāja jēdzienam nav vispāratzītas definīcijas [HOW12]. Cilvēki lieto datorus un citas ierīces ļoti atšķirīgiem mērķiem. Dažādas ir arī zināšanas un pieredze informācijas tehnoloģiju jomā. Šī darba ietvaros ikdienas datorlietotāju raksturo piederība mājsaimniecībai, datora lietošanas mērķi, zināšanas un pieredze, kā arī atbildība par datorresursiem (2. attēls).



2. attēls Ikdienas datorlietotājs mājsaimniecībā

Mājsaimniecības jēdzienu definē statistikas vajadzībām [Stat1, Stat2]. Balstoties uz [Stat2] definīciju, šī darba ietvaros mājsaimniecība ir viena vai vairākas personas, kas dzīvo vienā mājoklī un kopīgi vai katra atsevišķi atbild par datorresursu izmantošanu.

Ikdienas datorlietotājs ir persona, kas izmanto datorresursus personīgām vajadzībām. Datorresursu lietošanas mērķi ir gan interneta izmantošanas mērķi (4. tabula), gan fotogrāfiju, videomateriālu un dokumentu apstrāde. Ikdienas datorlietotājs lielāko daļu darbību elektroniskās vidē var izdarīt uz planšetdatora, nav nepieciešama sarežģīta programmatūra. Mērķi, kas saistīti ar profesionālo darbību, un pieslēgums darbavietas datortīklam ir ārpus šī darba tvēruma.

Ikdienas datorlietotāja zināšanas un pieredze informācijas tehnoloģiju vai līdzīgā jomā ir maza vai neliela, viņam nav formālas izglītības minētajās jomās. Izglītoti informācijas tehnoloģiju speciālisti un personas, kam ir padziļināta interese par minēto

jomu, ir ārpus šī darba tvēruma. Ikdienas datorlietotājam var būt nelielas zināšanas informācijas drošības jomā, kas saņemtas informācijas drošības apzināšanās veicināšanas aktivitātēs darba vietā.

Ikdienas datorlietotāja būtiska īpašība ir atbildība par datorresursa lietošanu. Mazi bērni un personas, kas pilnībā paļaujas uz citas personas veiktām darbībām datorresursu uzturēšanā un darbu ar datoru veic šīs personas uzraudzībā, ir ārpus šī darba tvēruma.

Mājsaimniecības datorresursa jēdziens iekļauj galddatoru, klēpjdatoru, planšetdatoru, viedtālruni un pieslēgumu internetam, izmantojot vadu vai bezvadu tīklu.

Tradicionāla asociācija vēsta, ka informācijas drošības problēma pamatā ir saistoša lieliem uzņēmumiem, varbūt arī valsts institūcijām. Šajā tradicionālajā izpratnē lietotājs ir viens no būtiskākiem drošības apdraudējumiem. Tomēr tehnoloģijas jau ir mums visapkārt, un lietotāju skaits palielinās milzīgā ātrumā, arī informācijas risku loks paplašinās un iekļauj arī personīgās informācijas riskus, kas būtu atbilstoši jāpārvalda.

Ikdienas datorlietotājam tieši informācijas privātumam ir vislielākā vērtība. Tā gan nav aprēķināma naudā vai citās precīzās mērvienībās. Tomēr privātuma zaudējums var būtiski ietekmēt indivīda vai ģimenes dzīvi. Elektroniskas informācijas privātuma aizsardzība ir viens no būtiskākajiem informācijas drošības pārvaldības mērķiem mājsaimniecībā. Ikdienas datorlietotājs tāpat kā uzņēmums ir ieinteresēts, lai "informācijas riski tiek atbilstoši pārvaldīti". Viņam ir sava attieksme pret risku (tolerance), kas jāņem vērā, tos vērtējot un izvēloties informācijas drošības pasākumus.

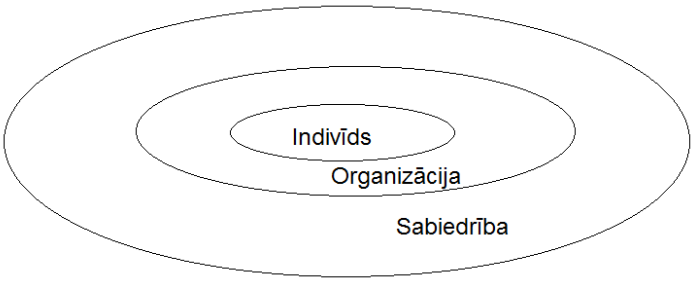
Kaut vismaz desmit gadus laiku pa laikam tiek publicēti raksti par uz lietotāju vērstu drošību [PIR08, DOU04, KOL09], joprojām nav atrasts vispārzināms risinājums drošības procesa pārvaldīšanai ikdienas datorlietotāja vajadzībām.

Vislabākā tehnoloģiskā sistēma nekad nenovērsīs apdraudējumus, ko var radīt tās lietotājs, bet ir iespējams "uzlabot" jeb izglītot lietotāju tā, lai šo apdraudējumu būtu mazāk [ATK09, WOL10, KRI10].

Promocijas darba pētījuma pamatā ir šāda problēma: ikdienas datorlietotājs ne vienmēr ir pietiekami izglītots un zinošs par riskiem rīcībā ar elektronisko informāciju, kā arī nesaņem atbilstošu atbalstu.

Minēto problēmu var risināt, izmantojot uzņēmējdarbības vidē uzkrāto pieredzi informācijas drošības pārvaldībā. Indivīds, kurš apguvis informācijas drošības pamatprasmes savā darbavietā, var tās izmantot arī privātā vidē [TAL10], tādējādi veicinot

informācijas drošības kultūras attīstību sabiedrībā (3. attēls). Sava loma ir arī valsts aktivitātēm un akadēmiskajai videi [KDS14].



3. attēls. Indivīds organizācijā un sabiedrībā

1.4. Saistītie pētījumi

Plašs tēmu klāsts par datoru drošības tematiku apkopots Kembridžas Universitātes profesora Rosa Andersona (*Ross Anderson*) grāmatā "Security Engineering: A Guide to Building Dependable Distributed Systems" [AND04]. Dažādu sistēmu vidū autors apraksta arī mājas vidi, mudinot padomāt, ka arī privātā vidē var tikt izmantotas nozīmīgas informācijas sistēmas un līdz ar to, strādājot pie drošības risinājumu izveides, nedrīkst aizmirst mājsaimniecību vajadzības [AND04, 10. lpp].

Svarīgi ir pievērst uzmanību lietojamībai un psiholoģijai [AND04, 17. lpp]. Mūsdienās nozīmīga daļa datoruzbrukumu vairāk saistīta ar psiholoģisku metožu izmantošanu, tehnoloģijām atstājot tikai papildus rīka statusu. Informācijas pikšķerēšana ar mērķi veikt krāpnieciskas darbības, izmanto cilvēcisku nezināšanu u.c. īpašības, tehnoloģijām atstājot tikai tehnisku informācijas pārsūtīšanas lomu. Autors analizē paroļu lietošanu, ņemot vērā gan lietojamību, gan psiholoģiju, gan drošību. Nodaļu noslēdz tālākas izpētes vērtu problēmu pārskats. Starp pētāmām tēmām minēta psiholoģijas un drošības attiecības. Promocijas darba ietvaros piedāvātais risinājums ir solis attiecīgā virzienā.

Pasaulē atzīta autoritāte Brūss Šneiers (*Bruce Schneier*) darbā [SCH] uzsver atšķirības starp sajūtām justies droši un faktisko drošību pēc objektīva vērtējuma. Autors analizē cilvēku uzvedības aspektus, riska novērtēšanas psiholoģiju un emocionālās uztveres dažādību. Tiek uzsvērta drošības kompromisa nepieciešamība. Informācijas

sistēmu drošības profesionāļiem ir pazīstama aksioma par 100% drošības neiespējamību, taču, skaidrojot informācijas drošības jautājumus ikdienas datorlietotājiem, nereti ir grūti pieņemt, ka katram kā cilvēkam ir atšķirīga attieksme pret risku un līdz ar to vēlme īstenot konkrētus drošības pasākumus. [SCH] uzsver faktu, ka cilvēkam ir tieksme pārvērtēt dažus riskus, savukārt citus – nepietiekami novērtēt. Autors to skaidro, analizējot cilvēku uzvedību un uztveri. Starp riskiem, ko cilvēki nepietiekami novērtē, ir arī datora un elektroniskas informācijas izmantošanas riski, t.sk. sociālajos tīklos publicētas informācijas iespējamā pielietošana negaidītiem mērķiem.

Grāmatas [LEE07] autori tās publiskajā aprakstā pozicionē paveikto kā pirmo visaptverošu publikāciju kopumu par datoru drošības vēsturi. Grāmata ir 28 rakstu apkopojums par tādām tēmām kā intelektuālā īpašuma aizsardzība, identitātes pārvaldība, komunikāciju drošība, privātuma aizsardzība u.c., ko izstrādājuši gan datorzinātnes, gan juridisko zinātņu speciālisti. Promocijas darba tematikai atbilstoši ir raksti par datoru drošības standartu vēsturi [LEE07, 595. lpp] un interneta drošības vēsturi [LEE07, 681. lpp].

Raksts par datoru drošības standartiem pamatā veltīts dažādiem tehnoloģiskiem standartiem, apskatot arī savulaik nozīmīgo "*The Orange Book*". Viena raksta nodaļa stāsta par datoru drošības attiecībām ar sabiedrību, tomēr tās apskatītas tikai no privātuma tiesiskās puses, analizējot atšķirības ASV un Eiropā un uzsverot privātuma svarīgumu darbā ar medicīnisku informāciju. Raksts noslēdzas ar atvērtu secinājumu: datoru tīkliem kļūstot visuresošiem, drošības produktu un procesu daudzveidība pieaugs.

Interneta drošības vēstures raksts pievērš uzmanību problēmai, ka tīkla drošības jautājumi kļūst daudz sarežģītāki, līdzko tajos iesaistās uzņēmumi un, jo īpaši – mājsaimniecības. Izejot ārpus akadēmiskās vides, drošības risinājumi ir komercializēti, ne vienmēr dārgākie risinājumi ir labākie, turklāt lietotāji, piemēram, uzņēmumi, kas nav datoru drošības jomas speciālisti, neprot izvēlēties piemērotākos. Datortīkli tiek izmantoti gan kā vērtība, ko iespējams bojāt (pakalpojumatteices uzbrukumi), gan kā rīks citām noziedzīgām darbībām (informācijas pikšķerēšana krāpnieciskos nolūkos). Kaut arī ir mēģinājumi atrast risinājumu interneta arhitektūras nozīmīgiem uzlabojumiem, tomēr nākas arī sadzīvot ar trūkumiem, ko rada ļoti strauja datortīkla izplešanās no šauras akadēmiskas vides uz visuresošu, komerciālu un publisku vidi.

Informācijas sistēmu drošības pārvaldībai veltīti dažādi pētījumi. Lielu daļu no tiem var raksturot ar citātu no [BJO05, Abstract]: "*This thesis is concerned with issues relating*

to the management of information security in organisations, motivated by the need for cost-efficient information security.", t.i., pētījumi pamatā veltīti informācijas drošības pārvaldībai organizācijās, turklāt ar nozīmīgu uzsvaru uz izmaksu analīzi. Nākamais teikums [BJO05, Abstract] saka "*It is based on the assumption that: in order to achieve cost-efficient information security, the point of departure must be knowledge about the empirical reality in which the management of information security takes place.*", t.i., izmaksu efektīvai informācijas drošības pārvaldībai nepieciešamas zināšanas par vidi, kurā šī pārvaldība tiek veikta.

[JOH09] pētot uzņēmumus, kas piedzīvojuši zaudējumus datoruzbrukumos, parādīta informācijas drošības pārvaldības pozitīva ietekme. Savukārt, [HIL09] uzsver privātuma lomas pieaugumu organizāciju atbildību privātuma nodrošināšanā un apraksta risku novērtēšanu kā vienu no rīkiem arī privātuma pārvaldībai.

Visuresošu tehnoloģiju laikmetā drošības risinājumi nav atkarīgi tikai no to matemātiskām un tehniskām īpašībām, bet arī no cilvēku spējām tos saprast un izmantot ("*Effective security solutions depend not only on the mathematical and technical properties of those solutions, but also on people's ability to understand them and use them as part of their work.*" [DOU04]). Raksta autori pievēršas drošības lietojamības problemātikai, lielu uzmanību pievēršot cilvēkfaktoram. Izmantojot kvalitatīvu uz intervijām balstītu izpēti, analizēta datoru lietotāju attieksme pret drošības pasākumiem. Kaut arī katrs parasti ir atradis veidu, kā sadzīvot ar drošības prasībām, tomēr, ne vienmēr tas ir darīts ar pilnvērtīgu izpratni par prasību mērķi. Tai pašā laikā nereti kopumā sarežģīts drošības pasākumu kopums nesasniedz mērķi, jo dažas lietotājam veicamas darbības netiek pareizi izdarītas. Autori secina, ka līdzās veiksmīgiem pētījumiem drošas skaitļošanas matemātiskos pamatos ne tik veiksmīgi ir izdevies atrast risinājumus, lai padarītu sistēmas drošas to ikdienas lietošanā ("*While the research community has been extremely successful in developing the mathematical and technical foundations of secure computing and communication services, we have, perhaps, been less successful in the more practical task of making systems effectively secure.*", [DOU04]).

Vairāki pētījumi veltīti datorlietotāju uzvedības pētīšanai uzņēmumos. Izmantojot intervijas ar uzņēmumu darbiniekiem, [BEA08] autori analizē iemeslus drošības noteikumu pārkāpumiem un piedāvā risinājumu cilvēku uzrunāšanai tādā veidā, lai būtu labāk izprotami uzņēmuma drošības pārvaldīšanas mērķi un darbinieku rīcības nozīme to sasniegšanā.

Uzņēmumu un iestāžu darbinieki ne vienmēr ievēro informācijas drošības politikas. Aptauja, kuras mērķis bija pētīt iemeslus, kāpēc sociālie darbinieki neseko drošības prasībām, ir konstatējusi, ka visbiežākais cēlonis ir informācijas drošības prasību neatbilstība darba ieradumiem [KOL09].

[KRU08] pētījums veikts, aptaujājot dažādu jomu studentus par viņu attieksmi un paradumiem drošības produktu un pasākumu izmantošanā. Kā viens no pētījuma izmantošanas virzieniem minēta iespējamība organizācijām izprast, kādu attieksmi pret drošības prasībām var sagaidīt no jauniem darbiniekiem.

Darbinieku informācijas drošības apzināšanās un drošības uzvedība pētīta disertācijā [GRA10], starp secinājumiem minēts, ka liela respondentu daļa zina, kā rīkoties, ja dators brīdina par iespējamu vīrusu. Tai pašā laikā lielai daļai ir slikti drošības ieradumi attiecībā uz e-pasta pielikumfailu skenēšanu un paroļu saglabāšanu lietojumprogrammu atmiņā. Pētījuma rezultāti noteikti ir noderīgi pētītās organizācijas drošības pilnveidei. Pētījuma autori konstatējuši saistību starp tā dalībnieku drošības uzvedību un drošības apzināšanās līmeni.

Grāmatas [AND04] secinājumu nodaļā prognozēts, ka drošības pārvaldība un realizācija šobrīd (rakstīts 21.gs. sākumā) atrodas lielu izmaiņu priekšā. Pirms 10 gadiem liela uzņēmuma drošības pārvaldnieks bieži bija atvaļināts policists, kam datoru drošība bija nenozīmīgs papildu pienākums. Pirms minētajiem 10 gadiem drošības tehnoloģijas bija atsevišķu speciālistu pārvaldītas "salas", starp kurām bija kriptogrāfijas joma, operētājsistēmu aizsardzība, signalizācijas sistēmas, utt. Pirms 10 gadiem valdības rūpes par drošības tehnoloģijām pamatā bija saistītas ar militāro jomu [AND04, 889. lpp].

[AND04] autors prognozē, ka 21.gs. drošības inženieris būs atbildīgs par nepārtraukti mainīgām sistēmām ar daudzveidīgiem apdraudējumiem, ievērojama daļa darba būs saistīta ar tehnoloģiju atjaunināšanu, ņemot vērā arī juridiskus aspektus un izprotot visas drošības pārvaldības daļas, piemēram, kriptogrāfiju, lietotāju tiesību pārvaldību, informācijas plūsmas un datortīklu darbību, tajā pašā laikā daudz būs jāsadarbojas ar uzņēmumu vadību un jāsaprot uzņēmējdarbības procesi: "*The security engineer of the twenty-first century will be responsible for systems that evolve constantly and face a changing spectrum of threats. She will have a large and constantly growing toolbox. A significant part of her job will be keeping up to date technically: understanding the latest attacks, learning how to use new tools, and keeping up on the legal and policy fronts. Like any engineer, she'll need a solid intellectual foundation; she will have to*

understand the core disciplines such as cryptology, access control, information flow, networking and signal detection. She'll also need to understand the basics of management: how accounts work, the principles of finance and the business processes of her client. But most important of all will be the ability to manage technology and play an effective part in the process of evolving a system to meet changing business needs. The ability to communicate with business people, rather than just with other engineers, will be vital; and experience will matter hugely." [AND04, 891. lpp].

1.5. Informācijas drošības pārvaldības labā prakse

Uzņēmējdarbības vidē jau ir uzkrāta zināma informācijas drošības pārvaldības pieredze. Katram uzņēmumam tā ir vispirms balstīta konkrēti piedzīvotos notikumos, piemēram, datora sabojāšanās un ar to saistīta informācijas nepieejamībā, vīrusa uzbrukums un neskaidrība par nodarītā kaitējuma apmēru. Palielinoties IT izmantošanas apjomiem un izmaiņu ātrumam, būtisku ieguvumu informācijas drošības pārvaldības uzlabošanā var dod sadarbība ar citiem uzņēmumiem, ko nodarbina līdzīgas problēmas.

Viens no šādas sadarbības piemēriem ir *The Information Security Forum* (ISF) – pasaules vadošā neatkarīgā autoritāte informācijas drošībā. ISF piedāvā praktiskus ieteikumus un risinājumus, ko rada tās biedru kolektīvās zināšanas un pieredze [ISF]. Lielākā daļa materiālu gan ir pieejami tikai organizācijas biedriem, tomēr nav aizliegts tos izmantot ideju meklēšanai akadēmiskām vajadzībām. Visiem pieejama ir Labās prakses standarta informācijas drošībai 2007. gada versija [ISFSt].

Eiropas Tīkla un informācijas drošība aģentūra (ENISA) dibināta 2004. gadā ar mērķi uzlabot tīklu un informācijas drošības pārvaldību Eiropas Savienībā. ENISA loma ir veicināt informācijas drošības kultūras veidošanos gan sabiedrībā kopumā, gan valsts pārvaldē, gan uzņēmējdarbības vidē. Viens no ENISA darbības rezultātiem ir ziņojumi par aktuālām tēmām informācijas drošībā [ENISAPP].

Organizācija OECD jau 1992. gadā izdeva pirmās Drošības vadlīnijas informācijas drošības jomā. Pilnveidota un papildināta vadlīniju versija apstiprināta 2002. gadā un piedāvā ieteikumus informācijas sabiedrības dalībniekiem ceļā uz drošības kultūru [OECD02]. Vadlīnijas iesaka deviņus principus, kas papildina viens otru un skatāmi kopumā (5. tabula).

5. tabula. Drošības pārvaldības principi

Princips	Skaidrojums
Apzināšanās	Katram jāapzinās informācijas sistēmu un tīklu drošības nepieciešamība un katra iespējas to uzlabot.
Atbildība	Katrs ir atbildīgs par informācijas sistēmu un tīklu drošību.
Reaģēšana	Katrs rīkojas savlaicīgi un sadarbojoties, lai novērstu, noteiktu un reaģētu uz drošības incidentiem.
Ētika	Katram jārespektē citu likumīgās intereses.
Demokrātija	Informācijas sistēmu un tīklu drošībai jābūt savienojamai ar demokrātiskas sabiedrības pamatvērtībām.
Risku novērtējums	Katram jāveic risku vērtēšana.
Drošības izstrāde un ieviešana	Katram jāiekļauj drošība kā informācijas sistēmu un tīklu būtisks elements.
Drošības pārvaldība	Katram jāpiemēro visaptveroša pieeja drošības pārvaldībai.
Pārskatīšana	Katram jāpārskata un jāpārvērtē informācijas sistēmu un tīklu drošība un jāveic atbilstoša pilnveide drošības politikā, paradumos, pasākumos un procedūrās.

Latvijā informācijas drošības pārvaldības labās prakses piemēri atrodami bankās. Šī pārvaldības joma banku sektorā uzsāka strauju attīstību 1998. gadā līdz ar Latvijas Bankas izstrādātām vadlīnijām. Konkrētas prasības noteica ar Latvijas Bankas padomes 1998. gada 16. jūlija lēmumu Nr. 48/5 apstiprinātie "Banku informācijas tehnoloģijas drošības noteikumi". Šobrīd prasības noteiktas Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības noteikumos [FKTK].

Valsts pārvaldē pirmais normatīvais akts elektroniskas informācijas drošībā bija Informācijas sistēmu drošības noteikumi, kas bija spēkā no 2000. gada 1. jūlija līdz 2002. gada 5. decembrim. Šos noteikumus savulaik izstrādāja tehnoloģiju speciālisti, tie bija atbilstoši standartiem un ietvēra gandrīz visus IT drošības pārvaldības aspektus, kas bija zināmi tajā laikā. Tomēr netika pilnvērtīgi veikta valsts pārvaldes darbinieku un likumdevēju izglītošana, lai iegūtu atbilstošu drošības apzināšanos. Līdz ar informācijas drošības apzināšanās trūkumu, turpmāk normatīvos aktos tika samazināts to regulētais laukums. Vairākus gadus informācijas sistēmu drošības pārvaldība bija noteikta tikai

nelielai valsts informācijas daļai, un to regulē Valsts informācijas sistēmu likums un ar to saistītie normatīvie akti.

Kopš 2011. gada 1. februāra informācijas tehnoloģiju drošības pārvaldību Latvijā regulē Informācijas tehnoloģiju drošības likums [ITDL]. Tas cita starpā visām valsts un pašvaldību iestādēm nosaka pienākumu ne retāk kā reizi gadā veikt darbinieku instruktāžu informācijas tehnoloģiju drošības jautājumos. Ar minēto likumu saistīti Ministru Kabineta noteikumi nosaka kārtību, kādā tīkla lietotājam var tikt īslaicīgi slēgta piekļuve elektronisko sakaru tīklam.

Lielās organizācijās informācijas drošības pārvaldību nodrošina atbilstoši speciālisti, tiek veltīts darbs, lai šie speciālisti nepārtraukti uzlabotu savas zināšanas drošības pasākumu uzturēšanā un mācētu palīdzēt lietotājiem. Taču joprojām bieži uzņēmumu vadība paļaujas uz informācijas tehnoloģiju speciālistiem un nevēlas uzņemties atbildību par riskiem, kas saistīti ar informācijas tehnoloģiju izmantošanu. Dažādās konferencēs un citās pieredzes apmaiņas vietās tiek nepārtraukti meklēti risinājumi, lai uzrunātu vadītājus ar piemēriem, kas tiem personīgi tuvi, meklētu skaidrojumus un salīdzinājumus, lai uzņēmumu vadītāji saprastu ar IT saistītos riskus. Informācijas drošība nav tikai tehnoloģijas, atbildīgajam informācijas drošības speciālistam jābūt ar labām komunikācijas spējām, jāspēj sarunāties gan IT speciālistiem saprotamā valodā, gan vadītājiem saprotamā valodā [JOH07].

Organizācijās būtiska ir pareizās attieksmes pret informācijas drošību noteikšana, sākot no visaugstākās vadības [JOH07]. Ikdienas datorlietotāju vidē mājsaimniecībā nav stingri noteiktas hierarhijas, kas prasa katram no lietotājiem saprast savu attieksmi un attiecīgi rīkoties.

1.6. Nodaļas secinājumi

Informācijas drošības tēma ir gan uzņēmumu, gan valsts pārvaldes iestāžu uzmanības lokā. Taču jaunās tehnoloģijas aktīvi tiek lietotas arī privātā vidē, bet nepieciešamās lietotāju drošības pārvaldības prasmes bieži nav pietiekamas.

Uzņēmējdarbības vidē ir noteiktas informācijas drošības prasību izpildes un atbilstošas pārvaldības prasības.

- Ārējas prasības ietver likumus, pārraugošo institūciju noteikumus, piemēram [FPDAL, FKTK].

- Iekšējās prasības tiek noteiktas ar Drošības politiku, kas ir pamats efektīvai informācijas drošības pārvaldībai uzņēmumos [ISFSt, ISO27002].
- Risku novērtēšana ir viens no būtiskiem instrumentiem nepieciešamo drošības pasākumu izvēlei [ISO27002]. Risku pārvaldīšana palīdz izprast uzņēmuma vajadzības un apdraudējumus mērķu sasniegšanā, kā arī plānot rīcību aizsardzībai pret apdraudējumiem [WHI10].
- Drošības kultūra ietver kultūrsociālus pasākumus, kas papildina tehniskus drošības pasākumus, ar mērķi veicināt informācijas drošības rīcības ienākšanu ikdienas rutīnā [SCH03].

Informācijas sistēmu drošības pārvaldībai veltīti dažādi pētījumi. Tomēr liela daļa no tiem pamatā apskata informācijas drošības pārvaldību organizācijās, turklāt ar nozīmīgu uzsvaru uz izmaksu analīzi. Otrs pētījumu virziens ir organizāciju darbinieku rīcība, ievērojot informācijas drošības pārvaldības prasības, kur starp risinājumiem situācijas uzlabošanai dominē darbinieku izglītošana un drošības kultūras pilnveide. Autorei neizdevās atrast avotus, kas piedāvātu sistemātisku skatījumu uz informācijas drošības pārvaldību mājsaimniecībā.

Labās prakses piemēri pārsvarā attīstās uzņēmējdarbības vidē. Atsevišķas organizācijas gatavo informācijas drošības padomus un materiālus izmantošanai plašākā sabiedrībā, bet to izmantošana bez vispārējas izpratnes ir ierobežota. Tomēr uzņēmējdarbības vidē uzkrāto pieredzi informācijas drošības pārvaldībā varētu izmantot, izstrādājot informācijas drošības pārvaldības vadlīnijas un risku novērtēšanas rīku mājsaimniecībai.

Likumdošana Latvijā un, cik autorei zināms, arī citur pasaulē nenosaka pienākumus informācijas drošībā katram iedzīvotājam. Motivācijai sargāt informāciju un elektronisko vidi jābūt brīvprātīgai. Darba turpmākajās nodaļās apkopotā informācija un aprakstītie rīki izmantojama ikdienas datorlietotāju drošības apzināšanās veicināšanā.

2. INFORMĀCIJAS DROŠĪBAS PĀRVALDĪBAS MODEĻI

2.1. Nodaļas mērķi

Informācijas drošības pārvaldībā ir uzkrāta daudzveidīga pieredze, kas bieži ir arī pierakstīta. Viens no šādu pieredzes pierakstu veidiem ir arī dažādi modeļi. Bieži tie ir noformēti kā standarti vai labās prakses apkopojumi.

Nodaļā apskatīti dažādi modeļu veidi, t.sk. piekļuves vadības, konfidencialitātes un integritātes modeļi un Latvijā populāri informācijas drošības pārvaldības standarti.

Šīs nodaļas ietvaros konceptuāli aprakstīts autores izveidots drošības pārvaldības konceptuāls modelis mājsaimniecībai. Balstoties uz [ISFSt], izveidots konceptuāla modeļa veidā pierakstīts informācijas drošības pārvaldības modelis uzņēmumam, kas izmantots kā starpposms mājsaimniecības informācijas drošības pārvaldības modeļa izveidei.

Nodaļas noslēgumā sniegts ieskats informācijas drošības vadlīnijās mājsaimniecībai.

2.2. Modeļu veidi

Starp modeļu veidiem ir gan piekļuves vadības modeļi, gan drošības arhitektūras modeļi, gan drošības pārvaldības modeļi. Drošības modelis ir vispārējs projekts (*blueprint*), ko piedāvā dažādas organizācijas. Kā paraugu var izmantot arī citas organizācijas paveikto. Modeļus izmanto atsaucēm vai salīdzinājumam un parasti pielāgo konkrētas organizācijas vajadzībām, jo, kas labi der vienam, ne vienmēr der arī citam. [WHI10, *Chapter 6*]

2.2.1. Piekļuves vadības, konfidencialitātes un integritātes modeļi

Ir zināmi dažādi piekļuves vadības modeļu veidi, to skaitā Izvēles piekļuves vadības (Discretionary Access Control (DAC)) modeļi un Obligātās piekļuves vadības (Mandatory Access Control (MAC)) modeļi. Izvēles piekļuves vadības modeļa svarīgākie jēdzieni ir 'datu īpašumtiesības' un 'piekļuves tiesības', t.i., katram datu kopumam vai informācijas sistēmai ir noteikts īpašnieks, un šis īpašnieks nosaka piekļuves tiesības katram lietotājam. Obligātās piekļuves vadība dot tiesības piekļūt datiem tikai tad, ja lietotājam iepriekš ir dotas tiesības piekļūt konkrēta klasifikācijas līmeņa datiem. Šo

modeļa veidu bieži izmanto informācijai, kas saistīta ar valsts drošību vai militāriem jautājumiem, un parasti tiek izmantoti klasifikācijas līmeņu apzīmējumi un ļoti stingras noteiktas prasības katra līmeņa informācijas aizsardzībai. [WHI10, *Chapter 6*]

Bell-LaPadula modeli tā autori izstrādāja valdības un militāras informācijas aizsardzības vajadzībām. Šajā modelī objekti, kas var būt ne tikai dati, sadalīti līmeņos pēc konfidencialitātes, piemēram, slepeni, konfidenciāli, neklasificēti. Lietotājiem var tikt piešķirtas piekļuves tiesības pa līmeņiem, turklāt tiesības piekļūt augstākam līmenim ietver tiesības arī uz zemāku, bet ne otrādi [WHI10, *Chapter 6*]. Šāds modelis tiek izmantots valsts noslēpuma aizsardzībā Latvijā.

Biba integritātes modelis ir līdzīgs Bell-LaPadula modelim aspektā, ka arī šajā modelī objekti tiek iedalīti līmeņos. Galvenā atšķirība ir tāda, ka iedalījums tiek veikts pēc integritātes svarīguma. Lietotājiem, kam ir piešķirtas tiesības piekļūt kādam noteiktam integritātes līmenim, nav tiesību mainīt datus, kas atrodas augstākā līmenī [WHI10, *Chapter 6*].

Nedaudz sarežģītāki, jo ietver daudzveidīgākus elementus, ir Clark-Wilson integritātes modelis un Graham-Denning piekļuves kontroles modelis [WHI10, *Chapter 6*].

Piekļuves vadības, datu konfidencialitātes un integritātes prasības mājsaimniecībā nav tik stingri noteiktas, un līdz ar to šajā apakšnodaļā aprakstītos modeļus nav lietderīgi izmantot.

2.2.2. Informācijas drošības pārvaldības standarti

Biežāk lietotie informācijas drošības pārvaldības modeļi mūsdienās ir dažādi šīs jomas standarti [WHI10, *Chapter 6*]. Šim apgalvojumam noteikti piekrīt arī autore. Kaut arī [WHI10] autori ir novērojuši, ka dažkārt rodas priekšstats, ka informācijas drošības pārvaldības modeļu ir tikpat, cik konsultantu, kas tos iesaka, daļa standartu ir populārāki un biežāk izmantoti.

Daļa no standartiem jāiegādājas par samaksu, kas nereti var būt iemesls, kāpēc ikdienas datorlietotājs mājsaimniecībā tos nez vai izmantos. Bez maksas visiem pieejami ir NIST publikācijas, t.sk. Pamata (*underlying*) tehniskie modeļi informācijas tehnoloģiju drošībai [NISTCS]. Publikāciju skaits ir apjomīgs [NIST], tomēr starp tām autorei neizdevās atrast pietiekami vispārīgu informācijas drošības pārvaldības aprakstu, kas būtu piemērots pārveidošanai par drošības pārvaldības modeli mājsaimniecībai.

Informācijas drošības pārvaldībā Latvijā visbiežāk tiek izmantoti trīs standarti:

- LVS ISO/IEC 27002:2008 "Informācijas tehnoloģija. Drošības metodika. Prakses kodekss informācijas drošības pārvaldībai" [ISO27002];
- Vadības uzdevumi informācijas un saistītām tehnoloģijām [COBIT];
- ISF Labās prakses standarts informācijas drošībai [ISFSt].

LVS ISO/IEC 27002:2008 "Informācijas tehnoloģija. Drošības metodika. Prakses kodekss informācijas drošības pārvaldībai" [ISO27002] – ISO standarts, kas noteikts arī kā Latvijas nacionālais standarts.

Vadības uzdevumi informācijas un saistītām tehnoloģijām (*The Control Objectives for Information and related Technology*) [COBIT] – Informācijas sistēmu audita un vadības asociācijas (ISACA) izstrādāts IT pārvaldības standarts, kas sākotnēji bija paredzēts auditoru darbam, bet tagad tam ir pievienots materiāls Drošības pamatnostādnes (*Security Baseline*).

ISF Labās prakses standarts informācijas drošībai (*ISF Standard of Good Practice for Information Security*) [ISFSt] – organizācijas ISF izstrādāts standarts, kas šobrīd bez maksas pieejams katram interesentam, tiek izmantots arī kā mācību materiāls LU DF.

LVS ISO/IEC 27002:2008 piedāvā vadlīnijas, kas palīdz noteikt, uzturēt un pilnveidot informācijas drošības pārvaldību organizācijā. Standarts aptver 39 drošības kategorijas, kas grupētas 11 sadaļās:

- Drošības politika;
- Informācijas drošības organizatorika;
- Aktīvu pārvaldība;
- Drošība attiecībā uz cilvēkresursiem;
- Fiziskā drošība un vides drošība;
- Sakaru un ekspluatācijas pārvaldība;
- Piekļuves kontrolēšana;
- Informācijas sistēmu iegāde, izstrāde un uzturēšana;
- Informācijas drošības incidentu pārvaldība;
- Organizācijas darbības nepārtraucamības pārvaldība;
- Atbilstība normām.

Katrai drošības kategorijai ir noteikts mērķis, nepieciešamās drošības vadīklas un to ieviešanas vadlīnijas.

Saskaņā ar ISO 27002 drošības pārvaldības būtisks elements ir risku pārvaldīšana. Uzsākot informācijas drošības procesa ieviešanu vai pilnveidi, pirmais uzdevums ir risku novērtēšana. Risku vērtējums ir pamats drošības vadīklu izvēlei. To vērtēšanā izmantojama gan informācija par organizācijas aktīviem, informāciju, apdraudējumiem, gan iepriekšējā pieredze, piemēram, notikušie drošības incidenti. Risku pārvaldīšanas metodes standartā nav iekļautas.

Promocijas darba tēmas ietvaros būtiskākās ir sadaļas par drošības politiku, personāla resursu drošību, jo īpaši – informācijas drošības apzināšanās, izglītība un apmācības.

Drošības politikas mērķis ir noteikt drošības pārvaldības uzdevumus, ņemot vērā gan organizācijas vajadzības, gan saistošās likumdošanas vai regulatoru prasības. Drošības politikai jābūt izstrādātai rakstiski un pieejamai visiem organizācijas darbiniekiem un citām iesaistītajām personām. Politika ir regulāri jāpārskata un, ja nepieciešams, jāuzlabo, lai tā atspoguļotu gan izmaiņas organizācijas vajadzībās, gan iekšējos procesos vai apdraudējumos.

Personāla resursu pārvaldības ietvaros jānodrošina, lai katra iesaistītā persona zinātu savus pienākumus informācijas drošības pārvaldībā un apzinātos informācijas drošības nozīmi. Vērtējot darbinieku piemērotību konkrētu pienākumu veikšanai, nedrīkst aizmirst informācijas drošības aspektus. Zināšanu pilnveidei šajā virzienā jābūt regulārai.

Vadības uzdevumi informācijas un saistītām tehnoloģijām COBIT, ko izstrādājusi asociācija ISACA, ir pasaulē samērā plaši lietots ietvars, kurā apkopota pieredze IT pārvaldībā ar misiju izstrādāt un publicēt IT vadības uzdevumu kopumu, ko var pielietot gan uzņēmumu vadītāji, gan auditori. Sākotnēji materiāls pamatā bija paredzēts auditoriem, kuru darbs aizvien vairāk bija saistīts ar informācijas sistēmu un saistīto tehnoloģiju pārbaudēm. Šobrīd COBIT ir "IT pārvaldības ietvars un atbalsta rīku kopums, kas dod iespēju vadītājiem novērst plaisu starp pārvaldības prasībām, tehniskiem jautājumiem un uzņēmējdarbības riskiem" [COBIT]. COBIT balstās uz četriem "vaļiem": pamatdarbības prasības, IT resursi, IT procesi un uzņēmuma informācija – tā pamatā ir procesu kopa. Starp pamatdarbības prasībām tiek apskatīta arī informācijas konfidencialitāte, integritāte un pieejamība. Bet detalizētākai drošības pārvaldībai tiek ieteikts izmantot ISO 27002 standartu.

Papildus pamata COBITam ir pieejams arī COBIT Drošības bāzlīnija jeb Informācijas drošības izdzīvošanas komplekts [CobSB]. Komplekts apraksta 44 vadības

uzdevumus informācijas drošības pārvaldībai un parāda, kā tiek atbilst COBIT procesiem un ISO 27002 nodaļām. Vadības uzdevumi ietver risku pārvaldību, bet īpaši neizceļ lietotāju drošības apzināšanās veicināšanu, aprobežojoties tikai ar drošības aspektiem jaunu darbinieku izvēlē.

Komplekta būtiska daļa ir padomu apkopojums konkrētām informācijas lietotāju grupām. Viena nodaļa šajā komplektā paredzēta mājas lietotājiem un ietver būtiskāko risku uzskaitījumu šai lietotāju grupai. Padomi dalīti grupās tehniski ne pārāk zinošiem lietotājiem (15 ieteikumi) un papildus 7 ieteikumi zinošākiem lietotājiem. Padomi ietver gan vispārīgus ieteikumus, piemēram, pārrunāt ar bērniem datora un interneta lietošanu, gan ļoti tehniskus padomus, piemēram, veidot rezerves kopijas un pierakstīties uz drošības jaunumiem internetā. Iekļauts arī padoms, kas iesaka meklēt speciālista palīdzību. Kopumā šī nodaļa noslēpta salīdzinoši sarežģīta dokumenta vidū, un mērķauditorijai izmantojama tikai pastarpināti, ja tehniski un šo dokumentu zinošs padomdevējs to ierāda.

ISF Labās prakses standarts informācijas drošībai [ISFSt] (tālāk tekstā – ISF standarts) ir izstrādāts ar mērķi palīdzēt organizācijām ieviest informācijas drošības pārvaldību visos informācijas dzīves cikla posmos un visās IT izmantošanas vietās. ISF standarta uzbūve ir veidota, lai būtu ērta praktiskā piemērošanā, lai tas vienlaikus būtu arī izglītojošs materiāls. ISF standarts ietver sešus aspektus, kas katrs sastāv no vairākām tēmām:

- Drošības pārvaldība;
- Kritiskas uzņēmuma darbības lietojumprogrammas;
- Datoru instalācijas;
- Tīkli;
- Sistēmu izstrāde;
- Gala lietotāja vide.

Katra tēma ir sadalīta nodaļās, kas ietver principu jeb uzdevumu, kas jāpaveic, lai standarts būtu ievērots, un mērķi, kāpēc minētās darbības ir nepieciešamas.

Nodaļas par drošības politiku un drošības apzināšanos ir ietvertas Drošības pārvaldības aspektā. Kā informācijas drošības politikas nodaļas uzdevums ir noteikta nepieciešamība izstrādāt visaptverošu informācijas drošības politiku un izplatīt to visiem, kas izmanto organizācijas informāciju un sistēmas. Šīs nodaļas mērķis ir dokumentēt organizācijas vadības norādījumus informācijas drošības pārvaldībā un darīt to zināmu visiem, kam nepieciešams.

Drošības apzināšanās nodaļas uzdevums ir nodrošināt tādas aktivitātes kā drošības apzināšanās programmu, lai veicinātu drošības apzināšanos katram, kam ir piekļuves tiesības organizācijas informācijai un sistēmām. Mērķis šai nodaļai ir panākt, lai katrs zinātu un mācētu pareizi pielietot drošības vadīklas, kas paredzētas informācijas sargāšanai no neatļautas lietošanas vai izpaušanas.

ISF standarts ietver arī nodaļu Drošības izglītošana un apmācība, kas apraksta uzdevumu un mērķi, lai darbinieki mācētu izstrādāt un uzstādīt drošības vadīklas. Šī nodaļa vairāk paredzēta tieši IT speciālistiem, kas apkalpo sistēmas.

Nodaļa par informācijas risku analīzes veikšanu nosaka nepieciešamību veikt šādu analīzi, atbildīgās lomas un galvenos uzdevumus, pamatā koncentrējoties uz uzņēmuma darbībai kritiskām informācijas sistēmām. Savukārt nodaļa par informācijas risku analīzes metodoloģiju nosaka nepieciešamību izmantot kādu strukturētu metodoloģiju, lai nodrošinātu vienotu skatījumu visām uzņēmuma sistēmām.

Gala lietotāja vides aspekts ietver nodaļas, kas paredzētas lielu organizāciju attālinātu filiāļu informācijas drošības pārvaldības organizēšanai. Liela daļa no šī aspekta nodaļām var būt noderīga, lai izprastu informācijas drošības pārvaldības laukumu arī mājsaimniecībā.

Drošības politikai atsevišķa nodaļa šajā aspektā nav paredzēta, jo tā ir centralizēta visai organizācijai. Mazliet atšķirīgi šajā aspektā aprakstīta drošības apzināšanās nodaļa, kurā kā uzdevums minēts lietotājiem apzināties informācijas drošības svarīgākos elementus un to nepieciešamību, kā arī saprast katra personīgo atbildību par to ievērošanu. Mērķis ir pārliecināt lietotājus izmantot drošības vadīklas un pasargāt informāciju no nokļūšanas pie personām, kam tā nepienākas.

Nodaļa par lietotāju apmācību nosaka uzdevumu veikt apmācību sistēmu atbilstošā izmantošanā, drošības vadīklu izstrādē un piemērošanā ar mērķi nodrošināt lietotājiem prasmes aizsargāt sistēmas un veikt savus pienākumus informācijas drošībā.

Informācijas drošības pārvaldība nav jāsāk no tukšas vietas, pieredze ir uzkrāta un apkopota arī standartos. Lielāko daļu no tiem gan nebūs viegli izmantot mājsaimniecībā. Daļa ir pārāk sarežģīti, lai to izmantotu nespeciālists. Nereti standarta iegūšanas izmaksas ir pārāk lielas samērojumā ar ieguvumiem privātā vidē. Vispiemērotākais privātai videi varētu būt ISF standarts [ISFSt], tas ir veidots, lai būtu ērti praktiski pielietojams, turklāt ir pieejams bez maksas.

Tomēr tā īsti neviens standarts nepielāgotā veidā nav izmantojams ikdienas datorlietotājam bez specifiskām zināšanām. Ir nepieciešams vienkāršāks risinājums, mājsaimniecībai nepieciešams atšķirīgs informācijas drošības pārvaldības modelis.

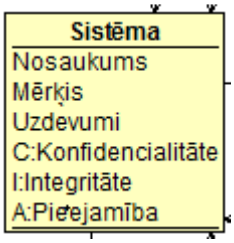
2.3. Informācijas drošības pārvaldības modelis uzņēmumam

Standarts ISO 27002 definē informāciju kā uzņēmuma aktīvu. Klasiskais skats uz informācijas drošību ir no organizācijas vai sistēmas skatupunkta. Arī citi standarti informācijas drošību apskata kā mērķi, kas jāsasniedz uzņēmuma informācijas sistēmai.

Kaut arī ir pētījumi [CRA08], kas iesaka drošībai būtiskos informācijas sistēmu izmantošanas posmos izvairīties no cilvēka klātbūtnes, izstrādājot sistēmas, kas spētu darboties bez cilvēka klātbūtnes. Tomēr ikdienas dzīvē cilvēks ir nozīmīgs informācijas sistēmu lietotājs. Un vairums standartu un drošības pilnveidošanas risinājumi paredzēti tieši cilvēku lietošanai.

Pārsvarā informācijas drošības standarti veidoti tekstuālā formātā. Lai atvieglotu informācijas drošības procesa uztveri, lietderīgi būtu to attēlot grafiska modeļa formātā. Balstoties uz [ISFSt] standartu, autore izstrādājusi formalizētu drošības pārvaldības modeli uzņēmumam. Standarta satura rādītājs pievienots 1. pielikumā. Modeļa izveides mērķis ir attēlot informācijas drošības procesa elementus organizācijā, lai tālāk varētu parādīt šo elementu pārgrupēšanos mājsaimniecības drošības procesā. Modelis veidots kā konceptuāla klašu diagramma [UML].

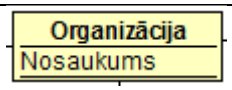
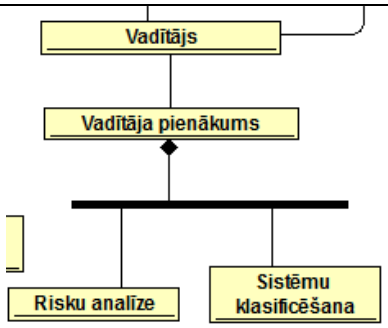
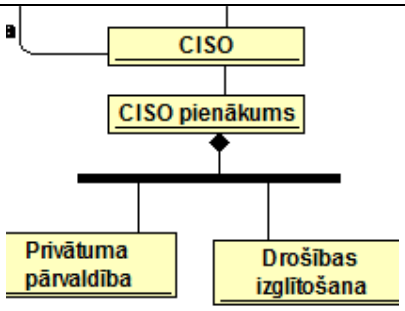
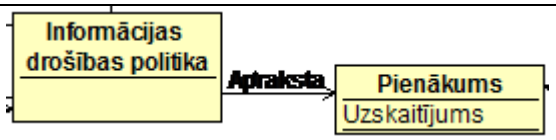
Organizācija izmanto vienu vai vairākas informācijas sistēmas, kas parasti atrodas informācijas drošības pārvaldības procesa centrā. Klasei "Sistēma" atribūti ir nosaukums, darbības mērķis un uzdevumi, kā arī drošības prasību līmenis konfidencialitātei, integritātei un pieejamībai (4. attēlā). Drošības prasības sistēmai raksturotas ISF standarta nodaļās SM3.1, CB1.1-CB2.6 (tālāk šajā nodaļā iekavās attiecīgo nodaļu numuri). Informācijas sistēma satur datus, kam tiek veikta rezerves kopēšana (CB4.4).



4. attēls. Informācijas sistēma – klase "Sistēma"

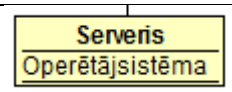
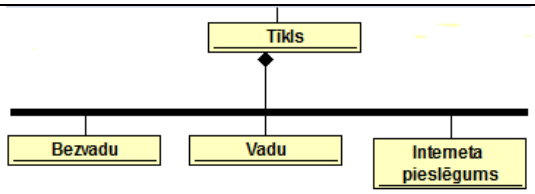
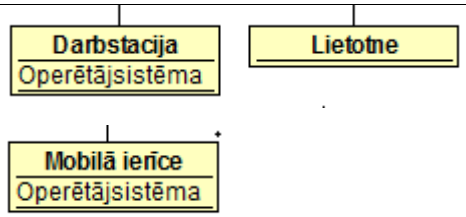
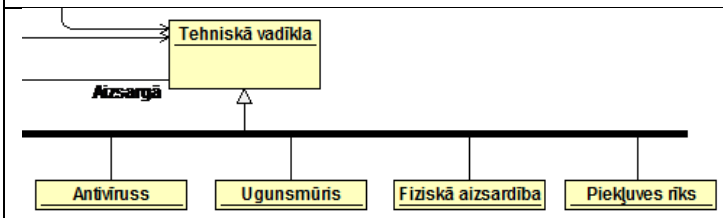
Pārējās klases veido trīs grupas. Pirmā no tām sastāv no organizācijas apraksta, drošības pārvaldības un lēmumu pieņēmēju klasēm. Katras klases apraksts sniegts 6. tabulā.

6. tabula. Organizācijas, drošības pārvaldības un lēmumu pieņēmēju klases

	Organizācijai uzdevumu veikšanai nepieciešamas informācijas sistēmas. Vadība apstiprina nepieciešamos pārvaldības dokumentus, t.sk. informācijas drošības politiku (SM1.1, SM1.2, SM2.1).
	Organizācija (departamentu vadītāji) pieņem lēmumus par sistēmu izvēli un pārvaldīšanu. Katrai sistēmai jābūt noteiktam īpašniekam, kas bieži ir tās struktūrvienības, kas ir galvenie sistēmas lietotāji, vadītājs. Sistēmas īpašnieks ir atbildīgs par piekļuves tiesību noteikšanu (SM3.2, SM3.3, CB1.1-1.3, CB2.1, CB3.1).
	Informācijas drošības pārvaldnieks (angliski – *Chief Information Security Officer* jeb CISO) nodrošina informācijas drošības politikas izveidi un attīstību, organizē drošības apzināšanās pasākumus, pārvalda informācijas privātuma nodrošināšanu (SM2.2, SM2.4, SM2.5, SM4.2).
	Informācijas drošības politika nosaka darbinieku, t.sk., administratora un lietotāja pienākumus, informācijas drošības vadīklas datorresursiem (SM1.2, SM1.3, CB, CI, NW, UE).

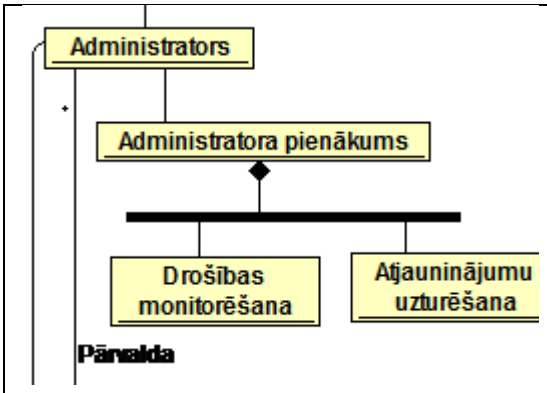
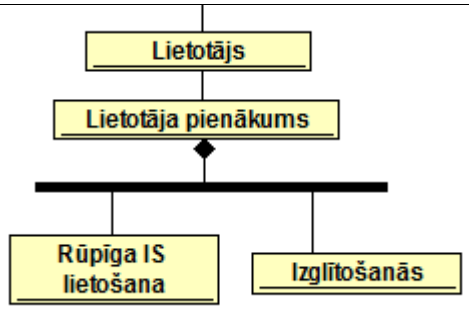
Otrā grupa aptver tehnoloģiskos rīkus: datorresursus un tehniskās drošības vadīklas, kas aprakstīti 7. tabulā.

7. tabula. Tehnoloģiskie rīki

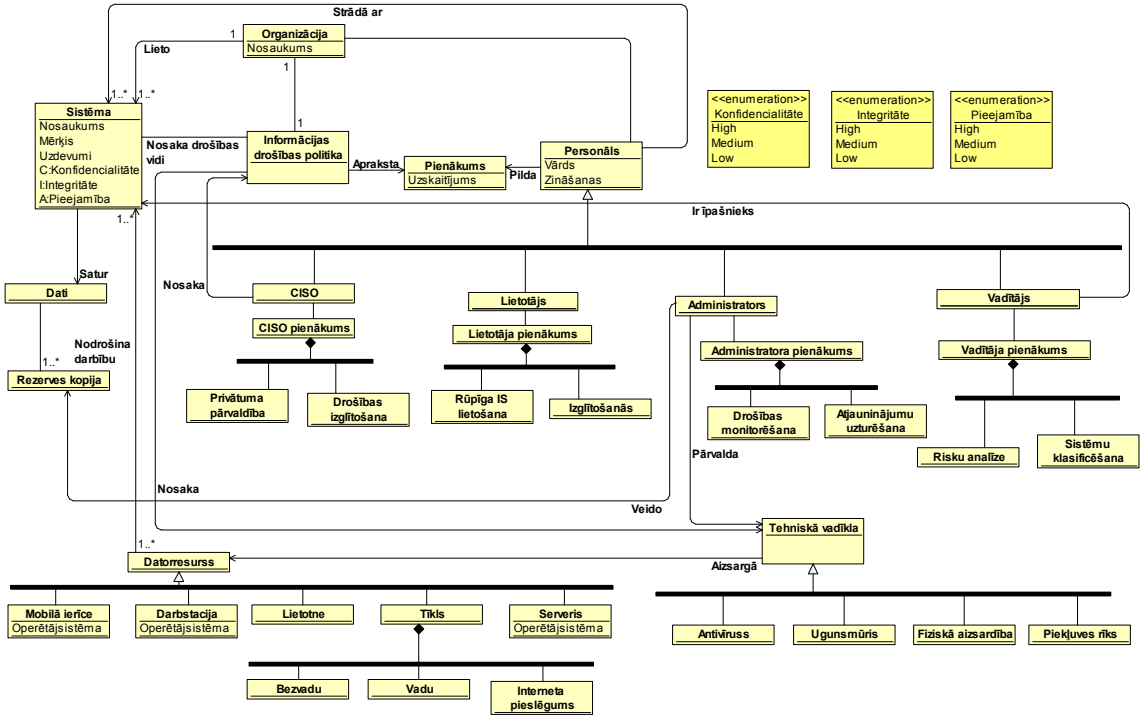
	Informācijas sistēmas parasti izmanto datorus ar īpašu uzdevumu – serverus. Serveri tiek izvietoti speciālās telpās, kurās nodrošināta atbilstoša fiziskā aizsardzība. Serveros lieto tiem piemērotas operētājsistēmas un nodrošina aizsardzību (CI).
	Datori ir savienoti tīklā, kam jābūt atbilstoši izplānotam un uzbūvētam. Tiek lietoti arī bezvadu tīkli, kā arī pieslēgums internetam (NW, UE5.4, UE5.6).
	Sistēmas lietotāju datori atrodas mazāk aizsargātā vidē nekā serveri. Tajos tiek izmantotas dažādas lietojumprogrammas. Nereti sistēmām var pieslēgties arī no mobilām ierīcēm (CB3.3, CI2.4, UE3, UE4).
	Informācijas sistēma, serveris, datortīkls un lietotāja darbstacija tiek aizsargāti ar dažādām drošības vadīklām. Noteikti tiek lietoti aizsardzības rīki pret kaitīgu programmatūru, t.sk. datorvīrusiem, ugunsmūris (CB2.2, CB3, CI2, CI4, UE5.1).

Trešā grupa ir personāls, t.sk., sistēmas administratori un lietotāji (8. tabula).

8. tabula. Sistēmas administratori un lietotāji

	Administrators veic drošības vadīklu uzstādīšanu un to izmantošanas pārvaldību. Nodrošina datu rezerves kopēšanu, atjauninājumu uzturēšanu un drošības notikumu monitorēšanu (CB2.1, CI1.1, NW1.1, CB2.3, CI3.3, NW3.2, CI1.3, CI1.4, CI2.2).
	Lietotājs lieto sistēmu (lietojumprogrammu). Svarīgi nodrošināt atbilstošu lietotāja izpratni par drošības jautājumiem (SM2.4, SM2.5, CB3, CI4).

Minētās klases kopā ar atbilstošām asociācijām veido informācijas drošības pārvaldības konceptuālo modeli (5. attēls).



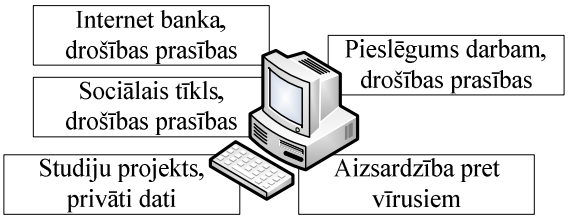
5. attēls. Informācijas sistēmas drošības procesa modelis

2.4. Modelis mājsaimniecībai

Vairāku autoru pētījumā [SIN07] secināts, ka inovācijas organizācijas struktūrā padara sarežģītāku drošības pārvaldību. Līdzīgi un varbūt pat sarežģītāk ir ar datoru mājās. Kamēr tas bija tikai pāris funkciju veikšanai, cilvēkam bija daudz vieglāk saprast gan tā lietojumu, gan apdraudējumus, gan piesardzības pasākumus.

Ir arī pētījumi [Web2.0], kas drošību analizē no servisu izstrādātāju puses. Kaut to sauc par *user-centric* jeb uz lietotājiem orientētiem tīmekļa servisiem, tomēr joprojām skatījums ir no sistēmas puses: "Web 2.0 ir visaptverošs (*umbrella*) jēdziens, kas ietver tehnoloģijas, ko izmanto, lai nodrošinātu lietotājiem tīmekļa servisus".

Šobrīd aizvien biežāk vienā darbstacijā (mājas datorā) darbojas dažādu uzņēmumu dažādas sistēmas ar dažādām prasībām drošībai (6. attēls). Tās var būt gan pieslēgums internetbankai, sociālo tīklu elementi, privāta informācija, darba devēja dati, u.c. Un lietotājs neprot salikt prioritātes starp dažādajām drošības prasībām. Nezināšanas dēļ liela daļa drošības ieteikumu netiek ievēroti.

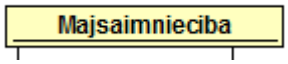
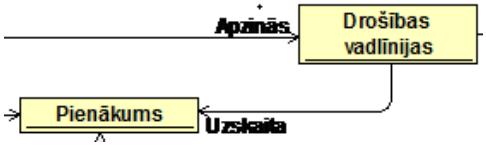


6. attēls. Drošības prasību daudzveidība

Sistemātisku informācijas drošības pārvaldību mājsaimniecībā apgrūtina šīs tēmas sarežģītība. Turpinājumā aprakstītā modeļa mērķis ir atvieglot minētās tēmas izprašanu ikdienas datorlietotājam.

Pārvaldības daļa (pirmā klašu grupa) mājsaimniecībā atšķiras būtiski (9. tabula). Tomēr parasti kāds ģimenē vai padomdevējs ārpusē ir vairāk zinošs un var ieteikt vadlīnijas pārējiem.

9. tabula. Mājsaimniecības pārvaldība

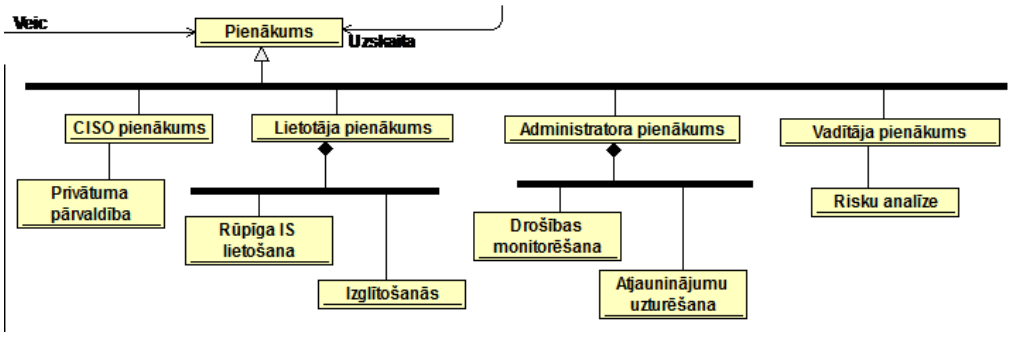
	Mājsaimniecība izmanto ikdienā tehnoloģiju priekšrocības.
	Drošības politika (mājsaimniecībā drīzāk – vadlīnijas), vadītājs un informācijas drošības pārvaldnieks nav strikti noteikti.

Atšķirības ir arī lietotāja un administratora lomās. Nereti lietotāju definē kā personu, kas lieto pilnībā sagatavotu datoru un programmatūru, jebkuru neskaidrību gadījumā meklē IT speciālista palīdzību. Ilgu laiku tika uzskatīts, ka sistēmas lietotājs ir būtiskākais sistēmas apdraudējums. Uz informācijas drošību parasti lūkojās no sistēmas skatupunkta.

Mājas datoru nereti uztver kā darbstaciju un līdz ar tu tās izmantotājus – par lietotājiem. Tehnoloģiju speciālisti lietotāju pamatā definē kā sistēmas ne pārāk zinošu (arī drošībā) "elementu", kas veic vienkāršas darbības, cenšas apiet drošības elementus, kas tam traucē, pie katras neskaidrības meklē padomu pie tehnoloģiju speciālista. Mājās tāds lietotājs papildus vēl grib arī atpūsties un piekļūt sociālajam tīklam, cik vien iespējams ātri.

Nereti mājas datorā strādā vairāki cilvēki, kas ir gan dažādu informācijas sistēmu lietotāji, gan savā ziņā rūpējas par pašu datoru, tā operētājsistēmu, pieslēgumu datortīklam, drošības programmatūru. Tradicionālajā modelī tos, kas rūpējas par tehnoloģijām un drošības risinājumu uzstādīšanu, sauc par administratoriem. Administrators ir tas "elements", kas vislabāk pārzina sistēmu, uzstāda un pārvalda drošības risinājumus, "cīnās" ar lietotājiem. Mājās dažreiz tiek izmantota speciālistu palīdzība programmatūras uzstādīšanā utml. Tomēr ikdienas rezerves kopiju veikšana tik un tā paliek pašam regulāri veicams darbs.

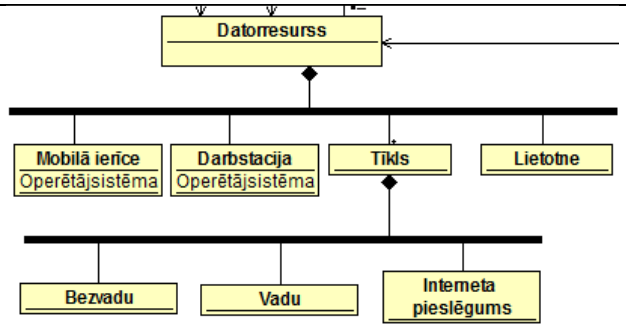
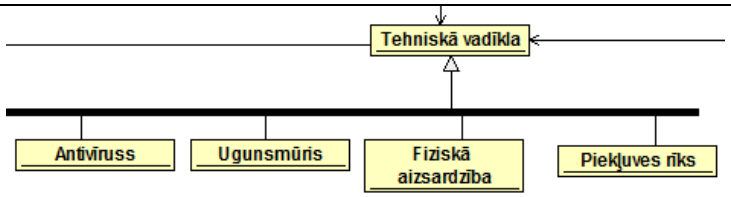
Kas tad varētu būt tas "elements", kas apvieno lietotāju un sistēmas administratoru? Autores publikācijā [IM09] definēts jauns jēdziens SASHE – *Security Aware Smart Household Employee*. SASHE apzinās drošības nozīmi un attiecīgi rīkojas, ir zinošs, darbojas mājās, savā ziņā ir "darbinieks". Tradicionālajā skatījumā uz informācijas sistēmu drošību starp lietotājiem un administratoriem ir neizbēgama viedokļu atšķirība, un SASHE ir risinājums, kā no šīs atšķirības veidot jauna līmeņa skatījumu. Ikdienas datorlietotājam mājsaimniecībā ir jāveic vairāk pienākumu nekā "parastam" lietotājam organizācijā (7. attēls), kā arī jāuzņemas atbildība (SM2.4, SM2.5, SM3.3, SM4.2, CI1.1, NW1.1, CI3.3, NW3.2, CI1.3, CI1.4).



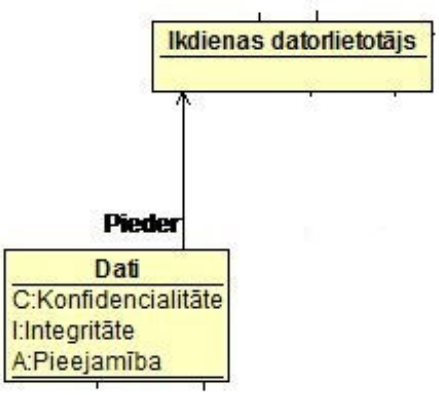
7. attēls. Ikdienas datorlietotāja pienākumi

Tehnoloģisko rīku grupa mājsaimniecībā pēc būtības sastāv no tādām pašām klasēm kā organizācijas modelī (10. tabula), izņemot serveri. Tomēr šo klašu instances ir salīdzinoši nelielas.

10. tabula. Tehnoloģiskie rīki mājsaimniecībā

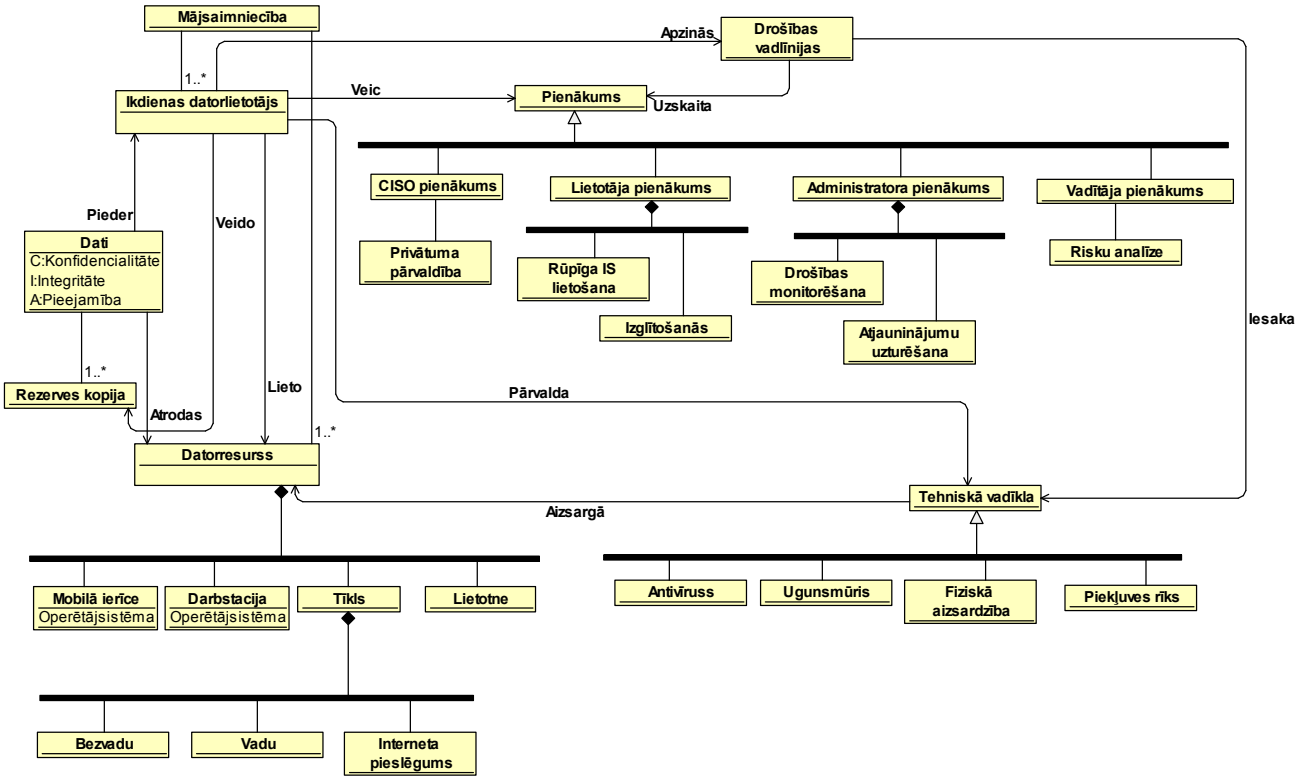
	Dators tiek izmantots līdzīgi kā lietotāja dators organizācijā. Mājas datorā lieto dažādas lietojumprogrammas. Mājas dators parasti ir pieslēgts internetam. Izmanto arī bezvadu tīklu, ko nodrošina īpašas ierīces (NW2.4, UE5.4, UE5.6, CB3.3, CI2.4, UE3, UE4).
	Mājas datorresursiem nepieciešamas atbilstošas drošības vadīklas. Noteikti tiek lietoti aizsardzības rīki pret kaitīgu programmatūru, t.sk. datorvīrusiem, ugunsmūris (CB2.2, CB3.3, CI2.4, CI4.5, UE5.1).

Ikdienas datorlietotājs kopā ar sev piederošiem datiem ir centrālais objekts mājsaimniecības drošības pārvaldības modelī (8. attēls).



8. attēls. Ikdienas datorlietotāja vērtības

Mājsaimniecības informācijas drošības pārvaldības modelis atainots 9. attēlā



9. attēls. Mājsaimniecības informācijas drošības procesa modelis

Aprakstītie modeļi var tikt izmantoti kā rīki mājas datorlietotāju drošības izglītošanas procesā, palīdzot izprast līdzības un atšķirības salīdzinājumā ar drošības pārvaldību organizācijās. To var izmantot gan datorspeciālisti, kas sniedz atbalstu mājsaimniecības datorlietotājiem, gan paši datorlietotāji, kas vēlas vairāk uzzināt par drošības pārvaldības elementiem un to savstarpējo saistību.

2.5. Informācijas drošības vadlīnijas mājsaimniecībai

Drošības politika ir pamats efektīvai informācijas drošības pārvaldībai. Uzņēmumos tas ir rīks, kā nodrošināt darbinieku pareizu attieksmi pret uzņēmuma informāciju. Izmantojot literatūras analīzi, lai novērtētu informācijas drošības politikas lomu lielās organizācijās, [QUI05] autori secina, ka informācijas nozīme organizācijas panākumu kaldināšanā aizvien pieaug, līdz ar to liela nozīme ir arī informācijas drošības politikai, kas nosaka informācijas pārvaldīšanas principus un noteikumus. Tomēr kvantitatīvi novērtēt šo ietekmi nav izdevies.

Tomēr drošības speciālisti ir pamanījuši, ka ir ļoti grūti pievērst darbinieku uzmanību drošības politikām un ievērot tās. Drošības personāls nepietiekamu uzmanību pievērš psiholoģijai. Informācijas drošības politikas dažreiz rada nopietnas emocijas. Cilvēkus šo politiku prasības var ļoti sadusmot [BOS02].

Drošības vadlīnijas mājsaimniecībai iespējams izveidot, izmantojot savu noderību uzņēmumos jau pierādījušu informācijas drošības standartu [ISFSt]. Standarta satura rādītājs pievienots 1. pielikumā.

Ne visas drošības prasības, kas svarīgas uzņēmumiem, ir nepieciešamas mājsaimniecībā. Turklāt arī nepieciešamo prasību sarežģītība atšķiras. Piemēram, sistēmu klasificēšana, dažādu tehnoloģisko vadīklu pārvaldība, uzņēmumā ir strukturēts process. Savukārt mājsaimniecībā tās var būt vienkāršas darbības. Mājsaimniecības vajadzību atšķirības no uzņēmuma parādītas 2. pielikumā. Tālāk šajā nodaļā izvērsts mājsaimniecības drošības pārvaldības vajadzību apraksts.

SM1.1 Vadības apņemšanās, SM2.4 Drošības apzināšanās, SM2.5 Drošības izglītība/apmācības: ikdienas datorlietotāja drošības apzināšanās nepieciešamība aprakstīta 3. nodaļā. SM1.2 Informācijas drošības politika: aizsargāt datorresursus, lai tos neizmantotu citas personas ļaunprātīgām vajadzībām. SM4.2 Informācijas privātums: informācijas drošības vadlīniju mērķis mājsaimniecībā ir aizsargāt ģimenes informāciju elektroniskā vidē no nesankcionētas lietošanas. CI1.1 Lomas un pienākumi: attēloti mājsaimniecības informācijas drošības pārvaldības modelī (6. attēls, 8. attēls).

SM3.1 Informācijas klasificēšana, SM3.2 Īpašumtiesības, SM4.3 Vērtību pārvaldība, CB1.1 Konfidencialitātes prasības, CB1.2 Integritātes prasības, CB1.3 Pieejamības prasības, UE3.1 Darbvirsmas lietojumprogrammu inventarizācija: mājsaimniecībā nepieciešama izpratne, kura informācija ir svarīga, ja datoram ir vairāki

lietotāji, jāsadala tiesības. Rezultāts klasificēšanai ir izvēlēts risinājums darbībai CB4.4 Rezerves kopēšana un izpratne, kuru informāciju nevajadzētu pubiskot.

SM3.3 Informācijas riska analīzes process, SM3.4 Informācijas riska analīzes metodes: risku analīze sniedz nozīmīgu informāciju, kuras no drošības procesa darbībām ir svarīgākās, risku novērtēšanas metode mājsaimniecībai un rīks aprakstīti 4. nodaļā.

SM5.2 Ļaunprogrammatūras aizsardzības programmatūra, SM5.6 Ielāpu pārvaldība, CB3.3 Darbstaciju aizsardzība, CI3.6 Ielāpu pārvaldība, NW2.2 Ugunsmūri, NW2.4 Bezvadu piekļuves: lai sasniegtu mērķi aizsargāt datorresursus, noteikti nepieciešamas tehniskās drošības vadīklas.

SM6.3 E-pasts, CB3.1 Piekļuves kontrole, CB3.2 Lietojumprogrammu pierakstīšanās process: ikdienas datorlietotājs attālināti piekļūst daudzveidīgām sistēmām, kam ir dažādi piekļuves kontroles risinājumi, paroļu utml. instrumentu pārvaldība ir svarīgs drošības procesa elements.

CI3.1 Darbs ar datoru ārējām ierīcēm, UE4.2 Rokas ierīces, UE4.3 Portatīvās glabāšanas ierīces, SM4.5 Fiziskā aizsardzība: nedrīkst aizmirst arī par fizisko drošību, kas jo īpaši būtiski ir viegli pazaudējamām lietām kā USB atmiņas kartes, fotoaparāti, mobilie telefoni.

2.6. Nodaļas secinājumi

Informācijas drošības pārvaldība uzņēmumos ir aprakstīta vairākos standartos un citos modeļu veidos. Dažādām vajadzībām ir iespējams piemeklēt piemērotu modeli. Mājsaimniecībai paredzētu informācijas drošības pārvaldības modeli autorei atrast neizdevās.

Parādīta uzņēmuma informācijas drošības pārvaldības modeļa transformācijas iespēja uz modeli mājsaimniecībai. Izstrādāto modeli var izmantot lietotāju izglītošanas procesā.

Uzņēmuma informācijas drošība pārvaldības procesā skaidri ir sadalītas lomas, atbildība un veicamie uzdevumi. Ir noteikta drošības politika. Mājsaimniecībā ikdienas datorlietotājs faktiski pilda dažādas lomas, bet atbildība nav skaidri noteikta.

Lai sistematizētu drošības pārvaldību mājsaimniecībā, lietderīgi ir izmantot Informācijas drošības vadlīnijas. Šīs vadlīnijas kalpo kā veicamo uzdevumu pārskats un atgādinājums neaizmirst svarīgus darbus.

3. INFORMĀCIJAS DROŠĪBAS APZINĀŠANĀS

3.1. Nodaļas mērķi

Gan standarti [ISFSt, ISO27002], gan publikācijas grāmatās [BOS02] ietver lietotāja rīcību kā nozīmīgu elementu informācijas tehnoloģiju drošības nodrošināšanā.

Lielākais apdraudējums bieži nav datorlauzis (*hacker*), bet – paša lietotāja kļūda. Tehnoloģijas pašas nevar novērst to neprasmīgas izmantošanas radītas problēmas. Beidzamo gadu laikā dažāda veida informācijas zādzības, nejaušas nozaudēšanas ir kļuvušas par bieži aprakstītu tematu mēdijos. Speciālisti strādā risinājumu meklējumos šīs problēmas novēršanai. Starp svarīgākajiem soļiem šīs problēmas risināšanā ir lietotāju izglītošana un informācijas drošības apzināšanās veicināšana [PWC13].

Informācijas drošības apzināšanās kā nozīmīgs informācijas tehnoloģiju drošības pārvaldības virziens strauji attīstās. Tomēr ir kāda nozīmīga nianse, kas nereti netiek ņemta vērā izglītošanas pasākumos – tiek aizmirsts, ka informācijas sargāšanā elektroniskā vidē cilvēkam nav uzkrāta pieredze. Piemēram, kā pareizi rīkoties ar atklātu liesmu vai piesargāties no bīstamiem dzīvniekiem, cilvēks uzsāk mācīties agrā bērnībā. Pieaugušais attiecīgās situācijās pareizi rīkojas intuitīvi. Pieaugušais arī māk rūpēties par informācijas aizsardzību, kamēr tā ir fiziski aptaustāma, piemēram, nez vai ģimenes fotoalbumi tiks izdalīti katram pretimnācējam. Toties cilvēku pieredze informācijas aizsardzībā elektroniskā jeb datorvidē tikai tagad veidojas.

Nodaļā aprakstīti informācijas drošības apzināšanās elementi un attiecīgo pasākumu veiksmes faktori. Analizēti pētījumi minētajā jomā, drošības apzināšanās programmas izveides ieteikumi uzņēmumam, labās prakses attīstība pasaulē un Latvijā, kā arī sniegts pārskats par pieejamiem informācijas drošības pārvaldības un izglītošanās rīkiem.

Promocijas darba rezultāti veidoti kā ieteikumu kopums pareizai rīcībai, piedāvājot rīku, ko var lietot tie, kas vēlas. Datorlietotāja faktisko rīcību var ietekmēt dažādi faktori [HOW12], ir arī metodes, kā piespiest jebkuru datorlietotāju patiešām rīkoties, bet šie aspekti ir ārpus šī darba tvēruma.

3.2. Informācijas drošības apzināšanās elementi

Informācijas drošības apzināšanās ir salīdzinoši jauns jēdziens, kas attīstās līdzās izpratnei, ka par IT izmantošanas riskiem atbildība jāuzņemas lietotājiem, tehnoloģiju speciālistus izmantojot tikai kā izpildītājus tehnisku darbu veikšanā. Saskaņā ar ISF standartu drošības apzināšanās ir pakāpe, cik lielā mērā darbinieki saprot informācijas drošības nozīmīgumu, nepieciešamo drošības līmeni, kas vajadzīgs organizācijai, un katra personīgos pienākumus [ISFSt].

Drošības apzināšanās veicināšanas procesam var izdalīt trīs līmeņus: datorlietotājs zina, kā vajadzētu pareizi rīkoties, datorlietotājs saprot, kāpēc tā rīkoties ir pareizi, datorlietotājs attiecīgi rīkojas.

[WOL10] apskata dažādas drošības apzināšanās (*security awareness*) definīcijas, analizējot to dažādību un piedāvājot savu variantu: "Drošības apzināšanās ir zināšanu par informācijas drošību izplatīšana tik lielā mērā, lai tās veicinātu drošības prasību ievērošanu." ("*Security awareness is the effort to impart knowledge of or about factors in the security of information to the degree that it influences behavior to adhere to policy*.").

Organizācijas darbinieki ir visizdevīgākais rīks aizsardzībai pret drošības apdraudējumiem. Tieši darbinieku rīkošanās atbilstoši drošības politikai vai to neievērojot, var uzlabot vai pasliktināt drošības situāciju. Drošības apzināšanās ir galvenā sastāvdaļa organizācijas informācijas drošības programmā. Daži avoti ziņo, ka šim uzdevumam ir atvēlēts pat 40% no visiem informācijas drošībai atvēlētajiem resursiem [BRI00].

Ja organizācijas personālam ir labas spējas sajust drošības apdraudējumu un savlaicīgi rīkoties, lai to novērstu, potenciālie zaudējumi var būt daudz mazāki vai pat nekādi. Drošības apzināšanās veicināšanas mērķis ir veidot spēju intuitīvi rīkoties atbilstoši situācijai.

Drošības apzināšanās procesa elementi ir [BOS02, *Chapter* 29]:

- kritiskie veiksmes faktori,
- drošības apzināšanās programmas izstrādes pieeja,
- apzināšanās principi,
- saturs,
- paņēmieni,
- rīki,
- novērtēšana un resursi.

Kritiskie veiksmes faktori ietver šādus elementus:

- informācijas drošības politika,
- augstākās vadības atbalsts un piedalīšanās,
- apzināšanās programmas koncentrēšanās uz skatījumu, ka drošība ir cilvēku problēma,
- mērķi (īsa termiņa, vidēja termiņa un tālāki),
- atbilstība mērķauditorijai,
- motivēšanas paņēmieni.

Laba informācijas drošības politika nosaka mērķus un atbildības, atļautās un aizliegtās aktivitātes, kā arī sodus par neatbilstību. Atbilstošā vadības līmenī apstiprināta informācijas drošības politika parāda organizācijas attieksmi pret šo tēmu. Drošības apzināšanās politika var būt gan informācijas drošības politikas sastāvdaļa, gan atsevišķi noteikta. Tai jānosaka katram darbiniekiem obligātu piedalīšanos šajā programmā, piemēram, jaunam darbiniekam pirms uzsākt darbu, ir jāapgūst noteikta programma. Savukārt, katram darbiniekam reizi gadā (vai biežāk, ja organizācijas specifika to prasa) ir jāveic drošības apzināšanās veicināšanas programmā noteiktās darbības.

Jābūt noteiktam, kurš ir atbildīgs par drošības apzināšanās programmas īstenošanu. Veiksmīgākas ir programmas, kuru īstenošanās sadarbojas tehnoloģiju speciālisti un apmācību vai personāla vadības speciālisti.

Latvijas Republikas likumdošanā ir noteikta nepieciešamība regulāri izglītot visus darbiniekus ugunsdrošībā un darba drošībā, bet informācijas drošībā šobrīd darbinieku izglītošanas prasības ir noteiktas tikai valsts [ITDL].

Augstākās vadības atbalsts ir svarīgs, gan atvēlot atbilstošus resursus, gan nodrošinot drošības personālu, gan arī ar faktisko rīcību, ievērojot drošības politikas noteiktos ierobežojumus.

Daudzi tehnoloģiju speciālisti uzskata datoru drošību par tehnoloģisku problēmu. Tomēr datoru drošība un jo īpaši plašākā nozīmē – informācijas drošība – ir cilvēku problēma. Aizvien vairāk datoriem esot saslēgtiem globālos tīklos, tīkla drošība kļūst lielā mērā atkarīga no katra lietotāja rīcības. Klasiskais drošības bauslis "drošība ir tikai tik stipra, cik vājākais posms" daudzlietotāju globāli savienotā datortīklā prasa, lai aizvien vairāk lietotāju kļūtu izglītotāki un līdz ar to "drošāki".

Drošības apzināšanās programmas mērķis ir mainīt informācijas un datoru lietotāju izturēšanos, lai aizvien vairāk informācijas drošībai svarīgas aktivitātes kļūtu par ikdienas rutīnas vai pat intuitīvas rīcības elementiem.

Drošības apzināšanās nav apmācība. Apmācība ietver daudz plašāku izglītošanu tehniskos paņēmienos, lai darbinieks varētu strādāt efektīvāk.

Ir svarīgi, lai drošības apzināšanās programma būtu pielāgota konkrētas mērķauditorijas uztverei. Programmas mērķi visām auditorijām ir līdzīgi, tomēr to sasniegšanas metodes un paņēmieni atšķirsies. Programmatūras izstrādes nodaļas darbiniekus uzrunās pavisam citāda pieeja nekā, piemēram, klientu apkalpošanas speciālistus. Turklāt dažādām auditorijām ir dažāda iepriekšējā pieredze.

Ārpus organizāciju vides ļoti plaša datorlietotāju auditorija mūsdienās ir bērni un jaunieši. Tieši šīs auditorijas atbilstošai uzrunāšanai atvēlēti nozīmīgi Eiropas Savienības resursi [SInt]. Arī Latvija piedalās šajā programmā, un jau vairākus gadus veiksmīgi darbojas droša interneta projekts [NetS].

Motivēšanai jābūt veiklai un piemērotai. Ja cilvēki uzskata, ka būt datorlauzim (*hacker*) ir forši, anti-hakeru ziņa netiks sadzirdēta. Svarīgs ir arī tāds elements, kā uzticēšanās ziņas nesējam. Internetā ir pieejami daudzveidīga informācija ar dažādām "drošības ziņām", bet tās netiek sadzirdētas. Piemērota institūcija, kuras teiktajam uzticētos Latvijas iedzīvotājs, drīzāk jāmeklē starp izglītības iestādēm vai sabiedriskām organizācijām.

3.3. Saistītie pētījumi

Galvenais elements informācijas drošības apzināšanās procesā ir cilvēks – skaidrojošās informācijas adresāts. Ja šī informācija ir nepietiekama vai nav atbilstoši pozicionēta, cilvēki turpina izpaust personīgu informāciju sociālos tīklos. Analizētas vairākas hipotēzes par informācijas izpaušanas saistību ar sociālā tīkla izmantošanas paradumiem. Secinājumi iekļauj arī apgalvojumu, ka par privātuma aspektiem labāk informēti studenti retāk izpauž personīgu informāciju sociālos tīklos [YOU09].

[BRY09] pievēršas jauniešu rīcībai, kas nezināšanas dēļ izpauž privātu informāciju internetā. Ir pieejami raksti par jauniešu izglītošanu, t.sk. skolās. Skolas ir daudz izmantota vide pētījumiem. [WOL10] tika analizēti kādas skolas darbinieku paroļu veidošanas paradumi, mērot paroļu sarežģītību pirms izglītošanas, kā arī pēc vairākām informēšanas

akcijām. Lai paroļu sarežģītību pārbaudītu, tika ievēroti vairāki nosacījumi, lai pārbaudes process, t.i., paroļu uzlaušana, nebojātu kopējo drošības līmeni. Pirmā informēšanas akcija bija prezentācija ar vispārēju informāciju par paroļu veidošanas nosacījumiem un labu un sliktu paroļu piemēriem, uzlaušanas laiku demonstrējumiem, otrā – e-pasts visiem darbiniekiem ar atgādinājumu nomainīt paroli, trešā – iznirstošais logs pieslēgšanās laikā ar jautājumu, vai parole nomainīta, bet ceturtā – kampaņa ar aicinājumu mainīt paroles. Pirms informēšanas tikai 44% paroļu atbilda noteiktajām prasībām, pēc pirmā informēšanas 55% paroļu bija atbilstošas, turpmāk atbilstība pieauga tikai par dažiem procentiem. Noderīgākais pētījuma secinājums ir, ka, informējot datorlietotājus par drošības prasībām un izskaidrojot tās, faktiskā rīcība uzlabojas. Diemžēl veikt līdzīgus pētījumus plašākam lietotāju lokam ir apgrūtinoši, jo testiem jānotiek ļoti kontrolētā vidē, turklāt visiem dalībniekiem ir jāuzticas testu veicējiem.

[SZE09] sniedz vispārēju priekšstatu par ikdienas datorlietotāju drošības vēlmēm, attieksmi un zināšanām par šī brīža apdraudējumiem internetā. Pētījums veikts 2008. gadā Austrālijā, aptaujājot 23 personas un izmantojot atvērtus jautājumus. Starp secinājumiem minēta nozīmīgu atšķirību esamība starp datorlietotāju attieksmi Lielbritānijā, kur bijis veikts līdzīgs pētījums, un Austrālijā. Austrālijā attieksme ir daudz izprotošāka, kas tiek skaidrots ar Austrālijā veiktām izglītojošām kampaņām masu medijos. Raksts noslēdzas ar secinājumu, kam pilnībā pievienojas arī autore. Jāuzlabo gan datoru pārdevēju sniegtais atbalsts, gan jāsniedz informācija masu medijos. Kaut tehnoloģiju speciālisti un nereti arī paši datorlietotāji sevi mēdz uzskatīt par naiviem un nezinošiem, saņemot pareizu skaidrojumu, liela daļa var uzstādīt un izmantot nepieciešamos drošības pasākumus, līdz ar to samazinot personu skaitu, kas kļūst par upuriem noziedzīgiem nodarījumiem internetā ("*The predominant outcome of this study identified that the support computer retailers, the media, and vendor literature should be improved upon. Whilst the study targeted self rated naïve individuals, it appears that individuals are reasonably capable of operating a computer and applying safeguards to a point. It is the belief of the author that if better quality support information was readily available then this could significantly minimise the number of individuals becoming victims to Internet crimes*." [SZE09]).

Pētījuma [ATK09] autori, analizējot jauniešu zināšanas par interneta apdraudējumiem un atbilstošu rīcību, konstatējuši neviendabību. Dažās jomās konstatētas labas zināšanas, pamatā saistībā ar uzvedību un attiecībā Internetā, tomēr tehnoloģiskiem drošības aspektiem veltītā uzmanība ne vienmēr ir atbilstoša.

Ir virkne rakstu par datorlietotāju zināšanu un uzvedības pētījumiem atsevišķās valstīs. Pamatā aptaujātas salīdzinoši nelielas personu grupas (daži desmiti). Starp secinājumiem bieži tiek minēta nepieciešamība vairāk informēt sabiedrību par apdraudējumiem, veidojot plašas kampaņas. Autorei neizdevās atrast risinājumu, kas piedāvātu nepieciešamo drošības informāciju pielāgot katra atsevišķa datorlietotāja vajadzībām. Ir veikti pētījumi, meklējot iespējas novērtēt drošības apzināšanās līmeni organizācijās [MEE09], nozīmīgi datu avoti parasti ir organizāciju iekšējā dokumentācija, intervijas ar darbiniekiem.

[TAL10] apstiprina autores novērojumus, ka lielākā daļa datorlietotāju izglītošanas stratēģijas un pasākumi ir vērsti uz organizāciju darbinieku izglītošanu, un tikai nedaudzas valstis ir veikušas aktivitātes mājas datorlietotāju izglītošanā. Veicot aptaujas, konstatēts, ka cilvēki saņem informācijas drošības izglītošanu vietās, kur šādu apmācību nepieciešamību nosaka tiesību akti. Lai pārbaudītu, vai zināšanas, kas apgūtas darba vietā, ir iespējams pielietot, un tiek pielietotas arī mājās, tika veikts pētījums. Pētījumā tika uzrunāti nedaudz vairāk nekā 300 dalībnieku, kas pamatā meklēti, izmantojot [TAL10] autoriem pieejamas e-pasta adreses.

Starp pētījuma mērķiem bija: izprast respondentu vispārējo drošības izpratni; noskaidrot, vai un kādu drošības apmācību viņi saņēmuši; noskaidrot saistību starp saņemto apmācību un faktisko rīcību. Tika analizēta drošības izpratne, faktiskā situācija darba vietā un faktiskā situācija mājās. Apmēram puse atbildējušo novērtēja savu drošības apzināšanās līmeni kā augstu vai ļoti augstu. Augstais rādītājs neraksturo situāciju sabiedrībā kopumā, jo tika uzrunātas personas no autoru paziņu loka. Taču pētījumam, vai apmācība darbā palīdz izvēlēties pareizo rīcību mājās, nozīmīgs skaits darbā apmācību personu ir noderīgs. Starp secinājumiem nozīmīga daļa nepārsteidz, piemēram, gandrīz visi zina, kas ir datorvīruss, par ko runā jau gadiem, bet tikai daži zina zombēto tīklu (*botnet*) jēdzienu. Kopumā ir konstatēta pozitīva saistība, ka personas, kas saņēmušas izglītošanu darbā, labāk zina, kā rīkoties arī mājās. Promocijas darba autore ir novērojusi šādu saistību arī savā praksē. Turklāt nelielā pētījumā (31 dalībnieks) vienas organizācijas ietvaros saņemts apstiprinājums, ka, organizācijas drošības apzināšanās pasākumos iekļaujot arī ziņas, kas svarīgas mājas vidē, labāk tiek izprasta ar organizācijas informācijas drošības politika.

Arī [KRI10] autori norāda, ka drošības izglītošana darba vietā palīdz labāk izprast šos jautājumus arī privātā vidē.

Organizācijās drošības apzināšanās sastāv no divām daļām – izglītojošas informācijas un prasību izpildīšanas, t.sk. drošības politikas vai procedūru ievērošana. Mājas lietotājiem situācija ir pavisam atšķirīga. Ja vēl atsevišķi izglītojoši materiāli ir pieejami, tad obligāta iepazīšanās ar tiem un sekošana padomiem nav nodrošināma.

Pētījuma autori piedāvā definēt apzināšanās nodrošināšanas modeli E-AM (*Electronic Awareness Model*), kas sastāv no izglītošanas daļas (KO darīt) – speciāla portāla un izpildes daļas (KĀ darīt) – padomiem, kā rīkoties. Izglītošanas daļa būtu papildināta ar iespējām pārbaudīt savas zināšanas. Portāla uzturēšana būtu jānodrošina organizācijai, kuru mājas lietotājs noteikti izmanto, piemēram, Interneta pakalpojuma sniedzējs vai banka [KRI10].

Tomēr piedāvātais modelis ir tikai teorētisks, un tā iedzīvināšanai ir saskatāmi daudzi apgrūtinājumi, gan pakalpojumu sniedzēju nevēlēšanās, gan lietotāju neizpratne. Tiek ieskicēti iespējami juridiski risinājumi, izglītošanas pienākumu nosakot kā obligātu Interneta pakalpojumu sniedzējam. Autori plāno izveidot piedāvātā modeļa prototipu un pārbaudīt to skolu vidē.

Visi autorei zināmie pētījumi, kas saistīti ar datorlietotāju izglītošanu drošības jomā, rāda šādas izglītošanas pozitīvus ieguvumus. Ir izmantotas atšķirīgas metodes izglītošanai un šo pasākumu novērtēšanai ne vienmēr ir iespējams ļoti precīzi aprēķināt pozitīvā ieguvuma lielumu, bet tas konstatēts vienmēr.

Vieglāk ieguvumu novērtēt slēgtā vidē, piemēram, organizācijā vai skolā. Biežāk lietotā novērtēšanas metode ir aptaujas rezultātu analīze. Ir pamats uzskatīt, ka informācijas drošības izglītošana sabiedrībai ir vajadzīga un noderīga.

3.4. Drošības apzināšanās programma uzņēmumā

Informācijas drošības apzināšanās veicināšanas kampaņa ir līdzīga tādām kampaņām kā izglītošana par smēķēšanas vai alkohola lietošanas kaitīgumu studentu kopmītnēs. Plānošana šādam pasākumam ir svarīga un ietver gan programmas mērķu noteikšanu, gan klausītāju loka identificēšanu, gan komunicējamās informācijas definēšanu, gan klausītāju ieguvumu aprakstīšanu. Izpēti var veikt gan ar novērojumiem, gan pētījumiem, gan testiem, gan intervijām. Ja organizācija veic sistemātisku drošības incidentu uzskaiti, tad noderīgu informāciju var sniegt šo incidentu analīze.

Tā kā informācijas drošības apzināšanās ir ļoti cieši saistīta ar ikdienas dzīvi, vērtīgs informācijas avots ir arī ziņu portāli. Ja par kādu drošības apdraudējumu vai aspektu vairāk runā mēdiji, ir ļoti iespējams, ka ir vērts šo ziņu atbilstošā noformējumā komunicēt arī organizācijas ietvaros.

Arī pašas programmas plānošana ir svarīga, plānam jāietver vismaz informāciju par līdz šim paveikto, jaunās programmas mērķus un to sasniegšanas līmeņa vērtēšanas metode, kā arī, protams, konkrētām paredzētajām aktivitātēm un atbildīgajām personām.

Drošības apzināšanās veicināšanas pasākumos jāņem vērā apzināšanās principi [BOS02]:

- uzmanības pievēršana,
- pievilcīgums mērķauditorijai,
- vienkārši un atmiņā paliekoši,
- ieinteresēt nevis piespiest,
- pašreizējs (*current*),
- uzticības cienīgs (*credible*),
- turpinošs (*continuing*).

Uzmanības pievēršana pozitīvā nozīmē var notikt ar pareizi izvēlētu attēlu vai saukļu palīdzību. Vairākas organizācijas izvēlas šim uzdevumam īsu organizācijas prezidenta vai citas augstas amatpersonas videouzrunu. Pārsvarā šādi rīki tiek veidoti organizācijas iekšējām vajadzībām. Tomēr dažus piemērus var iepazīt [InSec].

Programmai jābūt pievilcīgai mērķauditorijai, tai jāietilpst tās vērtību kopumā. Šī mērķa sasniegšanai ir svarīgi precīzi novērtēt un sadalīt mērķauditorijas grupas.

Kaut tehnoloģiju speciālistiem un nereti arī citiem, kas daudz lasa par jaunākajiem apdraudējumiem, var likties, ka ir svarīgi visiem pastāstīt par tiem visiem, drošības apzināšanās programmas ziņām jābūt vienkāršām un atmiņā paliekošām. Jāņem arī vērā, ka cilvēkiem ir dažāda uztvere, daļai labāk paliek prātā skaitļi, daļai – teksts, bet daļai attēli vai skaņa. Vēl labāk ir kombinēt vairākus no informācijas attēlošanas veidiem.

Laba organizācijas informācijas drošības politika prasa, lai dalība drošības apzināšanās aktivitātēs būtu obligāta. Tomēr būtu labi arī šo obligāto dalību atbalstīt ar ieinteresēšanu, nevis tiešu piespiešanu.

Vienu informācijas drošības apzināšanās materiālu nevajadzētu izmantot pārāk ilgi. Materiālam jābūt atbilstošam pašreizējai (*current*) situācijai. Konkrētais izmantošanas

ilgums ir atkarīgs no organizācijas lieluma un līdz ar to katras atsevišķas kampaņas garuma. Labi būtu, ja katrai kampaņai izmantotu svaigu materiālu. Organizējot informācijas drošības apzināšanās pasākums plašākai sabiedrībai un, izmantojot publicēšanu internetā, nereti tiek uzkrāti arī iepriekšējie materiāli. Kas ir pozitīvi, jo dažādas lietotāju grupas dažādā laikā atrod savu ceļu līdz drošības jautājumu izpētei. Tomēr par portālu kopumā jārada iespaids, ka tas ir aktuāls.

Drošības apzināšanās programmai jābūt uzticības cienīgai (*credible*) un saskaņotai ar reālo dzīvi. Ja darbiniekam ikdienā jālieto 15 dažādas paroles, tad prasīt, lai tās visas atceras no galvas, nav pareizi. Daudz vērtīgāk būs iemācīt izveidot atbilstoši aizsargātu pierakstīto paroļu sarakstu. Savukārt, privātā vidē jo īpaši, ir svarīgi atšķirt, kad parolei labāk būt sarežģītai un pierakstītai, nevis vienkāršai, lai tikai varētu atcerēties.

Drošības apzināšanas kampaņas materiālam jābūt svaigam, tomēr katra jauna ziņa jeb drošības paņēmiens līdz intuitīvai pielietošanai nonāk tikai pēc vairākiem atkārtojumiem. Apzināšanās veicināšanas programmai jābūt ilgtermiņa, ar dažādiem ziņu atkārtojumiem.

Apskatāmie riski katrā reizē būs atšķirīgi un atbilstoši pašreizējai organizācijas situācijai un ārējiem faktoriem, piemēram, vīrusi, privātuma apdraudējums vai neapdomīga organizācijas konfidenciālas informācijas publiskošana. Risku apskatu ar lielāko prieku sagatavos informācijas tehnoloģiju speciālisti, tomēr jāatceras, ka sekmīgai programmas uztverei ar risku daudzumu nedrīkst pārspīlēt. Apskatāmajiem riskiem jābūt saistītiem ar mērķauditorijas vajadzībām. Ja darbiniekiem ir atļauts strādāt ar organizācijas dokumentiem privātā mājas datorā, tad svarīgi ir runāt par riskiem, kas apdraud datoru ārpus organizācijas datortīkla. Savukārt, ja darbs ar informāciju notiek tikai organizācijas telpās, bet datori pieslēgti internetam, svarīgi vērst uzmanību uz riskiem, ka robeža, līdz informācija var tikt nejauši publiskota, ir ļoti trausla.

Galvenie pretpasākumi ir jāsaista ar iepriekš apskatītajiem riskiem. Pretpasākumi ietver procedūras drošai informācijas sistēmu lietošanai un ziņošanu par drošības starpgadījumiem.

Drošības apzināšanās programmai jāuzsver, ka drošība ir katra atbildība. Organizācijā, kur vadība noteikusi drošību par prioritāti, skaidri saprotams, ka katram darbiniekam ir atbilstoši pienākumi. Apzināšanās programma palīdz saprast, kādu tieši rīcību drošības jomā vadība sagaida no katra darbinieka.

Katram darbiniekam jāzina, kā pareizi reaģēt uz konstatētu incidentu. Uzņēmumos varētu būt noteiktas gan rīcības procedūras, gan kontaktpersonas. Autores pieredze drošības incidentu pārvaldīšanā ietver gan ļoti precīzi organizētas procedūras, gan risinājums, kuros liela nozīme ir lietotāju izpratnei pareizā lēmuma pieņemšanā.

Kopš 2011. gada 1. februāra ir spēkā Informācijas tehnoloģiju drošības likums [ITDL], kas valsts un pašvaldību iestādēm nosaka pienākumu reaģēt uz informācijas drošības incidentiem. Minētais likums paredz arī ne retāk kā reizi gadā veikt institūcijas darbinieku instruktāžu informācijas tehnoloģiju drošības jautājumos.

Privātajā vidē formālu prasību informācijas tehnoloģiju drošībai Latvijā nav. Atbalstu tehnoloģisku problēmu, galvenokārt, pieejamības ierobežojumu, risināšanā atbalstu nodrošina interneta pakalpojuma sniedzējs. Taču drošības incidentos, kas saistīti ar paša lietotāja datora vai tajā esošo informāciju, skaidru rīcības scenāriju nav. Šis fakts būtiski palielina paša lietotāja drošības apzināšanās nozīmi.

Privātā vidē atbildība par informācijas drošību jāuzņemas katram pašam. Situācijā, kad nav ne likumdošanas prasības, ne pietiekamas vēsturiskas pieredzes, paši iedzīvotāji tikai ļoti retos gadījumos varētu nonākt līdz mūsdienu situācijai atbilstošas informācijas drošības apzināšanās līmenim. Izglītošanas aktivitātes ir tradicionālas skolai, t.i. vecuma grupai līdz apmēram 20 gadiem. Bet elektronisku informāciju aizvien pieaugošā apjomā lieto dažādās vecuma grupās. Drošības apzināšanās veicināšana ir nepieciešama visiem. Konkrētu pasākumu realizācijā būtu jāņem vērā arī psiholoģiskie aspekti. Tie ir atsevišķu pētījumu lauks.

Visvienkāršākā drošības apzināšanās programmas novērtēšanas metode ir saskaitīt dalībniekus, kas noklausījušies semināru. Ar anketēšanu papildus ir iespējams novērtēt arī dalībnieku apmierinātību.

Lai novērtētu, ko darbinieki ir iemācījušies, izmanto dažādus testus. Tomēr svarīgākais mērķis drošības apzināšanās veicināšanas programmai ir darbinieku faktiskās rīcības maiņa. Un šī mērķa sasniegšanas novērtēšana ir sarežģīta. Viena no metodēm ir analizēt drošības incidentus, tomēr paļauties uz šiem mērījumiem nevar. Pēc aktīvas drošības apzināšanās veicināšanas programmas reģistrēto incidentu skaits pieaug, jo darbinieki labāk māk tos saskatīt un zina, kur par tiem jāziņo.

3.5. Informācijas drošības apzināšanās labās prakses attīstība

Lai mazinātu tehnoloģiju izmantošanas iespējamās ēnas puses, svarīgi ir iespējami ātrāk apgūt visjaunākās tehnoloģijas un savlaicīgi sagatavot atbilstošus speciālistus, kā arī iesaistīt šos sagatavotos speciālistus atbilstošo tehnoloģiju pārvaldībā un sabiedrības izglītošanā.

Viens no iemesliem, kāpēc Latvijā universitātēs netiek piedāvātas atsevišķas programmas informācijas drošībā, ir atbilstošu resursu trūkums. Tomēr studentiem tiek piedāvāti vairāki studiju kursi par dažādām ar informācijas drošību saistītām tēmām. Tāpat studenti tiek aicināti pētīt informācijas drošības jautājumus gan izstrādājot kursa darbus, gan bakalaura darbus, gan maģistra darbus. Beidzamo gadu studentu darbu vidū ļoti populāras bijušas tēmas par *WiFi* tīklu drošības jautājumiem, drošības aspektiem programmatūras izstrādē, kā arī drošības jautājumi tikuši pētīti citu tēmu ietvaros. Sekmīgi aizstāvēts arī pētījums par drošības apzināšanās programmas izstrādi, tās rezultātu novērtējumu.

Par drošības apzināšanos runā un raksta vairākas nozīmīgas organizācijas. OECD vadlīnijas apraksta deviņus pamatprincipus ar mērķi veicināt šīs apzināšanās lomu demokrātiskā informācijas sabiedrībā. [OECD02]. Aģentūra ENISA apkopo informāciju un piedāvā materiālus īpašās grupās gan pensionāriem, gan mazajiem uzņēmumiem, tomēr to pielietošanas veicināšana ir atstāta dalībvalstu ziņā [ENISAAR].

Savas darbības ietvaros 2008. gada februārī ENISA izveidoja Apzināšanās celšanas kopienu (*The Awareness Raising Community*), kurā piedalīties aicināti eksperti ar interesēm veicināt informācijas drošības apzināšanos savās organizācijās. Kopš 2008. gada maija šajā kopienā darbojas arī autore. Kopiena darbojas vairākos virzienos, no kuriem redzamākie ir materiāli ar padomiem dažādām mērķauditorijām un informācijas apkopošana par drošības apzināšanās veicināšanas aktivitātēm dalībvalstīs. Starp materiāliem ir tādi kā videoklipi, plakāti, ekrānsaudzētāji. Daļa no materiāliem apkopoti grupā speciāli vecākiem.

Eiropas Savienībā nozīmīgu pienesumu informācijas drošības veicināšanā nodrošina programma *Safer Internet plus* [SInt], kuras mērķi ir paaugstināt drošību interneta un citu jauno tehnoloģiju lietošanā, jo īpaši jaunatnes un bērnu vidū.

Drošības apzināšanās aktivitātēs iesaistās arī dažas korporācijas. *Microsoft* ir viena no pirmajām, kas runā ne tikai par tehnoloģijām un datora aizsardzību, bet arī par lietotāju personīgo drošību. Ir izstrādāti un publicēti vairāki izglītojoši materiāli. Tomēr līdzīgi kā

daudzkārt, arī šie materiāli veidoti universāli, un lēmuma pieņemšanas process, kuri padomi ir būtiski konkrētam lietotājam, atstāts pašplūsmā.

[AUS10] apkopota informācija par situāciju Austrālijā kibernoziegumu jomā. Materiālā ietvertas arī rekomendācijas, kas iesaka izglītot informācijas tehnoloģiju patērētājus. Pagaidām tas ir tikai plāns, tomēr šī uzdevuma atrašanās uz likumdevēju darba galda noteikti veicinās jomas attīstību.

Autorei ir bijusi iespēja dzirdēt atsevišķu lielu uzņēmumu pieredzes stāstus, kā tiek veikta darbinieku izglītošana informācijas drošībā ar mērķi apmācīt, kā aizsargāt mājas datoru. Šādu uzņēmumu darbiniekiem noteikti ir labāks priekšstats un prasmes savas ģimenes informācijas sargāšanā. Lai gūtu priekšstatu, cik plaši šādu drošības apzināšanās veicināšanas mērķi izmanto citur, pēc autores iniciatīvas organizācija ISF veica ātro aptauju savu biedru vidū. Tika saņemtas atbildes no 18 uzņēmumiem, kas nedēļu ilgušai tiešsaistes aptaujai vasaras vidū ir labs radītājs. Vairākums atbildējušo bija no finanšu sektora, tādējādi netieši apstiprinot, ka informācijas drošība tieši finanšu sektorā ir starp būtiskiem jautājumiem. 75% veic regulāru savu darbinieku izglītošanu, izmantojot gan seminārus, gan tiešsaistes apmācību sistēmas, gan atsevišķas publikācijas uzņēmuma intranetā, pārsvarā izmantojot vairākas no minētajām metodēm. 61% no atbildējušajiem iekļauj informācijas drošības apzināšanās programmā tematus par mājas datora aizsardzību, un vēl 17% apsver šādu iespēju. Kā iemeslus šīs tēmas iekļaušanai lielākā daļa min, ka tas paaugstina vispārējo drošības apzināšanās līmeni. Daļai aptaujas dalībnieku kā svarīgākais iemesls ir vēlme pasargāt sava uzņēmuma informāciju, kas dažreiz var tikt apstrādāta arī privātās elektroniskās ierīcēs. Aptaujas dalībnieki sniedza arī vispārīgus komentārus. Noderīgākie no tiem bija šādi: drošības apzināšanos ir grūti izmērīt, jo, piemēram, pēc drošības apzināšanās veicināšanas semināriem nereti novērojams reģistrēto incidentu skaita pieaugums, kas saistīts ar lietotāju uzlabojušos spēju incidentus atpazīt; drošības apzināšanās veicināšanas programmai jābūt personiski uzrunājošai; nedrīkst kampaņas materiālu būt par daudz, kas var tikt uztverti gandrīz tikpat negatīvi kā mēstuļu plūsma e-pastā; pēc iespējas jālieto dažādi informēšanas kanāli, jo daļai patīk lasīt ziņojumus, bet citiem – skatīties video.

Dažādie pieejamie materiāli sniedz daudzveidīgas atbildes un padomus, kā pasargāt sevi no dažādiem apdraudējumiem. Bet pārsvarā tie stāsta par katru apdraudējumu atsevišķi. Visaptverošs skats informācijas drošības pārvaldībai mājas datora līmenī īsti nav redzams.

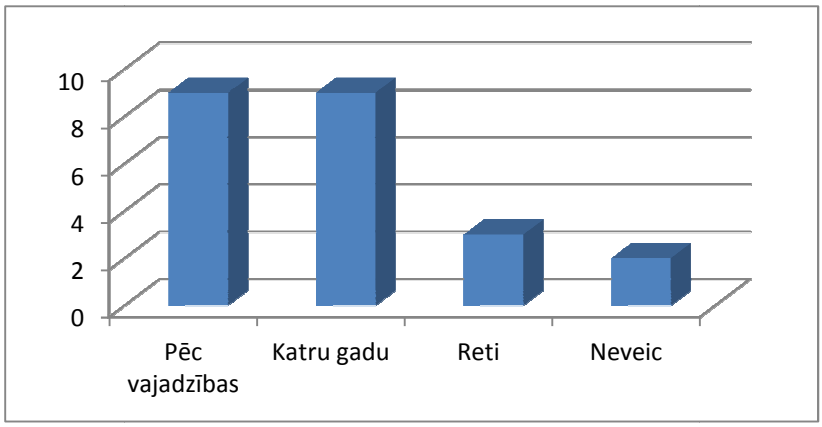
3.6. Informācijas drošības apzināšanās Latvijā

Ar devīzi "Mēs atbildam par savu drošību informācijas tehnoloģiju laikmetā" 2011. gada maijā darbu uzsācis portāls Esidrošs.lv [ED]. Portāla veidošanu organizē un to uztur Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. Materiālus portālam veido jomas speciālistu komanda.

Viena no redzamākajām drošības apzināšanās veicināšanas aktivitātēm Latvijā ir Droša interneta projekts, kas ir daļa no ES droša interneta programmas, tomēr šobrīd jau attīstās arī plašāk. "Projekts ir vērsts uz bērnu, jauniešu, skolotāju un vecāku informēšanu un izglītošanu interneta satura drošības jomā – par iespējamajiem draudiem internetā (naida kurināšana, rasisms, bērnu pornogrāfija un pedofilija, emocionāla pazemošana internetā, personas identitātes zagšana un datu ļaunprātīga izmantošana)" [NetS].

Savukārt pieaugušo vidē jauna iezīme drošības apzināšanās virzienā ir šīs tēmas parādīšanās izklaidējošos žurnālos. Raksts "No sava hakera neaizbēgsi" žurnāla "Klubs" 2010. gada augusta numurā atgādina gan par nepieciešamību veidot datu rezerves kopijas, gan piesardzību, lai nepazaudētu izmērā nelielos, bet informācijas daudzuma ziņā ietilpīgos datu nesējus, kā arī atgādina par nepieciešamību katram pašam vērtēt savus riskus.

Darba autore veica ekspromtaptauju foruma Baltic IT&T 2010 CIO sesijas dalībniekiem, kur piedalījās apmēram 50 uzņēmumu informācijas tehnoloģiju vadītāji. Semināra laikā tika lūgts atbildēt uz anketas jautājumiem par rīkiem un risinājumiem, kādus uzņēmumi lieto darbinieku informācijas drošības apzināšanās attīstībai. Tika saņemtas 23 aizpildītas anketas. Lielākā daļa jeb 21 aptaujas dalībnieks vismaz dažreiz veic informācijas drošības apzināšanās aktivitātes, aktivitāšu biežumu skatīt 10. attēlā. Tikai seši aptaujas dalībnieki atļauj strādāt ar uzņēmuma informāciju mājas datorā, gandrīz neviens neļauj to darīt citās privātās elektroniskās ierīcēs. Savukārt, par mājas datoru aizsardzību neko nestāsta lielākā daļa (61%) aptaujāto. No tiem, kas darbiniekus apmāca mājas datora aizsardzībā, vairāk nekā puse piedāvā iespēju saņemt individuālas konsultācijas pie uzņēmuma IT drošības speciālistiem.



10. attēls. Cik bieži veic informācijas drošības apzināšanās aktivitātes

Līdzīgi kā informācijas drošības pārvaldībā kopumā arī darbinieku informācijas drošības apzināšanās veicināšanā labi piemēri meklējami bankās. Vairākas no lielām komercbankām izmanto tiešsaistes apmācību un zināšanu pārbaudes programmas, kas centralizēti izstrādātas lietošanai filiālēs dažādās valstīs.

Lai drošības apzināšanās veicināšanas programma būtu veiksmīga, ir svarīga pareizo paņēmienu izmantošana. Tādu kā attēli, stāsti, piemēri, pārsteigumi, humors, auditorijas iesaistīšana u.c. [BOS02]. Darba autore ir vadījusi dažādus drošības apzināšanās veicināšanas seminārus. Pārsvarā Latvijā, taču dažus arī citās valstīs vai citu tautību auditorijai. Starp secinājumiem, kas gūti no šīs pieredzes, minams, ka veiksmes faktors noteikti ir auditorijai, organizācijas kultūrai vai valstij raksturīgu piemēru izmantošana. Jo īpaši tas ir svarīgi, uzrunājot sākumā ne visai ieinteresētus klausītājus.

Starp biežāk lietotajiem rīkiem jāmin internets vai uzņēmuma intranets, prezentācijas, ekrānsaudzētāji, plakāti, videoziņojumi, raksti, semināri, pasākumi un dāvanas u.c. [BOS02]. Salīdzinoši vienkārši ir izveidojami raksti par dažādiem drošības aspektiem, bet to iedarbība ir ne visai efektīva bez papildus atraktīvākiem pasākumiem. Spēles ir salīdzinoši labs rīks, taču to kvalitatīvai izveidošanai nepieciešami lieli resursi.

3.7. Informācijas drošības pārvaldības un apzināšanās veicināšanas rīki

Viens no pirmajiem, kas runā ne tikai par datora drošību, bet arī par tā lietotāju – cilvēku personīgo drošumu (*safety*), ir kompānija Microsoft. Šī kompānija ir izveidojusi un publicējusi vairākus izglītojošus materiālus. Aģentūra ENISA izstrādājusi dažādus materiālus [ENISAAR]. Latvijā aktīvi darbojas projekts Drošsinternets [NetS] un portāls Esi drošs [ED]. Autores vadībā ir izstrādāti vairāki kursa darbi, kas ietver izpēti gan par

pieejamajiem izglītojošajiem materiāliem informācijas drošībā, gan lietotāju zināšanu līmeni. Kursa darbu ietvaros izstrādāti un publicēti arī izglītojoši materiāli.

Darba "Mājas datorlietotāja izglītošana" [PUR09] mērķis ir "izpētīt, cik lielā mērā cilvēki ir informēti par datora drošību, un izanalizēt dažādu pamācību pieejamību internetā. Izanalizēt cik daudz, un, vai vispār mājas datorlietotājiem ir pieejama apmācība interneta vietnēs datora drošības jautājumos.". Lai sasniegtu mērķi, tika veikta lietotāju aptauja par viņu zināšanām datoru drošībā, un izpēte, cik daudz izglītojošu materiālu par informācijas drošību internetā varētu atrast parasts lietotājs, kas nedaudz orientējas darbā ar meklētājprogrammu *Google*.

Lielākā daļa aptaujāto cilvēku norādīja, ka zināšanas par datoru drošību ieguvuši skolā vai datoru apmācības kursos. Tomēr gan skolas informātikas programmā, gan kursos, kas orientēti uz lietošanas prasmju apguvi, drošības jautājumiem pievērsta pavisam maza uzmanība, aprobežojoties ar aizsardzību pret vīrusiem un paroļu lietošanu. Paveicies ir tiem datoru lietotājiem, kuru draugu vai paziņu lokā ir kāds, kas vismaz mazliet orientējas arī informācijas drošības jautājumos. Lietotāji tika aicināti atbildēt arī uz jautājumu "Kādas problēmas Jums bija gadījušās ar datoru?". Populārākā atbilde bija "vīrusi". Iespējamie iemesli šim apdraudējumam meklējami lietotāju rīcībā:

- "62% lejupielādē nepazīstamus failus no interneta;
- 46% lieto svešus datu nesējus, pirms tam neskenējot ar jebkādu antivīrusa programmatūru;
- 26% sāknē pielikumus no nepazīstamajiem e-pastiem, 16% to dara dažreiz;
- 19% neizmanto ugunsmūri;
- 13% ver vaļā nepazīstamus e-pastus, 34% to dažreiz dara;
- 7% nelieto antivīrusa programmatūru, 9% to nekad neatjauno" [PUR09].

Otrs darba [PUR09] uzdevums bija izanalizēt, kādas vietnes par informācijas un datoru drošības jautājumiem ir pieejamas internetā. Uzdevuma veikšanai tika izmantota meklētājprogramma, materiāli tika meklēti latviešu, krievu vai angļu valodās. Tālākai analīzei tika izvēlētas 12 vietnes, izmantojot kritērijus:

- atrašanās pirmajās *Google* lappusēs;
- manāmas pazīmes par drošības informācijas esamību;
- nerada nedrošuma sajūtu (pārlieku daudz reklāmkarogu, uzlecošo reklāmu, kuras netīšām atverot var iegūt vīrusus).

Katrai no izvēlētajām vietnēm tika aprakstīta tajā atrodamā informācija, vērtēts valodas stils, kā arī izdarīti secinājumi. Rezultāti tika apkopoti (11. attēls).

	INFORMĀCIJA									
LAPA	UGUNSMŪRIS	VĪRUSI	PROGRAMMAS SPIEGI	E_PASTA DROŠĪBA	FAILU LEJUPIELĀDĒŠANA NO INTERNETA	VECĀKU KONTROLE	PAROLES UN LIETOTĀJVĀRDI	REZERVES KOPIJAS	PAPILDUS INFORMĀCIJA	APRAKSTS
1.	-/+	+	-	-	-	-	-	-	Drošības brīdinājumi, atjauninājumi	Viegls, saprotošs
2.	+/-	+/-	-	+/-	+/-	-	+/-	+/-	Pieejas kontrole, failu šifrēšana	Stāstījuma veidā, ne pamācošs
3.	-/+	-/+	-	-/+	-	-	-/+	-	Kriptogrāfija, pieejas kontrole, IT infrastruktūras un vides drošība, komunikācijas drošība	Nabadzīgs, tikai definīcijas
4.	-/+	+/-	-	-	-	-	-/+	-/+	Datu šifrēšana, servisi, fiziskā drošība	Sarežģīts
5.	-	+/-	-	+/-	-	-	+/-	-	Datu un HDD aizsardzība, arhīvi, datora traucējumi	Pietiekami vienkāršs
6.	+	+	+	+	+	+	+	+	Datu aizsardzība, drošība tiešsaites, informācijas zagšana	Plašs, saprotams
7.	+	+	+	+	+	+	-	+	Atjauninājumi, datora uzturēšana, bezvadu tīkls	Plašs, saprotams
8.	-	-	-	-	-	+/-	-	-	Personas datu drošība	Vienkāršs
9.	-/+	-/+	-	-/+	-/+	-	-	-	Draudi Internetā un iemesls tiem	Vienkāršs
10.	-	+/-	-	-	-	-	-/+	-/+	Personisko datu aizsardzība, kopēšanas tiesības	Vienkāršs
11.	-	-	-	-	-	+	-	-	Bērnu un vecāku apmācība darbam Internetā	Video veidā
12.	+	+/-	-	+/-	-	-	-	-	Bezvadu tīkls, personas datu zagšana	Vienkāršs

Apzīmējumi: + (informācija ir), +/- (vidējais informācijas daudzums), -/+ (nepilnīga informācija), - (informācijas nav).

11. attēls Interneta resursu analīze [PUR09]

Viens no būtiskākajiem apkopojošajiem secinājumiem saka, ka ir pieejama informācija par katru svarīgu drošības lietu, tomēr visbiežāk tā atrodama par katru atsevišķi – vienā lapā ir par rezerves kopiju veidošanu, citā par bezvadu tīklu drošību, utt. [PUR09] autorei neizdevās atrast vietni, kur ērtā un parastam lietotājam saprotamā veidā vienkopus būtu pieejama pilnīga informācija par visiem vai vismaz lielāko daļu datoru drošības aspektiem.

Tomēr katra informācija par datoru un informācijas drošību var izrādīties kādam noderīga, tāpēc dažādu materiālu veidošana, jo īpaši latviešu valodā, ir atbalstāma. Vienam nelielam apdraudējumam tehnoloģijas *Bluetooth* drošībai veltīts izglītojošs materiāls izstrādāts un publicēts bērnu vidū vienā no biežāk lietotajiem portāliem par drošību internetā [KRU10].

Darba "Drošības politikas izstrāde mājas datorlietotājam" mērķis bija "Izstrādāt drošības politiku mājas datorlietotājam, kurā aprakstīts, kā rīkoties, lai aizsargātu savu mājas datoru. Padarīt šo materiālu viegli pieejamu." [MAZ09].

Arī [MAZ09] ietvaros tika veikta lietotāju aptauja. Tālākai analīzei noderīgākie secinājumi:

- "56% aptaujāto vienu paroli izmanto vairākās vietās;
- 73% paroles maina tikai tad, kad tas tiek prasīts;
- 45% aptaujāto nekad netaisa rezerves kopijas saviem failiem;
- 34% nezina, vai atjauno antivīrusa programmatūru vai nē, vai arī nekad to neatjaunina;
- 40% aptaujāto neskenē e-pasta pielikumus no nezināmiem avotiem;
- 56% neskenē e-pasta pielikumus no zināmiem avotiem (draugiem, paziņām);
- 16% nezina, kā skenēt e-pasta pielikumus;
- 47% aptaujāto mājās ir bezvadu internets un no tiem 49% nav aizsargājuši savu bezvadu internetu (manījuši noklusēto lietotājvārdu un paroli utt.) vai arī nezina, kā to darīt."

Ļoti svarīgi jebkuram izstrādājamam materiālam izvēlēties pareizu mērķi. Diezgan daudz materiālu par informācijas vai datoru drošību drīzāk izskatās izstrādāti ar mērķi "gribu pastāstīt, kādi apdraudējumi ir iespējami", nevis, domājot par potenciālā lasītāja interesēm.

Izstrādājamās drošības politikas mērķi bija izvēlēti šādi:

- "Veicināt drošības apzināšanos – pastāstīt, kādēļ drošība ir svarīga un iepazīstināt ar draudiem mājas datoriem.
- Dot zināšanas – informēt, kā samazināt riskus un aizsargāt savu mājas datoru.

- Dot padomus ikdienas lietošanai – sniegt ieteikumus, kādi piesardzības pasākumi jāievēro, strādājot ar datoru." [MAZ09]

Viens no darba mērķiem bija padarīt izstrādāto politiku pieejamu, tā publicēta emuārā [MD09]. Ieskatu izveidotajā materiālā skatīt 12. attēlā. Emuārā ir iespējas ievietoto tekstu komentēt, kā arī šo komentāru vietu izmantot, lai uzdotu jautājumus. Tomēr šī iespēja ir vērtīga tikai tad, ja kāds komentārus analizē un jautājumus atbild. Uzturēt vietni nebija kursa darba uzdevums.

12. attēls. Drošības ceļvedis

3.8. Nodaļas secinājumi

Ar tehnoloģiskiem aizsardzības rīkiem ir izrādījies par maz. Daudzveidīgi sociālās inženierijas rīki tiek lietoti ar mērķi izvilināt dažādu informāciju. Līdz ar to risinājums jāmeklē plašāk. Informācijas drošība vairāk nekā agrāk kļūst par tematu, kas tiek diskutēts ne tikai datorzinātnes un matemātikas ietvaros. Risinājuma meklējumos sadarbojas dažādu

jomu profesionāļi. Biežāk starp nozarēm, kas iesaistās, minētas ekonomika un psiholoģija [AND09].

Tai pašā laikā no personas skatupunkta raugoties, par drošību nereti domā kategorijās "vai antivīrusa programmatūru uzstādīji". Uzņēmējdarbības vidē informācijai nereti ir vismaz aptuveni izmērāma vērtība naudas izteiksmē, bet šāda domāšana netiek attiecināta uz personīgo informāciju. Privātai informācijai bieži ir vairāk emocionāla vērtība, tomēr nevērīga rīcība ar personīgo informāciju var radīt arī finansiālus zaudējumus, piemēram, tiek izkrāpta nauda.

Ikdienas lietotājs izmanto savu mājas datoru, lai pieslēgtos privātam e-pastam, darba dēvēja datortīklam, internetbankai, internetveikalam un tiešsaistes sociālajam tīklam. Gandrīz katrs glabā privātas fotogrāfijas un interesantus vai svarīgus dokumentus datorā. Mobilie telefoni aizvien vairāk kļūst par daudzfunkcionālām iekārtām, bet mājas datori tiek pieslēgti dažādiem, t.sk. bezvadu tīkliem.

Vairākos materiālos par drošības apzināšanos šis process tiek dalīts trīs posmos: zināt, saprast un rīkoties. Ar dažādas informācijas pieejamību var vairot zināšanas. Speciālās akcijās ar izskaidrojošu materiālu pielietošanu var uzlabot sapratni. Tomēr rīcība joprojām paliks paša lietotāja darbība. Un darbība būs atbilstošāka, ja par tās veikšanas iemesliem būs izpratne un tā nodrošinās labumu pašam lietotājam.

Datorlietotāja faktisko rīcību var ietekmēt dažādi faktori, kas atrodas ārpus šī promocijas darba pētījuma robežām. Darba rezultāti veidoti kā ieteikumu kopums pareizai rīcībai, piedāvājot risinājumu tiem, kas vēlas, bet neiekļauj metodes, kā nodrošināt, lai jebkurš datorlietotājs tiešām rīkotos atbilstoši.

4. INFORMĀCIJAS DROŠĪBAS RISKU NOVĒRTĒŠANA

4.1. Nodaļas mērķi

Statistisku datu par dažādiem apdraudējumiem ir daudz. Arī atsevišķu izglītojošu materiālu netrūkst. Visu izlasīt nav iespējams, bez pamatizglītības attiecīgajā jomā liela daļa ir grūti saprotama. Kā to visu salikt "kopīgā bildē"?

Informācijas drošības pārvaldības labā prakse ietver risku novērtēšanu kā būtisku elementu, kas palīdz izvēlēties piemērotākos aizsardzības risinājumus. Privātā vidē pārsvarā tiek izmantotas intuitīvas dažādu risku vērtēšanas metodes, kas balstītas iepriekšējā pieredzē. Bet elektroniskās informācijas risku jomā pieredze ir uzkrāta pavisam maz, un tā visbiežāk nav sistematizēta.

Ikdienas datorlietotājam ir gandrīz neiespējami orientēties plašajā informācijas tehnoloģiju apdraudējumu klāstā. Turklāt viens un tas pats apdraudējums, piemēram, datorvīrusa iekļūšana datorā, var izraisīt dažādus riskus, piemēram, datorā glabāto datu pazaudēšana vai sabojāšana vīrusa darbības rezultātā. Tehnoloģiju eksperti sniedz vispārējus ieteikumus, kas paredzēti visiem un jebkurai tehnoloģijai. Katram ikdienas datorlietotājam ir dažāda attieksme pret riskiem jeb riska tolerance, tāpēc vienādi risinājumi aizsardzībai pret apdraudējumiem visiem nederēs. Balstoties uz [NISTRM, 8 lpp.], autore informācijas drošības risku ikdienas datorlietotājam definē kā nevēlamas sekas, kas varētu iestāties, apdraudējumam izmantojot ievainojamību.

Nodaļā aprakstīta darba autores izstrādāta informācijas drošības risku novērtēšanas metode ikdienas datorlietotājam, kas ietver jomas ekspertu sagatavotas informācijas un paša datorlietotāja sniegtu atbilžu izmantošanu. Aprakstīta arī metodes aprobācija, izmantojot tīmekļa lietojumprogrammas prototipu.

4.2. Risku novērtēšanas metode

4.2.1. Vispārīgs pārskats

Autore ir izstrādājusi informācijas drošības risku novērtēšanas metodi privātai videi. Lai novērtētu riskus, tiek analizēta elektroniskā vide un ikdienas datorlietotāja rīcība. Elektroniskā vide ietver ikdienas datorlietotāja vai mājsaimniecības datoru ar pieslēgumu

internetam un to izmantošanas mērķus. Ikdienas datorlietotājam ir sava attieksme pret riskiem, kas tiek ņemta vērā, nosakot riska līmeni. Datorā tiek lietotas tehniskas drošības vadīklas, bet datorlietotāja prasmes, zināšanas un rīcība ir organizatoriskas drošības vadīklas. Metode ir izstrādāta, balstoties uz autores piecpadsmit gadu pieredzi dažādu ar IT izmantošanu saistītu risku vērtēšanā un NIST ceļvedi [NISTRM].

Ņemot vērā privātā vidē pieejamo pieredzes apjomu, potenciālo apdraudējumu un ievainojamību aptverošu analīzi nodrošina eksperti, balstoties uz dažādu avotu datu apkopojumiem. Lietotājam jāsniedz atbildes uz vienkāršiem jautājumiem par datora izmantošanas mērķiem un izmantojamajām sistēmām. Drošības pilnveides ieteikumi tiek veidoti kā padomu saraksts. Risku pārvaldīšanas metode var būt izpratnes vairošanas rīku arī jebkuram elektroniskas informācijas lietotājam.

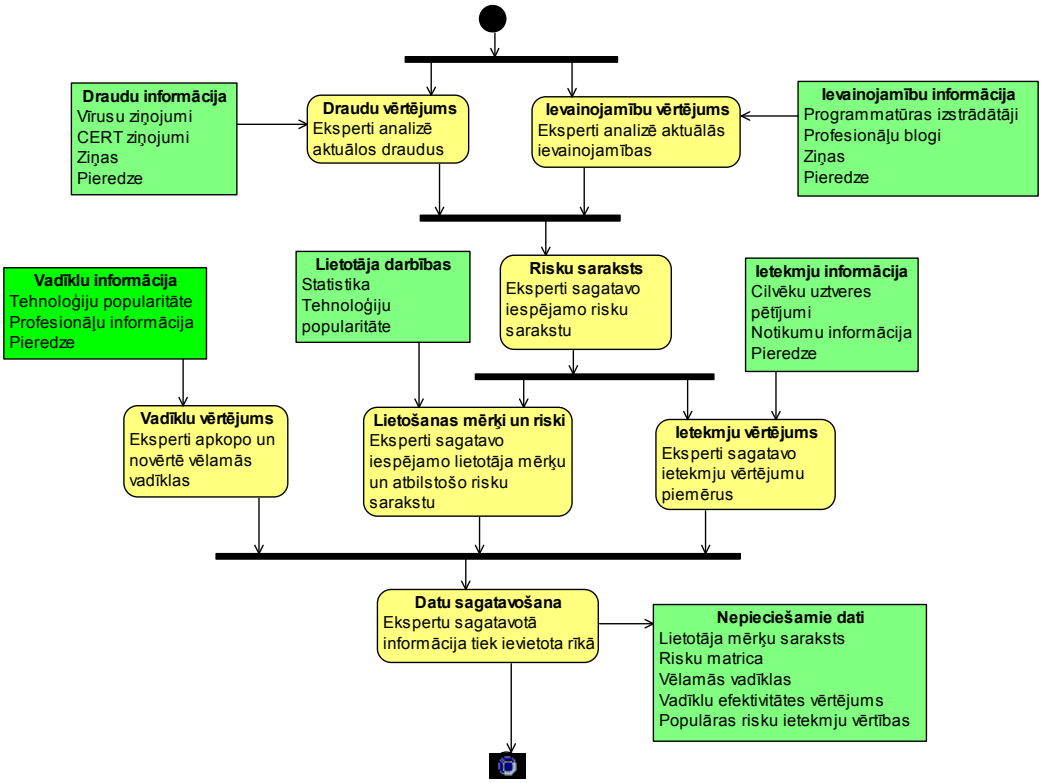
NIST ceļvedis ir ieteikts lietošanai dažādās institūcijās, taču tam nav ne oficiāla standarta, ne likuma spēka. To ir atļauts izmantot jebkuram, kas tādējādi var uzlabot savu informācijas sistēmu pārvaldību.

Riska novērtēšana ir pirmais posms riska pārvaldīšanas metodē. Šī posma rezultāts palīdz noteikt nepieciešamās vadīklas. Riska novērtēšanas posmā NIST ceļvedis apraksta deviņus soļus (11. tabula). Vairākus soļus var veikt paralēli.

11. tabula. Risku novērtēšanas procesa soļi

Solis 1	Sistēmas raksturošana
Solis 2	Apdraudējumu identificēšana
Solis 3	Ievainojamību identificēšana
Solis 4	Drošības vadīklu analīze
Solis 5	Iespējamību noteikšana
Solis 6	Ietekmju analīze
Solis 7	Risku noteikšana
Solis 8	Drošības vadīklu ieteikšana
Solis 9	Rezultātu dokumentēšana

Ņemot vērā privātā vidē pieejamo pieredzes apjomu, potenciālo apdraudējumu un ievainojamību, aptverošu analīzi nodrošina eksperti, balstoties uz tehnoloģisku datu apkopojumiem. Ekspertu iepriekš sagatavotai informācijai ir būtiska loma metodes pielietošanā. Eksperti sagatavo jautājumu sarakstus elektroniskās vides raksturošanai, risku sarakstu ikdienas datorlietotājam saprotamā vienkāršā valodā, risku saistību ar konkrētām lietotāja aktivitātēm (risku matricu), drošības vadīklu sarakstu un vērtējumu līmeņus, risku ietekmes vērtējuma ieteikumus (13. attēls, 12. tabula).



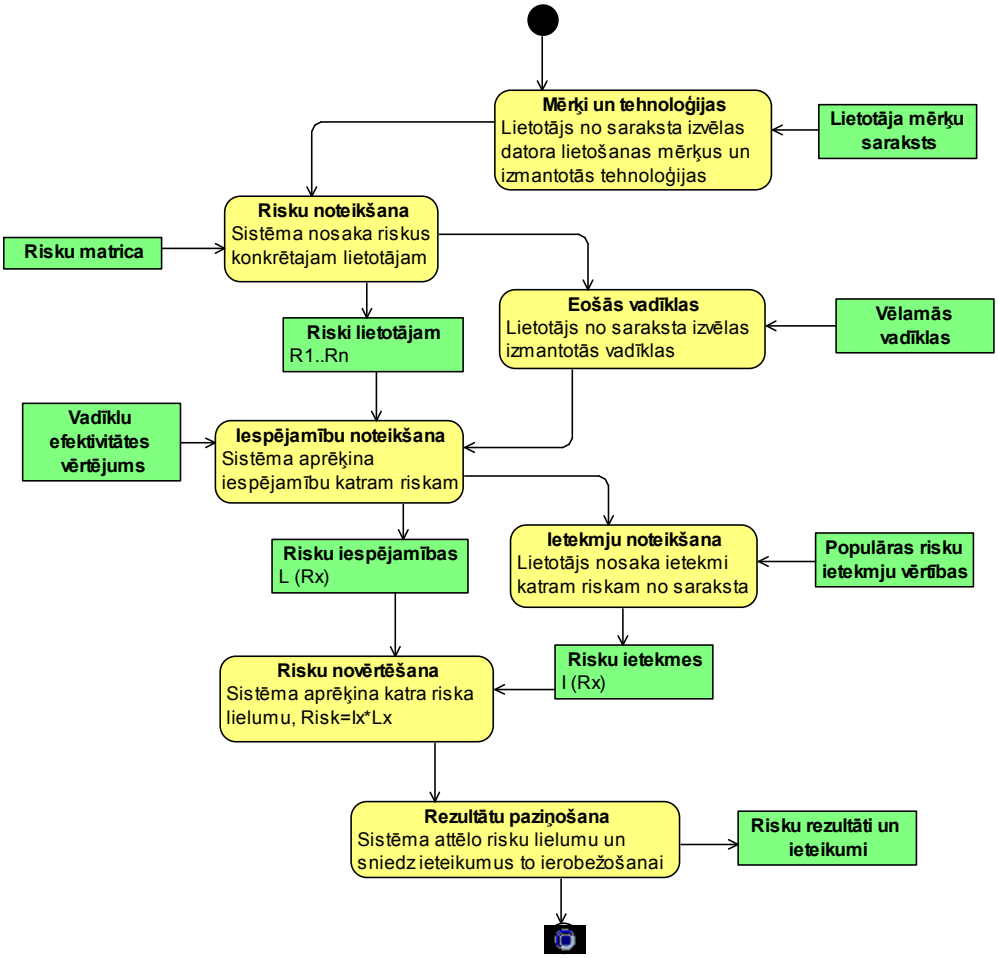
13. attēls Ekspertu informācijas sagatavošanas shematisks pārskats

12. tabula Ekspertu loma risku novērtēšanas metodē

Nr.	Solis	Datu avots – eksperti
1.	Elektroniskās vides raksturošana	Statistikas dati par datora/interneta izmantošanas mērķiem, informācija par populārām tehnoloģijām. Rezultāts – jautājumu saraksts ar atbilžu variantu izvēli.
2.	Apdraudējumu un ievainojamību identificēšana	Informāciju par iespējamiem datorlietotāju zaudējumiem, biežākajiem apdraudējumiem un tehnoloģiju ievainojamībām saskaņā ar publicētiem apskatiem un pieredzi. Rezultāts – ikdienas datorlietotājam būtisku risku saraksts.
3.	Drošības vadīklu apzināšana	Informācija par iespējamām vadīklām (tehniskām, organizatoriskām) saskaņā ar publicētiem apskatiem un pieredzi. Rezultāts – jautājumu saraksts ar atbilžu variantu izvēli, t.sk. noteikts, kuras vadīklas ir aktuālas konkrētām lietotām tehnoloģijām.
4.	Drošības vadīklu analīze un iespējamību noteikšana	Vadīklu ietekmes uz ievainojamību mazināšanu novērtējums, datu sagatavošana turpmākiem aprēķiniem.
5.	Ietekmju analīze	Katram riskam no 2. solī sagatavotā saraksta noteikta pieredzē balstīta biežāk iespējamā ietekmes vērtība.
6.	Risku noteikšana	Riska vērtības aprēķināšanas un līmeņa noteikšanas metodes izvēle.
7.	Drošības vadīklu ieteikšana	Katram no 2. solī noteiktajiem riskiem ir sagatavots ieteikumu pāris, ja konkrētais risks tiek iedalīts augstā vai vidējā līmenī.

Praktiskās pielietošanas gaitā lietotājam jāsniedz atbildes uz vienkāršiem jautājumiem par datora izmantošanas mērķiem un izmantojamajām sistēmām (14. attēls, 13. tabula).

Risku noteikšana un vadīklu ieteikšana veidota kā padomu saraksts. Savukārt rezultātu dokumentēšana formalizēta dokumenta veidā nav nepieciešama. Metodes detalizētāks izklāsts turpinājumā.



14. attēls. Praktiskās pielietošanas shematisks pārskats

13. tabula Lietotāja loma risku novērtēšanas metodē

Nr.	Solis	Datu avots – lietotājs
1.	Elektroniskās vides raksturošana	Atbildes uz jautājumiem par izmantoto aparatūru, t.sk. datorīklu, un programmatūru, kā arī darbībām, ko parasti dara datorā un/vai internetā.
2.	Apdraudējumu un ievainojamību identificēšana	Lietotājam nav darbību. Balstoties uz 1. soļa informāciju un visu iespējamo risku sarakstu, sistēmā tiek sagatavots konkrētajam lietotājam aktuālais risku saraksts.
3.	Drošības vadīklu apzināšana	Atbildes uz jautājumiem par izmantotajām vadīklām – gan tehniskām, gan zināšanām un prasmēm.
4.	Drošības vadīklu analīze un iespējamību noteikšana	Lietotājam nav darbību. Balstoties uz 2. un 3. soļu informāciju, sistēmā tiek aprēķināta katra riska iespējamība konkrētajam lietotājam aktuālajā risku sarakstā.
5.	Ietekmju analīze	Sarakstā ar riskiem, kas aktuāli konkrētajam lietotājam, izvēlas ietekmes vērtību, piekrītot ekspertu ieteikumam vai arī to mainot.
6.	Risku noteikšana	Lietotājam nav darbību. Sistēmā tiek veikta riska vērtības aprēķināšana un līmeņa noteikšana riskiem, kas aktuāli konkrētajam lietotājam, balstoties uz 4. un 5. soļa rezultātiem.
7.	Drošības vadīklu ieteikšana	Tiek attēlots risku novērtējums un ieteikumi.

4.2.2. Elektroniskās vides raksturošana

Elektroniskās vides raksturošanas solī uzskaita izmantoto aparatūru un programmatūru, tīkla pieslēgumus, informācijas grupas un tās izmantošanas mērķus. Jautājumu kopumu sagatavo eksperti, balstoties uz statistiskiem datiem par iedzīvotāju biežākajiem datora izmantošanas mērķiem, piemēram, e-pasta nosūtīšana un saņemšana, darbošanās sociālajā tīklā, maksājumi internetbankā. Otra jautājumu grupa paredzēta datorā izmantotās operētājsistēmas un interneta pieslēguma veida noskaidrošanai.

Jautājumu piemēri tālāk tekstā.

- Kādu operētājsistēmu izmanto (vairākas atbildes iespējamas)?
  - Windows XP
  - Windows 7
  - Linux
  - MacOS
- Kādu datortīkla pieslēgumu izmanto?
  - Tiešs pieslēgums pakalpojuma sniedzēja aparatūrai
  - WiFi maršrutētājs un bezvadu tīkls
  - Svešs bezvadu tīkls
- Ko parasti dara datorā/internetā (vairākas atbildes iespējamas)?
  - E-pasta nosūtīšana un saņemšana
  - Informācijas meklēšana
  - Spēļu, attēlu, filmu vai mūzikas lejupielāde
  - Apmaiņa ar filmām, mūziku utt., izmantojot peer-to-peer programmas
  - Interneta banka
  - Paša izveidota satura augšupielādēšana jebkurā tīmekļa vietnē
  - Fotogrāfiju glabāšana un apstrāde
  - Dokumentu rakstīšana un noformēšana

4.2.3. Apdraudējumu un ievainojamību identificēšana

Apdraudējumu un ievainojamību identificēšanā izmanto gan statistiskos datus, gan informāciju no elektroniskās vides apzināšanas, gan programmatūras ražotāju sniegto informāciju. Apdraudējumu kopa satur gan tehnoloģiskus apdraudējumus, piemēram, datorvīruss, gan informācijas neplānotas publiskošanas apdraudējumus. Uzturot metodi, laika gaitā tiek pilnveidots arī apdraudējumu saraksts. Balstoties uz informāciju par aktuālajiem apdraudējumiem, eksperti ir izveidojuši iespējamo risku sarakstu, piemēram, vīrusa darbības rezultātā sabojāti dati datorā, neapdomīgi publiskota informācija tiek izmantota, lai izkrāptu naudu, pārāk vienkāršas paroles dēļ sociālā tīkla profilā kāds darbojies saimnieka vietā. Elektroniskās vides apzināšanas aptauja iekļauj jautājumus, lai

varētu identificēt ievainojamības. Ņemot vērā minēto informāciju, tiek noteikts risku saraksts, kas ir aktuāls konkrētajam lietotājam.

Jāņem vērā, ka apdraudējums nav tas pats, kas risks. Daži piemēri. Apdraudējums ir vīrusa iekļūšana datorā. Šis apdraudējums var izraisīt dažādus riskus, piemēram, datorā glabāto datu pazaudēšanu vai sabojāšanu. Apdraudējums ir e-pasta mēstules saņemšana. Šis apdraudējums var radīt riskus, piemēram, "nepatīkamas sajūtas, lasot nepiedienīgu piedāvājumu" vai "trojas zirga iekļūšana datorā, kas var izraisīt privātu datu noplūdi".

Apdraudējumus mājas datoram var iedalīt vairākās grupās:

- trešo personu mērķtiecīgas darbības, lai iegūtu datorā glabātos datus, ko vēlāk izmantot krāpniecībā vai līdzīgās aktivitātēs;
- trešo personu mērķtiecīgas darbības, lai iegūtu iespēju izmantot datora resursus;
- tehniskas problēmas, iekārtas atteikumi;
- lietotāja neatbilstoša rīcība, t.sk. paroles aizmiršana vai savu datu publiskošana.

Agrāk populārs iemesls, kā datorlauzim palepoties, ka spēj to izdarīt, šobrīd nav bieži izplatīts. Taču nav izslēgts, ka jaunatnes vidū šāda rīcība kādā brīdī nekļūst par iecienītu. Tomēr atsevišķi apskatīt šo apdraudējumu grupu nav nepieciešams, jo izvairīšanās rīcība ir tāda pati, kā situācijā ar citām trešo personu mērķtiecīgām darbībām.

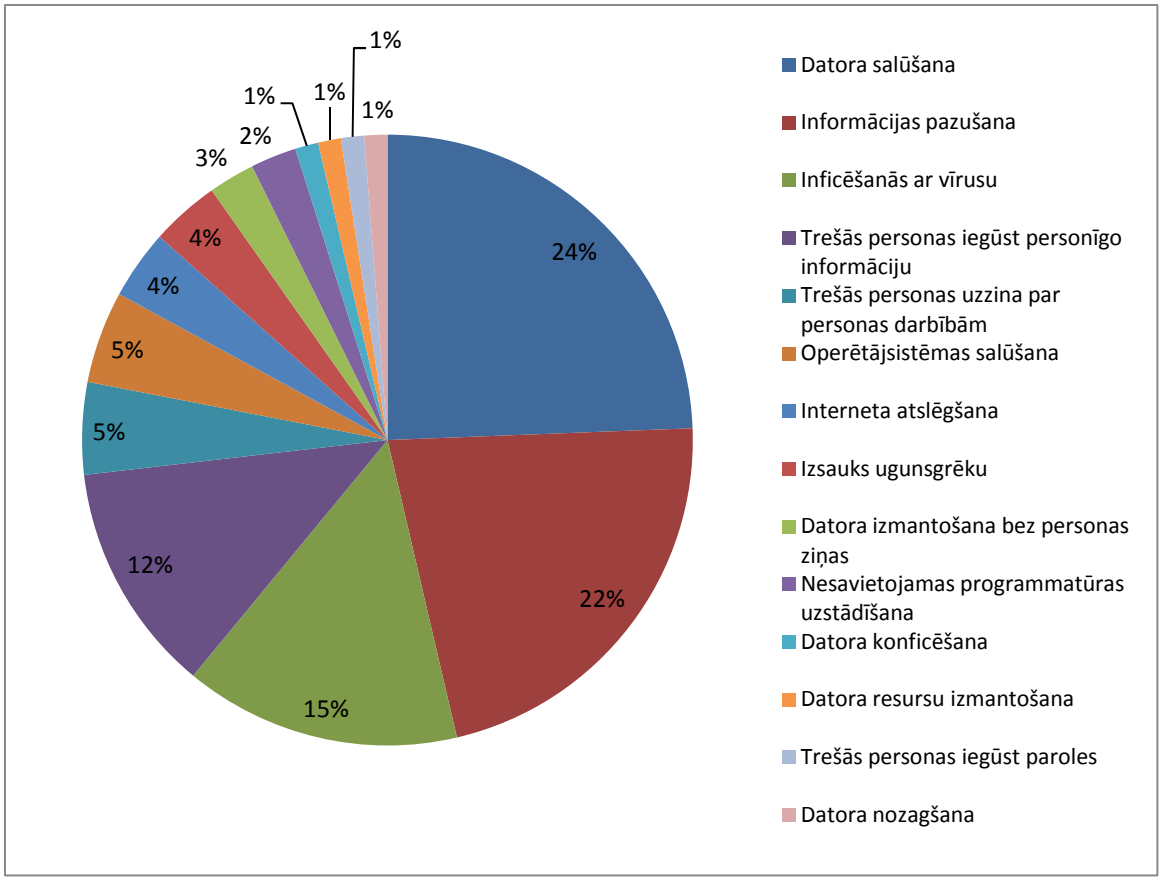
Ierocis, ar ko trešās personas visbiežāk izvēlas rīkoties, lai sasniegtu savus mērķus, ir kaitīga (kaitnieciska, nevēlama, utml.) programma jeb vīruss. Tehnoloģiju speciālistu vidū kaitīgas programmas tiek iedalītas dažādās grupās, populāras ir vīrusi, tārpi, trojas zirgi, spiegprogrammatūras, reklāmas programmas. Tomēr mājas lietotāja izpratnei piemērotāk ir lietot jēdzienu 'vīruss' visām programmām, kas mēģina veikt nevēlamas darbības. Turklāt arī aizsardzības programmas visbiežāk tiek sauktas tieši par antivīrusu programmām. Papildus varētu izmantot arī jēdzienu spiegprogrammatūra, lai uzsvērtu, ka daļa kaitīgo programmu ir ar tiešu mērķi iegūt datus.

Lai iegūtu datus, ne vienmēr tiek izmantoti tehnoloģiski rīki, sava vieta ir arī sociālās inženierijas metodēm. Šajos gadījumus vienīgā aizsardzība ir lietotāja izpratne par šāda apdraudējuma iespējamību un spēja adekvāti rīkoties jeb nesniegt informāciju. Jāņem vērā, ka ne vienmēr tiek uzdoti jautājumi ar mērķi izvilināt informāciju. Aizvien populārāka ir informācijas meklēšana, piemēram, sociālajos tīklos publicētajos datos.

Starp apdraudējumiem ar nepatīkamām sekām (risks pazaudēt visus datus) ir cietā diska sabojāšanās. Jo īpaši jāuzmanās, ja tiek izmantots papildus ārējais cietais disks. Pat viena nejauša nokrišana no galda var radīt neatgriezenisku bojājumu.

Pareizi izvēlēties rīcību attiecībā uz informācijas publiskošanu ir viens no grūtākajiem informācijas drošības pārvaldības un risku novērtēšanas procesu uzdevumiem. Riska novērtēšanas metode var tikai mudināt padomāt. Paroļu aizmiršanai "zāles" ir to pareiza veidošana vai pierakstīšana. Privātā vidē ir pilnībā pieļaujama vai pat ieteicama klasiskā datoru drošības likuma "paroli nedrīkst pierakstīt" pārkāpšana.

Kursa darbā "Populārākie apdraudējumi mājas datoram" veikta 39 mājas datoru lietotāju aptauja, lūdzot tos atbildēt uz jautājumu "Nosauciet 5 datora drošības riskus, kuri Jūs uztrauc visvairāk" (15. attēls) [MUR10]. Visbiežāk cilvēkus uztrauc datora sabojāšanās, kas, iespējams, saistīts ar finansiāliem iemesliem. Aptaujas apjoms un veikšanas metodes gan ļauj to izmantot tikai tālākas izpētes ideju gūšanai.



15. attēls. Riski, kas uztrauc mājas datoru lietotājus

Potenciālo risku saraksta veidošanu nodrošina speciālisti, pilnveidojot to atbilstoši attīstībai. Daži risku piemēri apkopoti 14. tabulā.

14. tabula. Risku piemēri

Vīrusa darbības rezultātā dati nokopēti nezināmā virzienā
Neapdomīgi publicēti dati tiek izmantoti, lai izkrāptu naudu
Dators iesaistīts botu tīklā, lai izsūtītu mēstules
Ārējā diska bojājuma dēļ, dati ir zuduši
Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā
Pārāk vienkāršas paroles dēļ, sociālā tīkla profilā kāds darbojies saimnieka vietā

4.2.4. Drošības vadīklu apzināšana

Drošības vadīklu apzināšanas solī ar jautājumu palīdzību tiek noskaidrotas elektroniskajā vidē izmantotās vadīklas, piemēram, pretvīrusu programma, ikdienas datorlietotāja IT zināšanas un prasmes, atbilstoši aizsargāts bezvadu tīkla maršrutētājs. Lai atvieglotu atbilžu sniegšanu un vēlāk arī analīzi, atbildēm ir sagatavoti varianti.

Daži jautājumu piemēri sniegti zemāk.

- Kādus drošības risinājumus lieto (vairākas atbildes iespējamas)?
    - A1.1 Antivīrusu programma, kas tiek regulāri atjaunināta
    - A1.2 Antivīrusu programma bez atjaunināšana
    - A2.1 Ugunsmūra programmatūra
    - A2.2 Operētājsistēmas ugunsmūris
    - A3.1 Rezerves kopijas pēc regulāras procedūras
    - A3.2 Rezerves kopijas šad un tad
- Kas nodrošina IT drošības pārvaldību?
    - P1 Neviens
    - P2 Pats, bet ne vienmēr pietiek zināšanu
    - P3 Pats visu, ko vajag, māku
    - P4 Aicinu atbilstošu speciālistu

4.2.5. Drošības vadīklu analīze un iespējamību noteikšana

Drošības vadīklu analīzes mērķis ir analizēt esošās vadīklas, kas samazina iespējamību apdraudējumam izmantot ievainojamību. Drošības vadīklu analīze ietver iespējamību izvēli. Vadīklas elektroniskā vidē ir gan tehniskas, gan organizatoriskas. Tehniskas vadīklas ir tādas, kas iebūvētas aparatūrā vai programmatūrā, piemēram, pieejas kontroles risinājums, šifrēšana, pretspiegošanas programmatūra. Organizatoriskas vadīklas iekļauj drošības politiku un noteikumus, procedūras un lietotāju pienākumus, arī fiziskās drošības pasākumus. Visas drošības vadīklas iedalāmas divās lielās grupās: preventīvās jeb profilaktiskās vadīklas un detektējošās jeb izmeklējošās vadīklas. Preventīvās vadīklas paredzētas apdraudējumu īstenošanās aizkavēšanai, piemēram, parole sargā ieeju vai arī šifrēšana neļauj nepiederošām acīm izlasīt tekstu. Detektējošās vadīklas pieraksta mēģinājumus apdraudējumiem notikt, piemēram, auditācijas pieraksti vai ielaušanās aizkavēšanas sistēmas. Detektējošās vadīklas veidotos pierakstus ir svarīgi arī analizēt, un šie rezultāti var noderēt jaunu preventīvo vadīklu nepieciešamības izvērtēšanā.

Metode privātai videi neparedz detektējošo vadīklu darbības rezultāta analīzi. Drošības vadīklas tiek analizētas, izvērtējot elektroniskās vides aprakstu, vadīklu uzskaiti un statistikā vai citā papildus informācijā balstītus ieteikumus. Šajā solī vēl netiek sniegti ieteikumi drošības vadīklu pilnveidei.

Iespējamību noteikšana tiek veikta, izmantojot statistikā vai citā pieredzē balstītus datus, ņemot vērā gan elektroniskās vides aprakstu, gan potenciālos apdraudējumus, gan vadīklu analīzi.

Iespējamību mēra līmeņos. Dažādām metodēm līmeņu skaits ir atšķirīgs. Biežāk lietoti ir trīs, četri vai pieci. Privātai videi pietiekami ir trīs līmeņi: augsts, vidējs un zems. Augsts iespējamības līmenis ir tad, ja apdraudējums ir ar motivētu mērķi un drošības vadīklas attiecīgām ievainojamībām nav vispār vai ir sliktas. Piemēram, botu tīklu veidotāji šobrīd ir ļoti motivēti iegūt savā kontrolē pēc iespējas daudz datoru, un katrs dators, kam nav gandrīz nekādas aizsardzības pret nevēlamu viesu iekļūšanu no interneta, ir ar augstu iespējamību, ka apdraudējums realizēsies. Vidējs iespējamības līmenis ir situācijā, kad apdraudējums ir daļēji motivēts un drošības vadīklas attiecīgām ievainojamībām ir gandrīz pilnvērtīgas. Piemēram, svešas personas grib izmantot interneta pieslēgumu, ir uzstādīts bezvadu maršrutētājs, bet tam ir tikai vienkārša parole. Zems iespējamības līmenis ir tad, ja apdraudējuma motivācija ir nenozīmīga un drošības vadīklas

ir labas. Piemēram, fotogrāfiju arhīva izzušana datora tehnisku iemeslu dēļ var notikt, bet, veidojot un, pareizi uzglabājot rezerves kopijas, notikuma iespējamība ir ļoti zema.

Ja ir vadīklas A1.1, A2.1 vai A3.1, tad iespējamība ir zema, ja ir A1.2, A2.2 vai A3.2 – vidēja, bet, ja nav šādas vadīklas, tad – augsta. Ne visas iespējamās vadīklas vienmēr nepieciešamas, piemēram, izmantojot dažu tipu operētājsistēmas, var iztikt bez antivīrusu programmatūras.

Drošības vadīklu analīzes un iespējamību noteikšanas soļa rezultāts ir iespējamības līmenis.

4.2.6. Ietekmju analīze

Ietekmju analīzei organizācijās izmanto ietekmes uz darbību vērtējumus, arī atbilstības prasības, piemēram, personas datu aizsardzības jomā. Viena no biežāk lietotajām metodēm ir pamatdarbības procesu vadītāju intervēšana. Šajā posmā jautājumi tiek strukturēti atbilstoši klasiskajai informācijas drošības triādei: konfidencialitāte, integritāte un pieejamība. Informācijas nokļūšana pie nepilnvarotām personām var izraisīt gan finansiālus, gan reputācijas zaudējumus. Integritātes zudums var izraisīt gan nepieciešamību ieguldīt resursus tās atjaunošanai, gan kļūdainu lēmumu pieņemšanu, gan nopietnu uzticēšanās zudumu IT kopumā. Pieejamības pārtraukumi var radīt problēmas gan pašai organizācijai, gan jo īpaši klientiem, kas sistēmai ir uzticējušies.

Katram no minētajiem drošības mērķiem var būt atšķirīga nozīme atkarībā no organizācijas darbības veida un informācijas satura. Privātā vidē pieejamība klasiskā nozīmē ir mazāk svarīga. Psiholoģiskos aspektus par atkarību no darbošanās sociālajos tīklos utml. šeit neapskatām. Integritātes nozīme šajā vidē ir neviendabīga. Sistemātiski veidotiem informācijas apkopojumiem, protams, jāpaliek neizmainītiem no vīrusu vai citu personu rīcības. Bet paša lietotāja neuzmanīgas rīcības rezultātā sajaukta fotoalbuma bilžu kārtība nav kritiska. Konfidencialitāte privātā vidē ir cieši saistīta ar privātumu, un ir visvairāk sargājama.

Tomēr privātā vidē nav nepieciešams apgrūtināt ar dalījumu drošības mērķos, un ietekmju analīzes posma pirmais uzdevums ir ar aptaujas palīdzību noskaidrot informācijas īpašnieka attieksmi pret informācijas svarīgumu elektroniskajā vidē kopumā.

Ietekmju analīzes solī lietotājs pats nosaka, cik liela ietekme ir katram no riskiem, kas uz viņu attiecas. Vērtēšanu veic, uzdot jautājumus par katru risku, kas sākotnēji

identificēts un nav ticis izslēgts, jo konkrētais lietotājs neveic darbības, kur tas varētu realizēties.

Ietekmi, tāpat kā iespējamību, iedala līmeņos. Tāpat kā iespējamības arī ietekmes novērtējumam privātā vidē pietiekami ir trīs līmeņi: augsts, vidējs un zems. Ietekmes novērtēšanai izmanto gan kvantitatīvus mērus, piemēram, zaudējumi naudas izteiksmē, gan kvalitatīvus mērus, kas ir vairāk subjektīvi. Privātā vidē gandrīz neiespējami ir ietekmi mērīt naudas izteiksmē, tāpēc piemērotāks ir kvalitatīvais vērtējums. Ietekme ir augsta, ja apdraudējuma rezultātā būtiski ir ietekmēta mājsaimniecības dzīve, piemēram, tiek atklāts, ka dators izmantots plašā botu tīklā, un tāpēc policija to konfiscē izmeklēšanai kopā ar visu privāto informāciju. Ietekme ir vidēja, ja apdraudējuma dēļ tiek bojāti vai pazaudēti nozīmīgi resursi, piemēram, cietā diska tehniskas problēmas dēļ tiek pazaudēta daļa tur glabātās informācijas. Ietekme ir zema, ja apdraudējums izraisa nelielu traucējumu darbā ar elektronisko vidi, piemēram, nenozīmīgas vīrusu darbības rezultātā uz laiku samazinās datora veiktspēja. Ietekmi vērtē sākotnējam riskam, t.i., neņemot vērā risku ierobežojošos pasākumus.

Šī soļa rezultāts ir ietekmes vērtība 1, 2 vai 3 katram no riskiem, kas attiecas uz konkrēto lietotāju.

4.2.7. Risku noteikšana

Risku noteikšanas soļa mērķis ir novērtēt riska līmeni. Vienkāršākā metode riska aprēķinam ir izmantot iespējamības un ietekmes līmeņu reizinājumu. Augsta, vidēja un zema līmeņa vērtējumu var aizstāt ar skaitļiem pēc dažādām shēmām. Metodē privātai videi izvēlēta viena no vienkāršākajām metodēm ar skaitļiem 1, 2 un 3.

Risks = 'Apdraudējuma iespējamība' * 'Ietekme'

Risku līmeņa vērtību piemērus skatīt 15. tabulā.

15. tabula Riska līmeņu matrica

Apdraudējuma iespējamība	Ietekme		
	Zema (1)	Vidēja (2)	Augsta (3)
Augsta (3)	Zems 1*3=3	Vidējs 2*3=6	Augsts 3*3=9
Vidēja (2)	Zems 1*2=2	Vidējs 2*2=4	Vidējs 3*2=6
Zema (1)	Zems 1*1=1	Zems 2*1=2	Zems 3*1=3

Šī soļa rezultāts ir riska līmeņa vērtējums.

4.2.8. Drošības vadīklu ieteikšana

Augstam riskam ir nepieciešama tūlītēja rīcība tā mazināšanā. Vidējam riskam ir vēlama mazināšana, tomēr šeit ir svarīgi izvērtēt ieguvumu uz izdevumu attiecību. Privātajā vidē nav mazsvarīgs arī subjektīvais viedoklis, kas palīdz izvēlēties, kuras papildu vadīklas ieviešana palielinās arī subjektīvo drošības sajūtu. Zemam riskam visbiežāk būs izdevīgāk to pieņemt.

Drošības vadīklu ieteikšanas soļa uzdevums ir ieteikt risinājumus riska līmeņa samazināšanai. Piemēram, kā augsts ir novērtēts risks "Neapdomīgi publiskota informācija tiek izmantota, lai izkrāptu naudu", tiek sniegts ieteikums: "Nevienas darbības internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, "parakstot" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par ieradumiem, hobijiem u.tml., lai iegūtu uzticību un izkrāptu naudu. Ir vērts atcerēties parunu "septiņreiz nomēri pirms nogriez" arī attiecībā uz informācijas publicēšanu internetā (sociālajos tīklos). Ja labprāt publisko daudz informācijas, uzmanies no nepazīstamiem saziņas partneriem, kas daudz zina par Tevi. Iespējams, ka būtu vērts izdzēst kaut daļu informācijas, lai tā nebūtu tik ērti pieejama.".

Ieteikumus sagatavo eksperti. Īsais ieteikums tiek papildināts ar vienu vai vairākām norādēm uz interneta vietnēm, kur var izlasīt vairāk informācijas vai saņemt skaidrojumu, kā veikt tehnoloģiskus pilnveidojumus. Noslēdzošais posms ir atlikušo risku akceptēšana.

4.3. Metodes aprobācija ar sistēmas prototipu IDRE

4.3.1. Datu sagatavošana rīka pielietošanai

Informācijas drošības risku novērtēšanas metodi var lietot kā mācību materiālu visi, kas vēlas izprast attiecīgo procesu. Lai pārbaudītu metodes pielietojamību, tā aprobēta, izmantojot tīmekļa sistēmas prototipu (rīku) IDRE (Informācijas Drošības Risku Eksperts).

Informācijas drošības risku novērtēšanas rīkam ir izvirzītas sekojošas prasības: lietojams datorlietotājam bez padziļinātām zināšanām tehnoloģijās, lietojams interneta vidē, papildināms, attīstoties tehnoloģiju ierīču un apdraudējumu klāstam.

Būtiska loma metodes pielietošanā ir ekspertu sagatavotai informācijai, balstoties uz statistikas datiem, publicētiem materiāliem un savu pieredzi[3].

Elektroniskās vides raksturošanas solī eksperti izmanto statistikas datus par datora/interneta izmantošanas mērķiem, piemēram, [CSP1]. Informāciju par populārām tehnoloģijām meklē internetā, piemēram, [BeOS], vai ikdienas pieredzē. Rezultāts šim solim ir jautājumu saraksts ar atbilžu variantu izvēli. Saraksts ietver datora izmantošanas mērķus (M1, M2, ... M13), piemēram, "M1 E-pasta nosūtīšana un saņemšana", "M3 Darbošanās sociālajā tīklā", "M11 Fotogrāfiju/video failu glabāšana un apstrāde savā datorā", izmantotās tehnoloģijas (OS1, OS2, ... OS5, IP1, IP2, IP3), piemēram, "OS1 Windows 7", "OS4 MAC OS X", "IP1 Bezvadu tīkls mājās". Rīkā IDRE izmantoto datora izmantošanas mērķu un tehnoloģiju sarakstu skat. 3. pielikumā.

Apdraudējumu un ievainojamību identificēšanas solī apkopo informāciju par iespējamiem datorlietotāju zaudējumiem, biežākajiem apdraudējumiem un tehnoloģiju ievainojamībām saskaņā ar publicētiem apskatiem un pieredzi, piemēram, CERT.LV informāciju par datoru incidentiem [CERT], pārskatus par datoru ievainojamībām, piemēram, [CoVul]. Risku saraksta sagatavošanai izmanto apdraudējumu sarakstu (A1, A2, ... A7), piemēram, "A1 Datorvīrusi", "A2 Datora iesaistīšana botu tīklā", "A5 Neapdomīga informācijas publiskošana", ievainojamību sarakstu (I1, I2, ... I7), piemēram, "I2 Datoram nav antivīrusa programmatūra", "I5 Nav datu kopiju", "I6 Lietotājs slikti pārzina IT drošības pārvaldību". Rīkā IDRE izmantoto datora un tā izmantošanas apdraudējumu un ievainojamību sarakstu skat. 3. pielikumā.

---

[3] Prototipa stadijā ekspertu viedokli pārstāv darba autore, balstoties uz studentu kursa darbos veiktām aptaujām un savu pieredzi.

Balstoties uz apdraudējumu un ievainojamību pārskatu, tiek sagatavots ikdienas datorlietotājam būtisku risku saraksts (R1, R2, ... R11), piemēram, "R1 Vīrusa darbības rezultātā lietotāja dati nokopēti nezināmā virzienā", "R3 Dators iesaistīts botu tīklā (zombēts) ar nezināmu mērķi (lietotājam nemanāmi)", "R8 Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā". Rīkā IDRE izmantoto risku sarakstu skat. 3. pielikumā.

Konkrētam lietotājam aktuālo risku sarakstu nosaka, izmantojot iespējamo risku matricu, piemēram, ja lietotājs izmanto datoru mērķim M1, tad viņam aktuāli var būt riski R1, R2, R3, R4, R7, R8, ja lietotājs izmanto tehnoloģiju IP1, tad viņam aktuāls var būt risks R11. Rīkā IDRE izmantoto risku matricu skat. 3. pielikumā, aktuālie riski tabulā atzīmēti ar 'X'.

Drošības vadīklu apzināšanas solī apkopo informāciju par iespējamām vadīklām (tehniskām, organizatoriskām) saskaņā ar publicētiem apskatiem, piemēram, programmatūras ražotāju vietnēs [MSddv], un pieredzi. Rezultāts šim solim ir jautājumu saraksts ar atbilžu variantu izvēli, t.sk. noteikts, kuras drošības vadīklas ir aktuālas konkrētām lietotām tehnoloģijām, piemēram, dažām operētājsistēmām nav aktuāli daļa apdraudējumu. Tiek sagatavots vadīklu saraksts (V1, V2, ... V7), piemēram, "V2 Antivīrusa programmatūra datoram", "V6 Regulāra programmatūras atjaunināšana", "V7 Paroļu izveides un lietošanas paradumi", un atbilstības matrica, kura vadīklas samazina, kura riska iespējamību, piemēram, vadīkla V2 samazina riska iespējamību riskiem R1 un R2. Rīkā IDRE izmantoto vadīklu sarakstu un vadīklu atbilstības matricu skat. 3. pielikumā, atbilstošās vadīklas, kas samazina riska iespējamību, tabulā atzīmētas ar 'X'.

Drošības vadīklu analīzes un iespējamību noteikšanas solī katrai vadīklai tiek sagatavoti atbilžu varianti, kas apraksta risinājumus ar dažādu ietekmi uz ievainojamību mazināšanu un līdz ar to riska iespējamības aprēķinu. Vadīklu ietekmes vērtējums var būt 2, 1 vai 0. Par attiecīgo vērtību tiek samazināta riska iespējamība, kuras sākotnējā vērtība, ja netiek lietota riskam atbilstošā vadīkla, ir maksimālā – 3. Piemēram,

- V2 Antivīrusa programmatūra datoram
    - Ir antivīrusa programmatūra un tā tiek regulāri atjaunota – 2
    - Ir antivīrusa programmatūra, bet tā netiek regulāri atjaunota – 1
    - Nav antivīrusa programmatūras – 0
    - Nezinu – 0

Pēc vadīklas piemērošanas riska iespējamība var būt 1, ja regulāri veic atbilstošas darbības, 2, ja darbības veic neregulāri, vai 3 – ja darbības neveic vai par tām neko nezina.

Rīkā IDRE izmantoto drošības vadīklu novērtēšanas jautājumu sarakstu skat. 3. pielikumā.

Ietekmju analīzes solī katram riskam ir noteikta pieredzē balstīta biežāk iespējamā ietekmes vērtība. Sākotnējā riska ietekme ir vērtība 1, 2 vai 3 katram no iespējamiem riskiem, piemēram, R1 – 3, R6 – 1. Rīkā IDRE izmantoto risku ietekmes novērtējumu sarakstu skat. 3. pielikumā.

Risku noteikšanas solī tiek aprēķināta katra riska vērtība saskaņā ar 4.2.7. nodaļā aprakstīto.

Drošības vadīklu ieteikšanas solī katram riskam ir sagatavots ieteikumu pāris, ja konkrētais risks tiek iedalīts augstā vai vidējā līmenī. Piemēram, ieteikums, ja risks ir augstu ietekmi: "R3 Ieteikums: Noziedznieki ne vienmēr uzreiz sabojā vai nozog datus no zombētiem datoriem, tomēr nekad nevar zināt, kad tas notiks. Ir iespējams, ka zombētais dators tiek iesaistīts uzbrukumā citiem datoriem, un izmeklēšanas gaitā var rasties problēmas tā īpašniekam. Noteikti jāpilnveido aizsardzības programmas (antivīrusu, ugunsmūra) un jāuzstāda labākas paroles, tas jāveic cik vien iespējams drīz.", ieteikums, ja risks ir vidēju ietekmi "R7 Ieteikums: Nevienas darbības Internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, "parakstot" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par ieradumiem, hobijiem vtml., lai iegūtu uzticību un izkrāptu naudu. Ir vērts atcerēties parunu "septiņreiz nomēri pirms nogriez" arī attiecībā uz informācijas publicēšanu Internetā (sociālajos tīklos). Ja labprāt publisko daudz informācijas, uzmanies no nepazīstamiem saziņas partneriem, kas daudz zina par Tevi."

4.3.2. Rīka IDRE izmantošana

Rīks IDRE pieejams internetā [IDRE]. Atverot sākuma lapu, lietotājs saņem skaidrojumu: "Datoru drošība nereti tiek uzskatīta par tikai atbilstošās jomas speciālistiem saprotamu un svarīgu tēmu. Tomēr par informācijas un datora drošību ir iespējams un nepieciešams rūpēties katram pašam. Atbildi uz jautājumiem par datora lietošanas paradumiem un noskaidro sev būtiskākos riskus, kas ar tiem saistīti. Ja Tavu datoru izmanto vairāki lietotāji vai Tu pats lieto vairākus datorus, tad jautājumi jāatbild katram un par katru datoru atsevišķi. Noslēgumā saņemsi ieteikumus, ko varētu vai vajadzētu darīt, ja šobrīd īstenotie drošības pasākumi neatbilst Tavām vēlmēm būt pasargātam elektroniskā vidē.". Rīks pieejams arī angļu valodā.

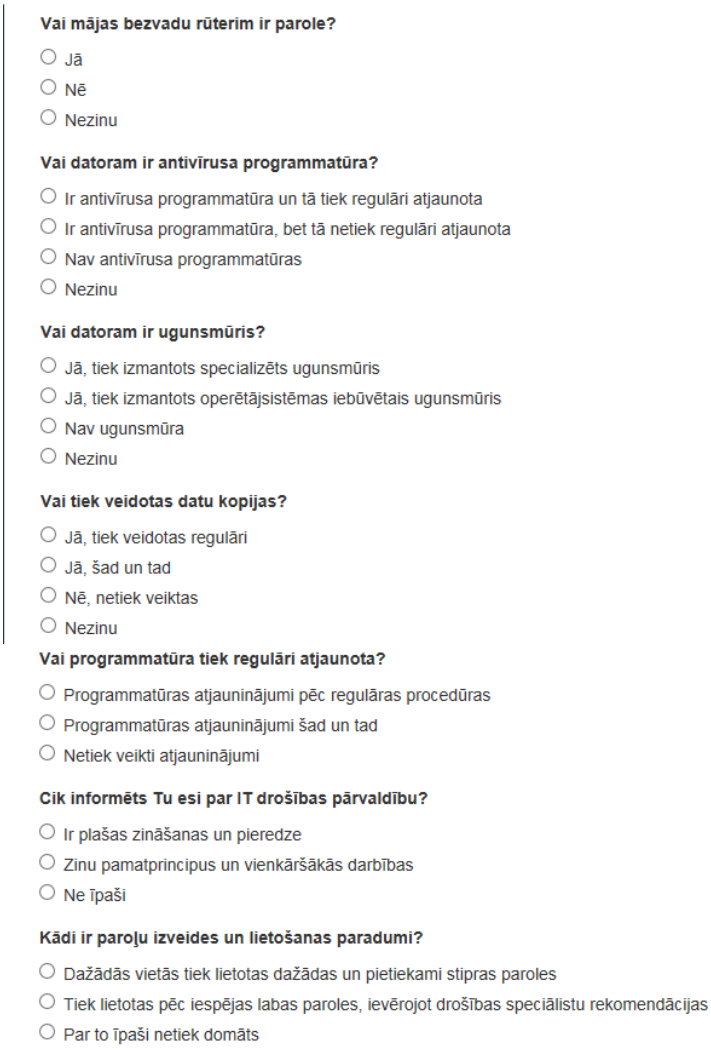
Apdraudējumu un ievainojamību identificēšanu rīks IDRE veic, balstoties uz datorlietotāja atbildēm par izmantoto operētājsistēmu, veiktajām darbībām un iepriekš sagatavotu ekspertu viedokli, kas iebūvēts rīkā.

Elektroniskās vides raksturošanai (1. solis, 16. tabula) datorlietotājs norāda, kādiem mērķiem viņš lieto datoru, kādu operētājsistēmu un tīkla pieslēguma veidu izmanto (16. attēls).

16. attēls. Elektroniskās vides raksturošana

Apdraudējumu un ievainojamību identificēšanu rīks IDRE veic, balstoties uz atbildēm par izmantoto operētājsistēmu, veiktajām darbībām un iepriekš sagatavotu ekspertu viedokli, kas iebūvēts sistēmā. Šī soļa rezultāts ir konkrētajam lietotājam atbilstošs risku saraksts. Šajā solī tas vēl netiek attēlots lietotājam (2. solis, 16. tabula).

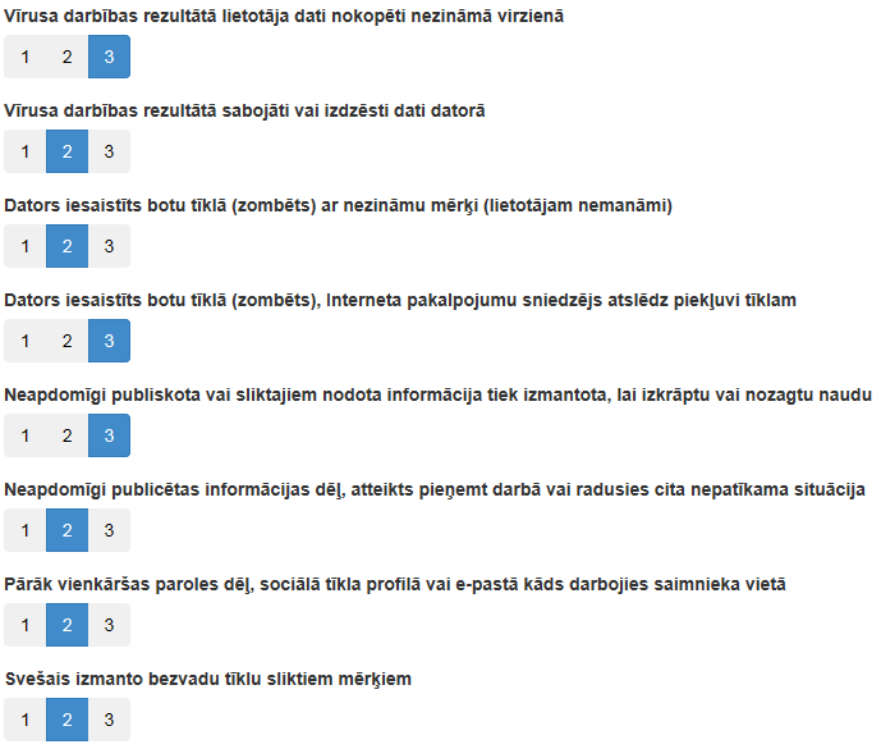
Drošības vadīklu apzināšanai, lietotājs atbild uz jautājumiem par izmantotajiem drošības risinājumiem, zināšanām un prasmēm (3. solis, 16. tabula). Ir iespējama arī atbilde "Nezinu", kas novērtēšanā ir līdzvērtīga attiecīgā drošības risinājuma neesamībai (17. attēls). Ja lietotājs iepriekš norādījis, ka izmanto bezvadu tīklu, papildus jāatbild uz jautājumu, vai tam ir uzstādīta parole.



17. attēls. Drošības vadīklu apzināšana

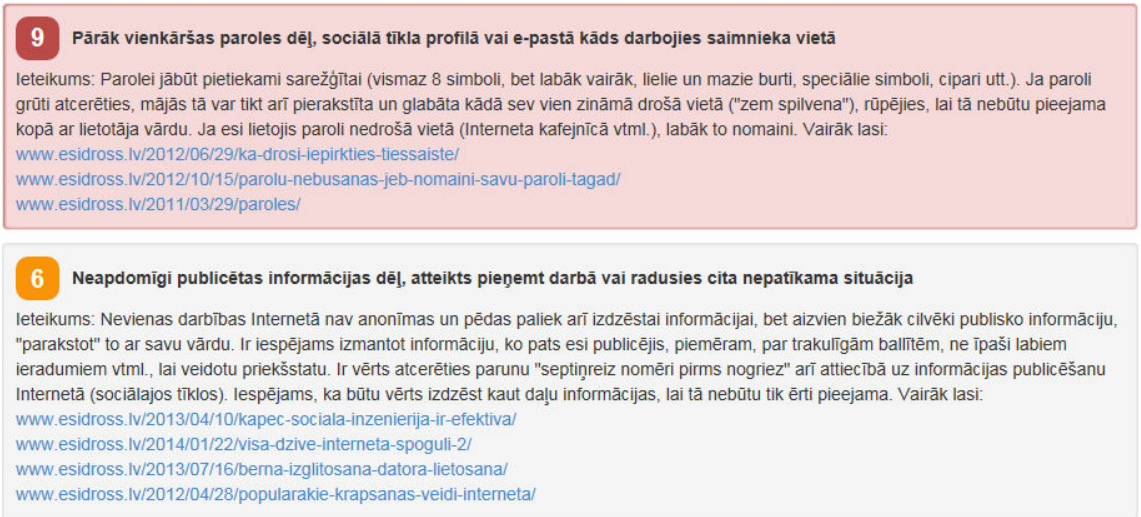
Drošības vadīklu analīzes un iespējamību noteikšanas aprēķins ir iebūvēts sistēmā, balstīts uz atbildēm par izmantotajām vadīklām un ekspertu viedokli par to svarīgumu. Šī soļa rezultāts ir iespējamības vērtība 1, 2 vai 3 katram no riskiem, kas attiecas uz konkrēto lietotāju (4. solis, 16. tabula).

Ietekmju analīzes solī lietotājs pats nosaka, cik liela ietekme ir katram no riskiem, kas uz viņu attiecas (5. solis, 16. tabula). Jāatbild uz jautājumu: "Iedomājies, ka minētais notikums būtu noticis. Cik svarīga Tev ir tā negatīvā ietekme: (1 – nemaz neuztrauc, 2 – gan jau pārdzīvošu, 3 – būtiska negatīva ietekme)?". Lai lietotājam būtu vieglāk, eksperti ir novērtējuši riskus, sniedzot biežāk lietotas vērtības ieteikumu, taču lietotājs ir aicināts to mainīt, ja viņa attieksme ir citāda (18. attēls). Šī soļa rezultāts ir ietekmes vērtība 1, 2 vai 3 katram no riskiem, kas attiecas uz konkrēto lietotāju.



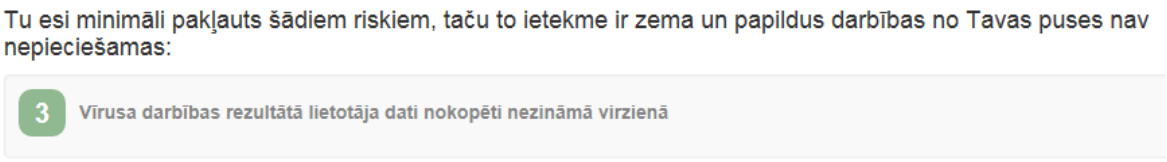
18. attēls. Ietekmju analīze

Risku noteikšanas solis ir risku vērtības aprēķins, kas notiek sistēmā automātiski, balstoties uz 4. un 5. soļa rezultātiem (6. solis, 16. tabula). Drošības vadīklu ieteikšanas solī tiek attēloti riski, kas attiecas uz konkrēto lietotāju (7. solis, 16. tabula). Riski ar augstu vērtību 9 tiek atzīmēti ar sarkanu krāsu, riski ar vidēju vērtību 4 vai 6 – ar dzeltenu. Katram riskam tiek sniegts padoms, ko vajadzētu darīt tā samazināšanai (19. attēls).



19. attēls. Drošības vadīklu ieteikšana

Riski, kuru vērtība ir zema – 1, 2 vai 3, tiek attēloti, bet papildus veicamas darbības netiek ieteiktas (20. attēls).



20. attēls. Risku informācija

Daži piemēri ar hipotētiskiem sistēmas lietotājiem parādīti 4. pielikumā. Pilns datu apraksts 5. pielikumā.

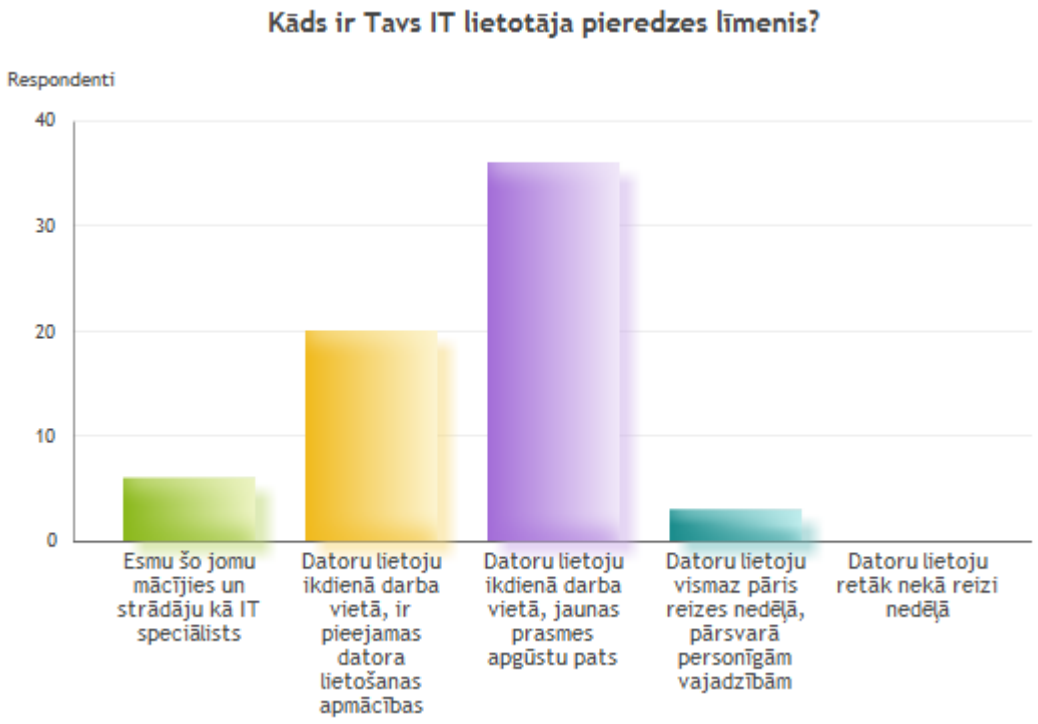
Rīks IDRE izvietots koplietošanas vidē GitHub. Programmatūra un dati ir brīvi pieejami.

4.3.3. Rīka IDRE novērtējums

Rīka IDRE novērtēšanai izmantota aptaujas metode. Aptauja veikta ar anketēšanas paņēmienu, izmantojot elektroniskās aptaujas metodi. Aptaujā piedalījās 65 respondenti. Pēc iespējas tika izslēgtas personas, kas labi pārzina informācijas tehnoloģijas. Respondenti vispirms izmēģināja rīku IDRE darbībā, pēc tam atbildēja uz novērtēšanas anketas jautājumiem. Aptauja bija anonīma.

Respondenti sniedza atbildes uz sešiem jautājumiem. Trīs no jautājumiem bija paredzēti lietotāja pieredzes un vispārējās attieksmes novērtēšanai, bet trīs jautājumi – rīka IDRE novērtējumam. Pilns jautājumu saraksts 6. pielikumā.

Lai novērtētu, vai ir izpildīts viens no aptaujas vēlamajiem kritērijiem – pēc iespējas mazāk aptaujāt lietotājus ar padziļinātām IT zināšanām – anketas sākumā tika uzdots jautājums par respondenta IT zināšanām un pieredzi darbā ar datoru. Atbildes uz šo jautājumu rāda, ka minētais kritērijs ir izpildīts, jo tikai daļai respondentu (30.8%) darba vietā ir pieejamas datoru lietošanas apmācības, bet vairāk nekā puse respondentu (55.4%) jaunas prasmes apgūst paši (21. attēls).

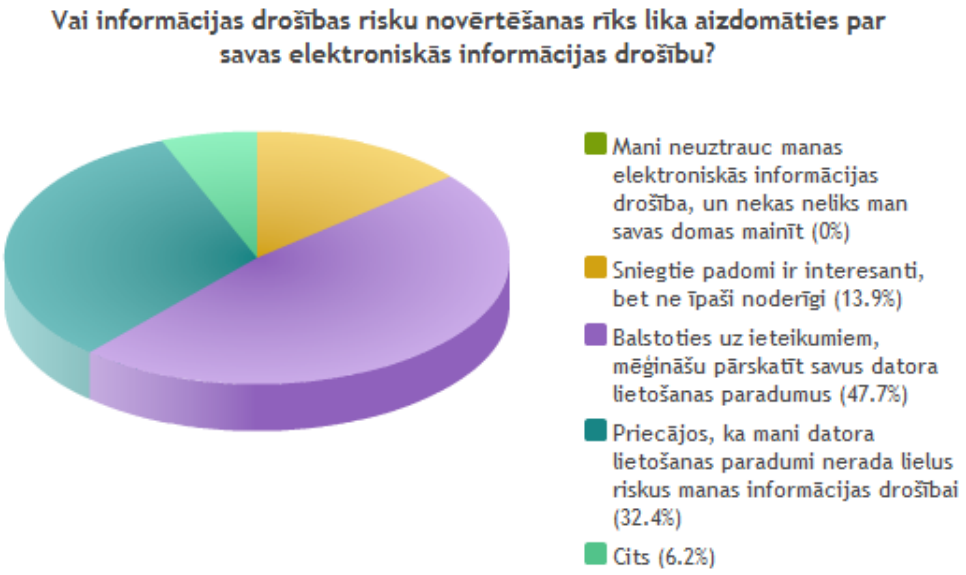


21. attēls. Lietotāja IT pieredzes līmenis

Lai novērtētu iespējas, kur un kā labāk novietot rīku IDRE ikdienas lietošanai, respondentiem tika lūgts atbildēt uz jautājumiem "Kur Tu visbiežāk meklē padomu, ja saskaries ar problēmu personīgā datora darbībā vai jautājumos par rīcību ar personīgo elektronisko informāciju?" un "Kas ir kritēriji, lai Tu uzticētos Interneta mājaslapas sniegtajai informācijai?". Atbilžu rezultāti analizēti 4.4.4. nodaļā.

Informācijas drošības risku novērtēšanas metode un rīks IDRE paredzēts gan ar datora darbību, gan ar lietotāja rīcību saistītu risku novērtēšanai. Katrai no minēto risku daļām anketā bija paredzēts savs jautājums. Privātā vidē biežāk svarīgi būs tieši tie riski, kas saistīti ar lietotāja rīcību (22. attēls). Gandrīz pusei respondentu (47.7%) sistēmas sniegtie ieteikumi palīdzēs pilnveidot datora lietošanas paradumus, apmēram trešā daļa (32.4%) respondentu priecājas, ka viņu paradumi jau ir pietiekami atbilstoši. Starp respondentiem nav neviena, kuru neuztrauc neatbilstoša rīcība ar informāciju, bet deviņiem respondentiem sistēma nesniedza noderīgu informāciju. Četri respondenti bija izvēlējušies sniegt savu atbildes variantu, no kuriem trīs pēc būtības ir ļoti tuvu atbildei, ka ieteikumi likuši padomāt.

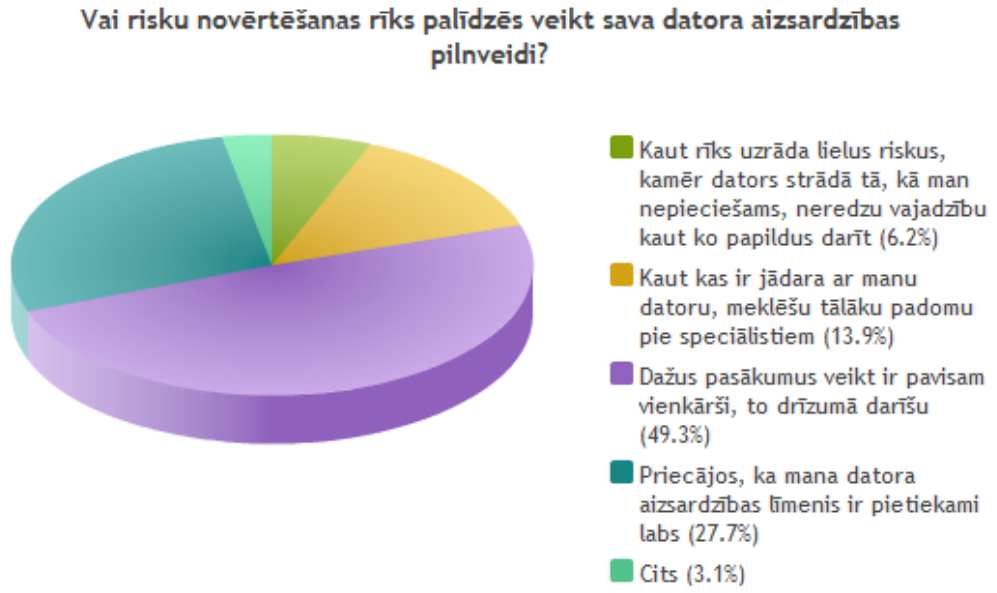
Kopumā vairāk nekā 80% respondentu, izmantojot rīku IDRE, guvuši noderīgu informāciju par drošu darbu ar informāciju elektroniskā vidē.



22. attēls. Palīdzības līmenis elektroniskās informācijas drošības pilnveidē

Neliela daļa respondentu (6.2%) negrasās pilnveidot datora aizsardzību, kaut arī saskaņā ar ieteikumiem to vajadzētu darīt. Gandrīz puse respondentu (49.3%) plāno drīzumā izpildīt vienkāršākos ieteikumus, bet daļa respondentu (13.9%) ir uzklausījuši ieteikumus kaut ko darīt, bet padomus praktiskai rīcībai meklēs pie speciālistiem. Nedaudz vairāk nekā ceturtā daļa var būt apmierināti ar sava datora drošības līmeni (23. attēls).

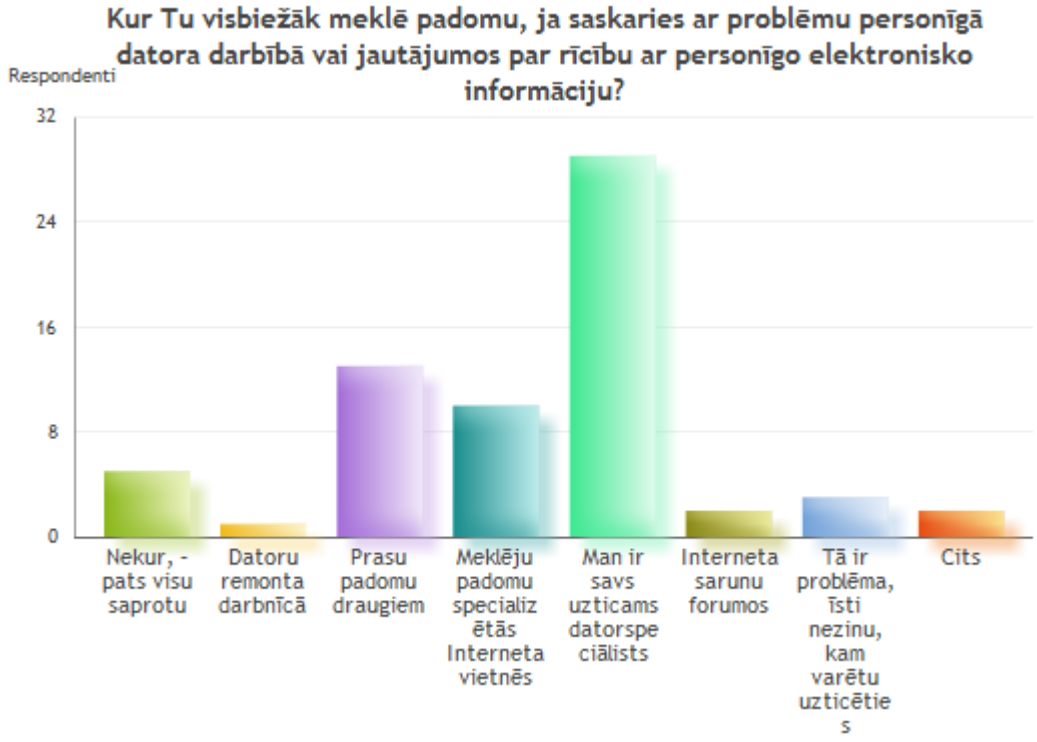
Kopumā vairāk nekā 90% respondentu, izmantojot rīku IDRE, guvuši noderīgu informāciju par datora aizsardzību.



23. attēls. Palīdzības līmenis datora aizsardzības pilnveidē

4.3.4. Risku novērtēšanas metodes attīstība

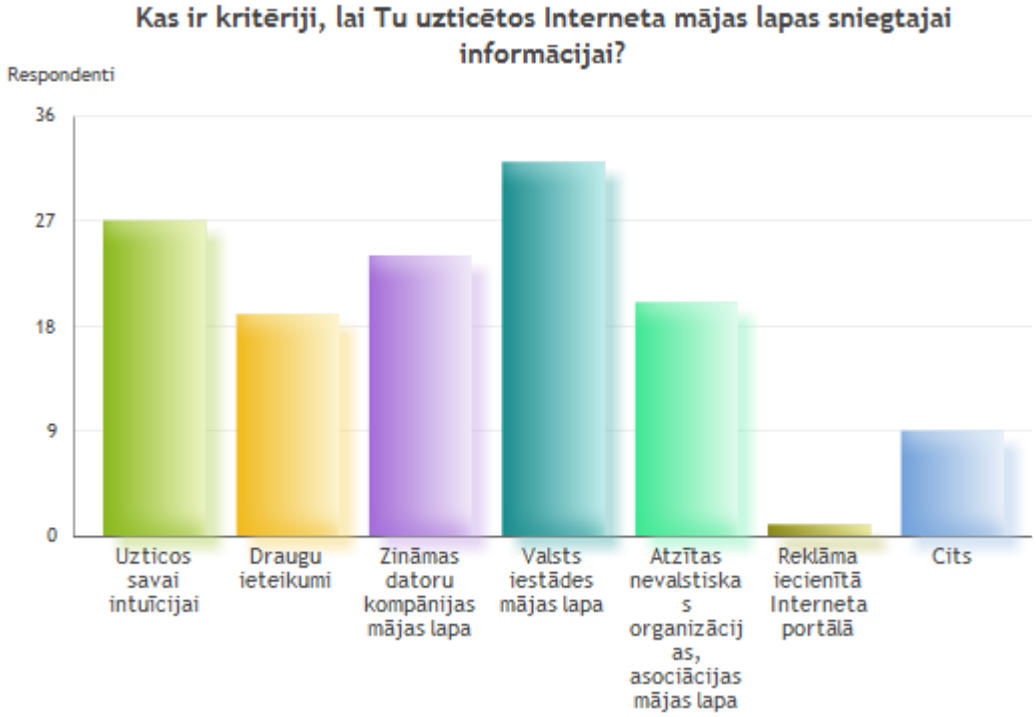
Aptaujas rezultāti rāda, ka gandrīz pusei (44.6%) respondentu ir savs uzticams datorspeciālists, 20% respondentu prasa padomu draugiem, bet 15.4% biežāk meklē padomu specializētās interneta vietnēs. Šim jautājumam bija jāizvēlas tikai viena atbilde, tāpēc eksperti pieļauj, ka respondentiem bija jāizvēlas biežāk lietotais variants, un ir iespējams, ka citās situācijās tiek izvēlēts cits risinājums (24. attēls).



24. attēls. Padoma meklēšanas vietas

Lai rīks IDRE būtu pieejams izmantošanai pēc iespējas vairāk lietotājiem, tas jānovieto kādā interneta vietnē. Tomēr, ņemot vērā, ka cilvēki nereti izvairās apmeklēt nepazīstama tīmekļa vietnes, tīmekļa vietnei jābūt tādai, kam lietotāju uzticas. Aptaujā respondentiem tika lūgts atbildēt, kādi ir kritēriji, lai uzticētos interneta mājaslapas sniegtajai informācijai. Šim jautājumam bija iespējams sniegt vairākas atbildes, un kopā tika saņemtas 132 atbildes, t.i., katrs respondents sniedza vidēji 2 atbildes.

Visvairāk uzticēšanos respondentos raisa valsts iestādes mājaslapa, turklāt 5 respondenti uzticas tikai šādām lapām (25. attēls). Starp atbildēm, ko lietotāji sniedza brīvā formā, dominē tādi kritēriji kā vietnes reputācija un uzticama medija ieteikumi.



25. attēls. Kritēriji tīmekļa vietnes uzticamībai

Lai nodrošinātu uzticēšanos informācijas drošības risku novērtēšanas rīkam IDRE, tas jāizvieto portālā, kam ir uzticams saimnieks. Ņemot vērā portāla Esidrošs [ED] mērķi un faktu, kas tas izveidots ar Satiksmes ministrijas atbalstu, tas varētu būt piemērota vieta.

Informācijas drošības risku novērtēšanas metode izmanto iepriekš sagatavotus datus gan par izmantoto aparatūru un programmatūru, gan – iespējamiem apdraudējumiem un risku variantiem. Daļa izmantoto datu tiek meklēta statistikā un pētījumos. Datus par iedzīvotāju biežākajām darbībām internetā var iegūt CSP publikācijās, tomēr publicēti parasti tiek dati uz iepriekšējā gada sākumu. Ņemot vērā salīdzinoši būtiskās izmaiņas dažu gadu laikā, arī turpmāk cilvēku paradumi var nozīmīgi mainīties. Par citiem datora izmantošanas mērķiem Latvijas iedzīvotāju vidū autorei neizdevās atrast autoritatīvus datus. Ir iespējams pilnveidot rīku IDRE, lai tas kalpotu arī par šādu datu uzkrāšanas rīku. Lietotājam tiktu dota iespēja atbildēt arī uz atvērtajiem jautājumiem par izmantoto aparatūru, programmatūru un lietošanas paradumiem, tādējādi papildinot datu kopumu.

Lai izmantotie dati par apdraudējumiem un riskiem būtu atbilstoši tehnoloģiju attīstībai, nepieciešama to regulāra uzturēšana.

Lai nodrošinātu minēto datu uzturēšanu, nepieciešama ekspertu komanda. Portāla Esidrošs atbalsta komanda var nodrošināt ekspertu pieredzi sistēmas attīstībai. Labs risinājums varētu būt LU DF studentu iesaistīšana. Studenti, kas apmeklē kursu "IS drošība", izstrādātu studiju darbus, veicot jaunākās informācijas apkopošanu.

4.4. Ekspertu vērtējums

Lai gūtu vispusīgu rīka IDRE novērtējumu un paplašinātu vienas metodes rezultātus ar citu metodi, papildu anketēšanai izmantots cits aptaujas paņēmiens – intervijas ar ekspertiem. Izvēloties intervējamās personas, tika izmantots mērķtiecīgās izlases veidošanas princips – izvēlētas tās personas, kurām ir personīgā pieredze attiecībā uz pētāmo jautājumu un kuras spēj paust argumentētu viedokli.

Kvalitatīvajā novērtēšanas posmā izmantotas intervijas ar pieciem ekspertiem, kas izmēģināja rīku IDRE darbībā, iepazinās ar lietotāju aptaujas rezultātiem un tika intervēti klātienē.

Eksperts1 ir ilggadējs datorlietotājs, kurš ar datoru strādā mājās, veicot organizatoriska rakstura uzdevumus liela uzņēmuma vajadzībām. Nepieciešamības gadījumā viņam ir pieejams IT speciālistu atbalsts uzņēmumā, tomēr arī pašam ir nozīmīga pieredze. Minētā pieredze ļauj sniegt padomus drošā datora lietošanā arī ģimenes locekļiem.

Eksperts2 strādā mājās individuāli, veicot darbu, kas prasa gan meklēt informāciju internetā, gan aprakstīt rezultātus, gan droši saglabāt paveikto. Papildus pieredzi guvis, vairākus gadus strādājot ASV.

Eksperts3 ir tīmekļa vides komunikācijas eksperts, kurš datoru lieto, gan strādājot lielā uzņēmumā, kurā tiek veikta datorlietotāju izglītošana, gan mājās.

Eksperts4 savā ikdienas darbā ir interneta risinājumu eksperts. Ģimenes un draugu lokā ir viens no retajiem ar IT izglītību un nereti tiek aicināts palīdzēt atrisināt kādu ar datoru saistītu problēmu. Uzskatāms par datorspeciālistu-amatieri.

Eksperts5 šobrīd atbild par informācijas drošības pārvaldības procesu lielā uzņēmumā. Iepriekš ir strādājis gan lietotāju atbalsta jomā, gan bijis sistēmu administrators. Pārvalda māku sarunāties gan ar IT speciālistiem, gan datorlietotājiem.

Interviju sākumā ar ekspertiem tika pārrunāti lietotāju aptaujas rezultāti, bet turpinājumā tika apspriesti jautājumi par informācijas drošības pārvaldību un riskiem mājsaimniecībā, nepieciešamība un iespējas izglītot datorlietotājus. Intervijās apspriestie jautājumi apkopoti 16. tabulā.

16. tabula. Jautājumi ekspertiem

1.	Kāds ir informācijas drošības mērķis mājsaimniecībā?
2.	Kas ir lielākie riski?
3.	Vai piekrītat apgalvojumam "IT/informācijas drošību var pilnvērtīgi pārvaldīt tikai, ja pareizi novērtēti lielākie riski"?
4.	Cik liela ir nepieciešamība elektroniskās informācijas drošību izskaidrot ikdienas datorlietotājiem?
5.	Kā šo izskaidrošanu būtu vislabāk veikt?
6.	Vai interaktīva ekspertu sistēma noderētu?
7.	Savs "datorārsts" – pazīstama persona vai interneta vietne?
8.	Cik būtiska atbilstošas valodas izvēle?
9.	Vai mājsaimniecība ir gatava par datoru drošības pasākumiem un informācijas drošības izglītošanu maksāt?

Vairāki eksperti pauda viedokli, ka informācijas drošības mērķis mājsaimniecībā vairāk ir emocionāls, ko var raksturot ar vārdiem 'saglabāt sirdsmieru', 'nepiedzīvot kaunu', 'neielaužas visprivātākajā'. Eksperti arī norādīja, ka katram svarīgākās informācijas vērtības ir atšķirīgas. Eksperts4 un Eksperts5 norādīja, ka informācijas drošības mērķim mājsaimniecībā ir daudz līdzību ar informācijas drošību uzņēmumā, proti, atbilstoši pārvaldīt informācijas konfidencialitāti, integritāti un pieejamību.

Vairums ekspertu uzskata, ka lielākie riski ir subjektīvs rādītājs, tomēr privātā vidē "sāpīgāki" ir tie, kas apdraud cilvēku pašu. Eksperts4 to raksturoja kā nepareizu rīcību nezināšanas dēļ. Bet, piemēram, datora izmantošana botu tīklā lietotājam ir neredzama un parasti netiek uztverts kā personīgs apdraudējums. Ar tehnoloģijām saistīts risks, kas apdraud lietotāju emocionālā līmenī, ir laikā neveikta rezerves kopēšana kopā ar tehnisku iemeslu dēļ notikušu datu, piemēram, ģimenes fotogrāfiju, zudumu.

Visi eksperti piekrīt apgalvojumam, ka IT un informācijas drošību var pilnvērtīgi pārvaldīt tikai, ja ir pareizi novērtēti riski. Savukārt, lai pareizi novērtētu riskus, noteikti ir svarīgi elektroniskās informācijas drošību izskaidrot ikdienas datorlietotājiem. Eksperts2

atceras, ka, dzīvojot ASV, redzējis daudz informācijas par interneta drošības jautājumiem, un tāpēc daļa jautājumu sistēmā IDRE likušies uzdoti par pašsaprotamām lietām.

Eksperts4 saskāries ar situāciju, kur lietotājs tik ļoti uzticas savam datorspeciālistam, ka atklāj viņam vairākas paroles. Eksperts5 uzsver, ka svarīgākais ir izskaidrot, jo ir pieejams salīdzinoši daudz informācijas, KO vajadzētu darīt, arī – KĀ darīt, bet pietrūkst skaidrojuma, KĀPĒC to darīt. Otrs iemesls runāt par informācijas drošību, ir atgādināt, kā arī dot iespēju paskatīties uz potenciālo problēmu citā redzesleņķī un, iespējams, ieraudzīt risinājumu.

Eksperts3 atgādina vēsturiskus faktus, kā cilvēki tika izglītoti droši lietot elektrību vai uzvesties uz ielām, kur brauc automašīnas. Kamēr jaunā situācija vai tehnoloģija nav vispārpazīstama, ir nepieciešams veikt izglītojošus pasākumus. Bērni daudz ko apgūst skolā, bet datorus un internetu uzsāk lietot dažāda vecuma cilvēki, tāpēc nedrīkst aizmirst arī par viņu izglītošanu. Papildus Eksperts3 piebilst, ka dažkārt vienkāršs cilvēks domā, ka viņa, kā sabiedrībā nepazīstamas personas, dati datorā neinteresē citus.

Eksperts4 savā datorspeciālista darbā ir redzējis vairākas salīdzinoši jaunas ierīces, kam ir iespēja ar vienu pogas nospiedienu veikt "ātru drošu konfigurēšanu", kas ir patīkama virzība uz vienkāršāku drošības pārvaldību tehnoloģiskā līmenī. Tomēr pārejas periodā neiztikt bez izglītošanas. Turklāt cilvēka rīcībai tuvākajā nākotnē nav paredzama tāda "poga", un vispārējā izpratne par informācijas drošību ir jāattīsta.

Vairāki eksperti norāda, ka cilvēkiem ir dažādi labākie veidi, kā apgūt jaunas lietas. Daļa parasti padomu meklē pie cilvēka, tas var būt gan draugs, gan pavisam svešs, bet uzticams, piemēram, interneta pakalpojuma sniedzēja darbinieks. Daļa padomu atrod sociālajos tīklos, daļa – interešu portālos.

Eksperts2 kā iemeslu cilvēciskā kontakta izvēlei min cilvēku bailes no nepazīstamām vietām, t.sk. svešām interneta vietnēm. Eksperts1 kā iemeslu min nezināšanu, kur tieši internetā meklēt vajadzīgo padomu. Gan tiešs kontakts ar cilvēku, gan netiešs sociālajos tīklos parasti nodrošina personalizētu padomu konkrētā situācijā.

Eksperts5 atgādina, ka ne visi cilvēki grib daudz lasīt, padomiem būtu jābūt iegūstamiem ātri (arī videopamācības).

Kopumā eksperti nodala vispārējo drošības apzināšanās veicināšanu, kam noderīgi būtu, piemēram, sižeti televīzijā vai reklāmas kampaņas, un padomus konkrētam lietotājam konkrētā situācijā.

Lai piedāvātu personificētu padomu, piemērots rīks varētu būt interaktīva ekspertu sistēma. Kopumā eksperti piekrīt lietotāju aptaujas rezultātiem un atzīst, ka atbildes uz ekspertu sistēmas jautājumiem vedināja padomāt un saprast, vai drošības rīcība ir atbilstoša risku uztverei. Eksperts1 to raksturoja šādi: "Aizdomājos, ka jāveic rezerves kopijas un nopirku papildus disku.".

Kā jau minēts, katram ir savs iecienīts veids, kā saņemt padomu vai mācīties jaunas lietas. Tomēr nav iespējams viennozīmīgi atbildēt, ka visos gadījumos jāizvēlas viens risinājums. Savu reizi kā "datorārsts" labāk derēs pazīstama persona, bet citreiz ātru padomu sniegs interneta vietne. Vairāki eksperti norāda, ka vislabāk būtu izmantot abus.

Eksperts5 norāda, ka datorspeciālists var uzstādīt antivīrusa programmatūru, bet nez vai varēs daudz izskaidrot. Papildus noderētu lasāms materiāls interneta vietnē. Eksperts3 vērš uzmanību, ka garus tekstus grūti uztvert, un tieši speciālists-lektors var izstāstīt konkrētajam lietotājam svarīgāko. Eksperti piekrīt, ka interaktīva ekspertu sistēma ir viens no iespējamiem vidusceļa risinājumiem. Eksperts4 rezumē, ka interaktīva ekspertu sistēma rada interesi lietotājam un izskaidro, bet praktisko uzdevu veikšanai var pieaicināt speciālistu.

Ir svarīgi ekspertu sistēmā nelietot valodu, kas saprotama tikai IT speciālistiem, tomēr Eksperts2 norāda, ka pilnīgi izvairīties no terminiem nevajag. Ja tekstā tiks lietoti pazīstami atslēgas vārdi, piemēram, bērni, ģimenes fotogrāfijas, dokumenti, un lietotājam pašam būs vēlme uzzināt, tad arī saprasties nebūs sarežģīti.

Mājsaimniecības vēlmes un iespējas maksāt par datoru drošības pasākumiem un informācijas drošības izglītošanu ir dažādas. Un tam ir gan objektīvi, gan subjektīvi iemesli. Eksperts3 atgādina, ka joprojām spēkā ir mīts par programmatūras dārdzību, dažāda ir attieksme pret autortiesību jautājumu. Eksperts4 ir saskāries ar situāciju, kur lietotājs par datu, t.sk. mazmeitiņas fotogrāfiju, atjaunošanu no bojāta diska nebija gatavs maksāt dažus simtus latu. Eksperts2 šo raksturo, ka preventīvu pasākumu kultūra nav cieņā. Tai pašā laikā cilvēki ir gatavi maksāt par fotogrāfiju galeriju ievietošanu sociālajos tīklos. Arī par datorspeciālista pakalpojumiem cilvēki ir ar mieru maksāt.

Noslēgumā Eksperts1 piebilst: "Drošība ir neatņemama sastāvdaļa datora lietot prasmēm (*literacy*).".

Lietotāju aptaujas un ekspertu interviju rezultāti sniedz pietiekamu pamatu apgalvot, ka izstrādātā metode un tās realizācija apskatītā rīka IDRE veidā ir noderīga praktiskai izmantošanai un veicina datorlietotāju informācijas drošības apzināšanos.

4.5. Nodaļas secinājumi

Ikdienas datorlietotāji līdz šim nav bijusi informācijas drošības risku pārvaldīšanas metožu mērķauditorija. Tomēr autores pieredze dažādu līmeņu datorlietotāju izglītošanā liecina par nepieciešamību pēc kāda risinājuma, kas palīdzētu katram apgūt sev nepieciešamo daļu no tehnoloģiju speciālistu zināšanām informācijas drošības pārvaldībā.

Pavirši iepazīstoties ar internetā pieejamajiem materiāliem, liekas, ka dažādas informācijas ir daudz. Rūpīgāk analizējot, gan izrādās, ka ir atrodama informācija par katru svarīgu drošības lietu atsevišķi. Turklāt parasti tiek stāstīts par apdraudējumu un risinājumiem tā mazināšanai, neņemot vērā, cik būtiskus riskus tas varētu radīt konkrētam lietotājam.

Nodaļā aprakstīta informācijas drošības riska novērtēšanas metode privātai videi, kas balstās uz informācijas drošības pārvaldības modeli mājsaimniecībai, un palīdz novērtēt gan riskus saistībā ar apdraudējumiem datoram, gan ikdienas datorlietotāja rīcību ar elektronisko informāciju.

Metode izmanto jautājumus ar atbilžu variantu izvēli, speciālistu analītisku darbu gan risku saraksta izstrādē, gan turpmākā jautājumu pilnveidē. Metode ietver šādus posmus: elektroniskās vides raksturošana, apdraudējumu un ievainojamību identificēšana, drošības vadīklu apzināšana, drošības vadīklu analīze un iespējamību noteikšana, ietekmju analīze, risku noteikšana un drošības vadīklu ieteikšana. Risku iespējamību un ietekmi mēra trīs līmeņos. Augsta līmeņa riskiem jāveic tūlītēji pasākumi situācijas uzlabošanai, vidēja līmeņa riskiem pasākumu veikšana atkarīga no to izmaksām un lietotāja attieksmes pret risku.

Metode aprobēta, izstrādājot risku novērtēšanas rīku IDRE. Sistēmas sniegtais rezultāts novērtēts, aptaujājot lietotājus un ekspertus. Gan lietotāji, gan eksperti apstiprina, ka rīka IDRE sniegtie padomi ir noderīgi un veicina informācijas drošības apzināšanos.

Šāda tipa rīka noderīgumu apliecina arī publikācija [MAG12], kas apraksta līdzīgu ideju vienkāršam tīmekļa rīkam. Šī darba ietvaros aprakstītais rīks publiski internetā bija pieejams kopš 2011. gada augusta (šobrīd vietnē http://idre.github.io/#/), bet ideja publicēta vēl agrāk. Savukārt [MAG12] pirmo reizi publicēts *10th Australian Information Security Management Conference* materiālos 2012. gada decembrī.

NOBEIGUMS

Promocijas darba mērķis bija izstrādāt pieeju, kā veicināt informācijas drošības apzināšanos privātā vidē, informācijas drošības risku novērtēšanas metodi un sistēmu (rīku), kas palīdz atbildību par drošību realizēt, sniedzot praktiskus padomus, kas pielāgoti ikdienas datorlietotāja vajadzībām.

Promocijas darba izstrādes gaitā izpildīti visi plānotie uzdevumi:

- analizēti pētījumi par datorlietotāju informācijas drošības apzināšanās veicināšanu un informācijas drošības pārvaldību mājsaimniecībās;
- apskatīti labās prakses piemēri uzņēmējdarbības vides pieredzē informācijas drošības pārvaldībā un informācijas drošības apzināšanās veicināšanā;
- apskatīti dažādi informācijas drošības pārvaldības modeļu veidi, t.sk. piekļuves vadības, konfidencialitātes un integritātes modeļi un Latvijā populāri informācijas drošības pārvaldības standarti;
- balstoties uz uzņēmējdarbības vidē populāru informācijas drošības pārvaldības standartu, izveidots formalizēts konceptuālais modelis informācijas drošības pārvaldībai uzņēmumā;
- izveidots formalizēts konceptuālais modelis, ko var izmantot ikdienas datorlietotāju izglītošanas procesā;
- izstrādātas vadlīnijas informācijas drošības pārvaldībai mājsaimniecībā, kas var kalpot kā veicamo uzdevumu pārskats un atgādinājums neaizmirst svarīgus darbus;
- izpētīti statistikas dati par informācijas tehnoloģiju pielietojumu privātā vidē un apzināti informācijas tehnoloģiju apdraudējumi, kas ir būtiski privātā vidē;
- izstrādāta metode informācijas drošības risku pārvaldībai ikdienas datorlietotājam, kas ietver jomas ekspertu sagatavotas informācijas un paša datorlietotāja sniegtu atbilžu izmantošanu;
- informācijas risku novērtēšanas metode aprobēta, izstrādājot praktiski izmantojamu sistēmas prototipu (rīku IDRE), ar ko katrs ikdienas datorlietotājs var novērtēt riskus savas elektroniskās informācijas drošībai un saņemt drošības pilnveidošanas ieteikumus;
- informācijas drošības risku novērtēšanas metode un rīks novērtēti, aptaujājot lietotājus un nozares ekspertus.

Darba galvenais rezultāts ir jauna pieeja ikdienas datorlietotāja elektroniskās informācijas drošības apzināšanās veicināšanai un pārvaldībai, kas sastāv no informācijas drošības pārvaldības formalizēta modeļa un vadlīnijām mājsaimniecībai, ko var izmantot drošības apzināšanās pasākumu plānošanai un izpratnes veicināšanai, un informācijas drošības risku novērtēšanas metodes, kas aprobēta kā tīmekļa lietojumprogrammas prototips (rīks), ar ko katrs ikdienas datorlietotājs var novērtēt riskus savas elektroniskās informācijas drošībai un saņemt drošības pilnveidošanas ieteikumus.

Tēzi "Ir nepieciešams un, balstoties uz uzņēmējdarbības vides pieredzi, ir izveidojams risinājums, lai pilnveidotu informācijas drošības pārvaldības procesu mājsaimniecībā" apstiprina literatūras analīzē, standartu izpētē balstītie secinājumi un izstrādātais formalizētais modelis informācijas drošības pārvaldībai mājsaimniecībā.

Tēzi "Ikdienas datorlietotāja informācijas drošības apzināšanos iespējams uzlabot, izmantojot informācijas risku novērtēšanas metodi, kas realizēta kā praktiski izmantojama tīmekļa lietojumprogramma." apstiprina izstrādātā metode, tās aprobācija ar rīku IDRE, kas novērtēts ar aptauju palīdzību. Rīks IDRE ir pieejams ikvienam LR Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas CERT.LV uzturētā vietnē "Esi drošs" [ED].

Promocijas darba saturs parāda, ka formulētie uzdevumi, izpildīti izvirzītās tēzes apstiprinātas un darba mērķis ir sasniegts.

Pētījuma atziņas publicētas piecos zinātniskos rakstos un referētas piecās zinātniskās konferencēs.

Būtiskākie autores secinājumi par informācijas drošības apzināšanās sistēmu ikdienas datorlietotājam ir šādi:

- pilnvērtīgai informācijas drošības pārvaldībai nepietiek tikai ar tehnoloģiju rīkiem, nepieciešama to lietotāju atbildības apzināšanās;
- mājsaimniecības informācijas drošības pārvaldības modelis var veicināt izpratnes attīstību par līdzīgo un atšķirīgo informācijas drošības pārvaldībā uzņēmumā un privātā vidē;
- ikdienas datorlietotājam informācijas drošības risku novērtēšanai ir nepieciešams palīgs, un šo lomu var pildīt risku novērtēšanas rīks.

IZMANTOTĀ LITERATŪRA

Autores publikācijas

[IM08] Murane I., Raising Awareness in Information Security: Everyone Should Participate// Proceedings of the 2008 International Conference on Security and Management. – Las Vegas, USA, 2008, pp. 190-195.

[IM09] Murane I., A New Element in Information Security Process Security Aware Smart Household Employee// Proceedings of the 2009 International Conference on Security and Management. – Las Vegas, USA, 2009, pp. 46-51.

[IM10] Murane I., New Responsibility for a Household: Information Security Management// Proceedings of the Ninth International Baltic Conference on Databases and Information Systems (Baltic DB&IS'2010). – Riga, Latvia, 2010, pp. 187–201.

[IM11a] Murane I., Information Security Management Method for Households// Databases and Information Systems VI: Selected Papers from the Ninth International Baltic Conference, DB&IS 2010. – Riga, Latvia, 2011, pp. 353-366.

[IM11b] Murane I., Raising information security awareness of society: organisations could be important participants//Proceedings of the 2011 European Security Conference (ESC'11). – Örebro, Sweden, 2011, pp. 6-17.

[BAR07] Bārzdiņš G., Murāne I., Jauno tehnoloģiju ēnas puses// LU žurnāls Latvijas Vēsture 2007 1(65). – Rīga, Latvija, 2007, 33.-37. lpp.

Citu autoru publikācijas

[AND04] Anderson R.J., Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition. – Wiley, 2008.

[AND09] Anderson R., Information security: where computer science, economics and psychology meet// Philosophical Transactions: Mathematical, Physical & Engineering Sciences, Jul2009, Vol. 367 Issue 1898. – Royal Society Publishing, 2009, pp. 2717-2727.

[ATK09] Atkinson S., Furnell S.M., Phippen A.D., E-Safety and E-Security: Raising security awareness among young people using peer education// Proceedings of the Annual Security Conference. Dhillon, G. "Security, Assurance and Privacy: organizational challenges". April 15-17 2009. – DC: Information Institute Publishing, 2009.

[AUS10] Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime, pieejams tiešsaistē (08.02.2015.) http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms/cybercrime/report.htm

[BEA08] Beautement A., Sasse M. A., Wonham M., The Compliance Budget: Managing Security Behaviour in Organisations// Proceedings of the 2008 workshop on New security paradigms. – ACM, New York, USA, 2008, pp. 47-58.

[BeOS] pieejams tiešsaistē (08.02.2015.) http://www.squidoo.com/best-operating-systems

[BER09] Berthold S., Böhme R., Valuating Privacy with Option Pricing Theory, pieejams tiešsaistē (08.02.2015.) http://www1.inf.tu-dresden.de/~rb21/publications/BB2009_PrivacyOptions_WEIS.pdf

[BJO05] Björck F. J., Discovering Information Security Management// Department of Computer and Systems Sciences Stockholm University & Royal Institute of Technology Report series No. 05-010. – Stockholm, 2005.

[BOS02] Computer security handbook, edited by Bosworth S., Kabay M.E.. – New York, Wiley, 2002.

[BOY07] Boyd D., Why youth (heart) social network sites: the role of networked publics in teenage social life// MacArthur Foundation Series on Digital Learning: Youth, Identity, and Digital Media Volume (ed. David Buckingham). – Cambridge, MA, 2007.

[BRI00] McBride P., How to Spend a Dollar on Security// Computerworld, November 9, 2000, pieejams tiešsaistē (08.02.2015.) http://www.computerworld.com/s/article/53651/How_to_Spend_a_Dollar_on_Security_

[BRY09] Bryce J., Klang M., Young people, disclosure of personal information and online privacy: Control, choice and consequences// Information Security Technical Report, Aug2009, Vol. 14 Issue 3. – Elsevier Advanced Technology Publications, Oxford, UK, 2009, pp. 160-166.

[CERT] pieejams tiešsaistē (08.02.2015.) http://www.cert.lv/section/show/90

[COBIT] COBIT, pieejams tiešsaistē (08.02.2015.) https://cobitonline.isaca.org/

[CobSB] COBIT Security Baseline, pieejams tiešsaistē (08.02.2015.)

http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT-Security-Baseline-2ndEd-Research-18Sept07.pdf?Token=248FF24F-4CAE-4B31-A820-9AD99E560372

[CoVul] Secunia Vulnerability Review 2013, pieejams tiešsaistē (19.03.2015.) http://secunia.com/?action=fetch&filename=Secunia_Vulnerability_Review_2013.pdf

[CRA08] Cranor L. F., A Framework for Reasoning About Human in the Loop, pieejams tiešsaistē (08.02.2015.) http://www.usenix.org/events/upsec08/tech/full_papers/cranor/cranor.pdf

[CSP1] Statistikas datubāzes: Informācijas tehnoloģijas, pieejams tiešsaistē (08.02.2015.) http://www.csb.gov.lv/statistikas-temas/informacijas-tehnologijas-datubaze-30129.html

[CSR11] 2011 Top Cyber Security Risks Report, pieejams tiešsaistē (08.02.2015.) http://www.hpenterprisesecurity.com/collateral/report/2011FullYearCyberSecurityRisksReport.pdf

[CSR13a] Hatchimonji G., Biggest data security threats come from inside, report says, pieejams tiešsaistē (08.02.2015.) http://www.pcworld.com/article/2054462/biggest-data-security-threats-come-from-inside-report-says.html

[CSR13b] pieejams tiešsaistē (08.02.2015.) http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/ENISA_Threat_Landscape

[CSR13c] SOPHOS Security Threat Report 2013, pieejams tiešsaistē (08.02.2015.) http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

[CSR15] Our top 10 predictions for security threats in 2015 and beyond, pieejams tiešsaistē (08.02.2015.) http://blogs.sophos.com/2014/12/11/our-top-10-predictions-for-security-threats-in-2015-and-beyond/

[DOU04] Dourish P., Grinter R. E., Delgado de la Flor J., Joseph M., Security in the wild: user strategies for managing security as an everyday, practical problem// Journal Personal and Ubiquitous Computing archive, Volume 8 Issue 6, November 2004. – Springer-Verlag, London, UK, 2004, pieejams tiešsaistē (08.02.2015.)

http://www-static.cc.gatech.edu/~beki/j8.pdf

[ED] pieejams tiešsaistē (08.02.2015.) www.esidross.lv

[ENISAAR] Awareness Raising Quizzes Templates: Targeting Parents, End-users and SMEs, pieejams tiešsaistē (08.02.2015.) https://www.enisa.europa.eu/publications/archive/ar-quizzes-templates-da

[ENISAPP] ENISA Position Papers, pieejams tiešsaistē (08.02.2015.) https://www.enisa.europa.eu/activities/identity-and-trust/library/pp

[FKTK] pieejams tiešsaistē (08.02.2015.)

http://www.fktk.lv/lv/tiesibu_akti/vispareja/fktk_izdotie_noteikumi/20021022_finansu_un_kapitala_t/

[FPDAL] Fizisko personu datu aizsardzības likums, pieejams tiešsaistē (08.02.2015.) http://likumi.lv/doc.php?id=4042

[Gar06] New Gartner Hype Cycle Highlights Five High Impact IT Security Risks, pieejams tiešsaistē (08.02.2015.)

http://www.gartner.com/it/page.jsp?id=496247

[GLI10] Bryan Glick, Users remain the weakest link in the IT security chain, pieejams tiešsaistē (08.02.2015.) http://www.computerweekly.com/blogs/editors-blog/2010/03/users-remain-the-weakest-link.html

[GMst] Google Milestones, pieejams tiešsaistē (08.02.2015.)

www.google.com/corporate/history.html

[GRA10] Grant, Gordon J., Ascertaining the relationship between security awareness and the security behavior of individuals. – Nova Southeastern University, 2010

[HIL09] Hilton J., Improving the secure management of personal data: Privacy on-line IS important, but it's not easy// Journal Information Security Techical Report Volume 14 Issue 3, August, 2009. – Elsevier Advanced Technology Publications, Oxford, UK pp. 124-130.

[HOW12] Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, Zinta Byrne, The Psychology of Security for the Home Computer User// IEEE Symposium on Security and Privacy, pp. 209-223, IEEE Computer Society, 2012, pieejams tiešsaistē (08.02.2015.) http://www.ieee-security.org/TC/SP2012/papers/4681a209.pdf

[IDRE] pieejams tiešsaistē (08.02.2015.) http://idre.github.io/#/

[InSec] pieejams tiešsaistē (08.02.2015.) http://www.infosecuregroup.com/index.php?id=21

[ISAP06] Par Informācijas sabiedrības attīstības pamatnostādnēm 2006.-2013. gadam, pieejams tiešsaistē (21.05.2015.) http://likumi.lv/doc.php?id=140215

[ISAP14] Par Informācijas sabiedrības attīstības pamatnostādnēm 2014..-2020. gadam, pieejams tiešsaistē (21.05.2015.) http://likumi.lv/doc.php?id=260931

[ISFSt] ISF Standard of Good Practice for Information Security, pieejams tiešsaistē (08.02.2015.) https://www.securityforum.org/userfiles/public/2007_sogp_pub.pdf

[ISF] pieejams tiešsaistē (08.02.2015.) https://www.securityforum.org/

[ISO27002] An Introduction to ISO 27001, ISO 27002....ISO 27008, pieejams tiešsaistē (08.02.2015.) http://www.27000.org

[ITDL] Informācijas tehnoloģiju drošības likums, pieejams tiešsaistē (18.03.2015.) http://likumi.lv/doc.php?id=220962

[INT13] http://nomadcapitalist.com/2013/12/01/top-5-countries-fastest-internet-speeds-world/

[JAC04] Jacobsson A., Exploring Privacy Risks in Information Networks, pieejams tiešsaistē (08.02.2015.)

http://www.bth.se/fou/forskinfo.nsf/0/80533d43ac292724c125707f003aafbd/$FILE/Avhandling.pdf

[JAC08] Jacobsson A., Privacy and Security in Internet-Based Information Systems, pieejams tiešsaistē (08.02.2015.)

http://www.bth.se/fou/forskinfo.nsf/all/f26dd7141e165324c12573f6002db90c/$file/Jacobsson_diss.pdf

[JOH09] Johnston A.C., Hale R., Improved security through information security governance//Communications of the ACM, Volume 52 Issue 1, January 2009 – ACM, New York, USA.

[JOH07] Johnson M.E. Goetz E., Embedding Information Security into the Organisation//IEEE Security& Privacy May/June 2007, pp 16 – 24, pieejams tiešsaistē (08.02.2015.) www.ists.dartmouth.edu/library/352.pdf

[JOH08] Johnson M.E., McGuire D., Willey N.D., The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users//Proceedings of the 41st Hawaii International Conference on System Sciences. – IEEE Computer Society Washington, DC, USA, 2008.

[Kab09] Kabooza Global Backup Survey, pieejams tiešsaistē (08.02.2015.) http://www.kabooza.com/globalsurvey.html

[KAP10] Dan Kaplan, Weakest link: End-user education, pieejams tiešsaistē (08.02.2015.) http://www.scmagazine.com/weakest-link-end-user-education/article/161685/

[KDS14] Par pamatnostādnēm "Latvijas kiberdrošības stratēģija 2014.-2018. gadam", pieejams tiešsaistē (08.02.2015.), http://doc.mod.gov.lv/lv/brosuras/kiberstrategija_2014/files/Kiberdrosibas_strategija.pdf

[KIL14] Killilea, A., Sussman, H.E., Trendy “Cybersecurity” Versus Traditional “Information Security” Two Sides of the Same Security Coin, pieejams tiešsaistē (08.02.2015.) http://www.jdsupra.com/legalnews/trendy-cybersecurity-versus-traditiona-45143/

[KOL09] Kolkowska, E.. Lack of compliance with IS security rules-value conflicts in Social Services in Sweden//Proceedings of the Annual Security Conference. Dhillon, G. "Security, Assurance and Privacy: organizational challenges". April 15-17 2009. – DC: Information Institute Publishing, 2009.

[KRI10] Kritzinger, E., Von Solms, S.H., Cyber security for home users: A new way of protection through awareness enforcement//Computers & Security, Volume 29, Issue 8, November 2010., pp. 840-847.

[KRU08] Kruck S.E., Teer F.P., Computer Security Practices and Perceptions of the Next Generation of Corporate Computer Users//International Journal of Information Security and Privacy, 2008. Vol. 2, Iss. 1.

[KRU10] Krūmiņš I., Bluetooth drošība, pieejams tiešsaistē (08.02.2015.) http://www.netsafe.lv/upload/materiali/bluetooth_drosiba.pdf

[LEE07] The History of Information Security, Edited By Karl de Leeuw, Jan Bergstra. – Elsevier, 2007.

[MAG12] Magaya, R. T., Clarke, N. L., Web-Based Risk Analysis for Home Users// 10th Australian Information Security Management Conference, Perth, December 3-5, 2012, pieejams tiešsaistē (18.03.2015.) http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1138&context=ism

[MAZ09] Maziņa L., Drošības politikas izstrāde mājas datorlietotājam, kursa darbs LU Datorikas fakultātē, 2009

[MD09] Mājas datora drošība, pieejams tiešsaistē (08.02.2015.) http://datoradrosiba.wordpress.com/

[MEE09] Mee W.J., A Methodology to Assess Security Awareness in the Organization// Proceedings of the Annual Security Conference. Dhillon, G. "Security, Assurance and Privacy: organizational challenges". April 15-17 2009. – DC: Information Institute Publishing, 2009.

[MSddv] pieejams tiešsaistē (08.02.2015.) http://windows.microsoft.com/en-US/windows7/taking-control-of-computer-security

[MUR10] Murzins V., Populārākie apdraudējumi mājas datoram, kursa darbs LU Datorikas fakultātē, 2010

[NDK11] pieejams tiešsaistē (08.02.2015.) http://www.likumi.lv/doc.php?id=227460

[NetS] NetSafe, pieejams tiešsaistē (08.02.2015.) http://www.drossinternets.lv/page/53

[NIST] pieejams tiešsaistē (08.02.2015.) http://csrc.nist.gov/

[NISTCS] Underlying Technical Models for Information Technology Security, pieejams tiešsaistē (08.02.2015.) http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

[NISTRM] pieejams tiešsaistē (08.02.2015.) http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[NISTTerm] Glossary of Key Information Security Terms, pieejams tiešsaistē (08.02.2015.) http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[OECD02] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, pieejams tiešsaistē (08.02.2015.) http://www.oecd.org/dataoecd/16/22/15582260.pdf

[PIR08] Pirim T., James T., Boswell K., Reithel B., Barkhi R., An Empirical Investigation of an Individual's Perceived Need for Privacy and Security// International Journal of Information Security and Privacy, 2008, Vol. 2, Iss. 1, pp. 42-53

[PK] Cik personisks ir personas kods, pieejams tiešsaistē (08.02.2015.) http://www.juristavards.lv/doc.php?id=214594

[PUR09] Purene Z., Mājas datorlietotāja izglītošana, kursa darbs LU Datorikas fakultātē, 2009

[PWC13] Raising security awareness in your employees, pieejams tiešsaistē (19.03.2015.)

http://www.pwc.ch/user_content/editor/files/publ_adv/pwc_raising_security_awareness_e.pdf

[QUI05] Quigley M., Information Security and Ethics: social and organizational issues. – Hershey, London, IRM Press, 2005

[Re08] Research 2008: "Safer Internet for Children and Youth", pieejams tiešsaistē (08.02.2015.) http://www.netsafe.lv/page/117

[SANS] Critical Security Controls for Effective Cyber Defense, pieejams tiešsaistē (08.02.2015.) http://www.sans.org/critical-security-controls/?ref=top20#summary

[SCH] Schneir B., The Psychology of Security, pieejams tiešsaistē (08.02.2015.) http://www.schneier.com/essay-155.pdf

[SCH03] Schlienger T., Teufel S., Information security culture – from analysis to change// Proceedings of ISSA 2003, 3rd Annual Information Security South Africa Conference. – 2003, pp. 183 - 195.

[SE09] Information security in Sweden: Situational assessment 2009, pieejams tiešsaistē (08.02.2015.) https://www.msb.se/RibData/Filer/pdf/25357.pdf

[SIN07] Sinclair S., Smith S.W., Trudeau S., Johnson M.E., Portera A., Information Risk in the Professional Services – Field Study Results from Financial Institutions and a Roadmap for Research, pieejams tiešsaistē (08.02.2015.) http://www.cs.dartmouth.edu/~sws/pubs/sstjp07.pdf

[SInt] Safer Internet plus Programme, pieejams tiešsaistē (08.02.2015.) http://ec.europa.eu/information_society/activities/sip/index_en.htm

[SMI05] Šmite D., Dosbergs D., Borzovs J. Informācijas un komunikācijas tehnoloģiju nozares tiesību un standartu pamati. – LU akadēmiskais apgāds, LU, 2005.

[SocE] Social Engineering, pieejams tiešsaistē (08.02.2015.) http://www.securityfocus.com/infocus/1527

[Stat1] pieejams tiešsaistē (18.03.2015.) http://stats.oecd.org/glossary/detail.asp?ID=1255

[Stat2] pieejams tiešsaistē (18.03.2015.) http://www.csb.gov.lv/statistikas-temas/termini/privata-majsaimnieciba-majsaimnieciba-35257.html

[StWorm] Storm worm botnet threatens national security?, pieejams tiešsaistē (08.02.2015.) http://www.zdnet.com/article/storm-worm-botnet-threatens-national-security/

[SW] pieejams tiešsaistē (08.02.2015.) http://www.symantec.com/security_response/writeup.jsp?docid=2001-060615-1534-99

[SZE09] Szewczyk P., Assessing the online security awareness of Australian Internet users// Proceedings of the Annual Security Conference. Dhillon, G. "Security, Assurance and Privacy: organizational challenges". April 15-17 2009. – DC: Information Institute Publishing, 2009.

[TAL10] Talib S., Clarke N.L., Furnell S.M., An analysis of information security awareness within home and work environments// Proceedings of ARES 2010 - 5th International Conference on Availability, Reliability, and Security, pp. 196-203.

[Term] Terminoloģijas portāls, pieejams tiešsaistē (08.02.2015.) http://www.termnet.lv/Term.aspx?tabindex=1&subject=44

[TEx] Threat Explorer, pieejams tiešsaistē (08.02.2015.) http://www.symantec.com/norton/security_response/threatexplorer/threats.jsp

[ThrCat] Threats Catalogue – Elementary Threats, pieejams tiešsaistē (08.02.2015.) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile

[UML] pieejams tiešsaistē (08.02.2015.) http://www.agilemodeling.com/artifacts/classDiagram.htm

[Ver08] 2008 data breach investigations report, pieejams tiešsaistē (08.02.2015.) http://www.verizonbusiness.com/resources/security/databreachreport.pdf

[Vispa] Brit ISP knocked offline by Latvian DDOS, pieejams tiešsaistē (08.02.2015.) http://www.theregister.co.uk/2010/01/08/vispa_ddoa/

[VW10] Virus Watch, pieejams tiešsaistē (08.02.2015.) http://www.kaspersky.com/viruswatchlite?hour_offset=-1

[Web2.0] pieejams tiešsaistē (08.02.2015.) http://www.net-security.org/dl/articles/Web2_0Security.pdf

[WEIS09] The Eighth Workshop on the Economics of Information Security (WEIS 2009), pieejams tiešsaistē (08.02.2015.) http://weis09.infosecon.net/programme.html

[WES10] Wester M., Assessing acceptance of privacy-invasive technology// Proceedings of the 1st Security Conference – Europe. Örebro, Sweden, August 15-17, 2010.

[WOL10] Wolf M., Measuring an information security awareness program// University of Nebraska at Omaha, 2010.

[WHI10] Whitman M. E., Mattord H. J., Management of information security. – Thomson/Course Technology, Boston, MA, 2010.

[YOU09] Young A.L., Quan-Haase A., Information revelation and internet privacy concerns on social network sites: a case study of facebook// C&T '09 Proceedings of the fourth international conference on Communities and technologies. – ACM, NY, 2009.

PIELIKUMI

1. ISF standarta nodaļas

Security Management	**Drošības pārvaldība**
SM1 High-level Direction	*SM1 Augsta līmeņa norādījumi*
SM1.1 Management commitment	SM1.1 Vadības apņemšanās
SM1.2 Information security policy	SM1.2 Informācijas drošības politika
SM1.3 Staff agreements	SM1.3 Personāla līgumi
SM2 Security Organisation	*SM2 Drošības organizācija*
SM2.1 High-level control	SM2.1 Augsta līmeņa vadība
SM2.2 Information security function	SM2.2 Informācijas drošības funkcija
SM2.3 Local security co-ordination	SM2.3 Vietējā drošības koordinēšana
SM2.4 Security awareness	SM2.4 Drošības apzināšanās
SM2.5 Security education / training	SM2.5 Drošības izglītība/apmācības
SM3 Security Requirements	*SM3 Drošības prasības*
SM3.1 Information classification	SM3.1 Informācijas klasificēšana
SM3.2 Ownership	SM3.2 Īpašumtiesības
SM3.3 Managing information risk analysis	SM3.3 Informācijas riska analīzes process
SM3.4 Information risk analysis methodologies	SM3.4 Informācijas riska analīzes metodes
SM3.5 Legal and regulatory compliance	SM3.5 Tiesiskā un uzraudzības regulējuma atbilstība
SM4 Secure Environment	*SM4 Droša vide*
SM4.1 Security architecture	SM4.1 Drošības arhitektūra
SM4.2 Information privacy	SM4.2 Informācijas privātums
SM4.3 Asset management	SM4.3 Vērtību pārvaldība
SM4.4 Identity and access management	SM4.4 Identitātes un piekļuves vadība
SM4.5 Physical protection	SM4.5 Fiziskā aizsardzība
SM4.6 Information security incident management	SM4.6 Informācijas drošības incidentu pārvaldība
SM4.7 Business continuity	SM4.7 Uzņēmējdarbības nepārtrauktība
SM5 Malicious Attack	*SM5 Ļaunprātīgi uzbrukumi*
SM5.1 General malware protection	SM5.1 Vispārēja ļaunprogrammatūras aizsardzība
SM5.2 Malware protection software	SM5.2 Ļaunprogrammatūras aizsardzības programmatūra
SM5.3 Intrusion detection	SM5.3 Ielaušanās atklāšana
SM5.4 Emergency response	SM5.4 Reaģēšana neparedzētās situācijās
SM5.5 Forensic investigations	SM5.5 Pirmstiesas izmeklēšana
SM5.6 Patch management	SM5.6 Ielāpu pārvaldība

SM6 Special Topics	*SM6 Īpašas tēmas*
SM6.1 Cryptographic solutions	SM6.1 Kriptogrāfijas risinājumi
SM6.2 Public key infrastructure	SM6.2 Publisko atslēgu infrastruktūra
SM6.3 E-mail	SM6.3 E-pasts
SM6.4 Remote working	SM6.4 Attālināts darbs
SM6.5 Third party access	SM6.5 Trešo pušu piekļuve
SM6.6 Electronic commerce	SM6.6 Elektroniskā komercija
SM6.7 Outsourcing	SM6.7 Ārpakalpojumi
SM6.8 Instant messaging	SM6.8 Tūlītējā ziņapmaiņa
SM7 Management Review	*SM7 Pārskati vadībai*
SM7.1 Security audit / review	SM7.1 Drošības audits/apskats
SM7.2 Security monitoring	SM7.2 Drošības pārraudzība
Critical Business Applications	**Kritiskās biznesa lietojumprogrammas**
CB1 Business requirements for security	*CB1 Biznesa prasības drošībai*
CB1.1 Confidentiality requirements	CB1.1 Konfidencialitātes prasības
CB1.2 Integrity requirements	CB1.2 Integritātes prasības
CB1.3 Availability requirements	CB1.3 Pieejamības prasības
CB2 Application Management	*CB2 Lietojumprogrammu pārvaldība*
CB2.1 Roles and responsibilities	CB2.1 Lomas un pienākumi
CB2.2 Application controls	CB2.2 Lietojumprogrammu vadīklas
CB2.3 Change management	CB2.3 Pārmaiņu vadība
CB2.4 Information security incident management	CB2.4 Informācijas drošības incidentu pārvaldība
CB2.5 Business continuity	CB2.5 Uzņēmējdarbības nepārtrauktība
CB2.6 Sensitive information	CB2.6 Jutīga informācija
CB3 User Environment	*CB3 Lietotāju vide*
CB3.1 Access control	CB3.1 Piekļuves kontrole
CB3.2 Application sign-on process	CB3.2 Lietojumprogrammu pierakstīšanās process
CB3.3 Workstation protection	CB3.3 Darbstaciju aizsardzība
CB3.4 Security awareness	CB3.4 Drošības apzināšanās
CB4 System Management	*CB4 Sistēmu pārvaldība*
CB4.1 Service agreements	CB4.1 Pakalpojumu līgumi
CB4.2 Resilience	CB4.2 Elastīgums
CB4.3 External connections	CB4.3 Ārējie pieslēgumi
CB4.4 Back-up	CB4.4 Rezerves kopēšana
CB5 Local Security Management	*CB5 Vietējā drošības pārvaldība*
CB5.1 Local security co-ordination	CB5.1 Vietējā drošības koordinēšana
CB5.2 Information classification	CB5.2 Informācijas klasificēšana
CB5.3 Information risk analysis	CB5.3 Informācijas risku analīze
CB5.4 Security audit / review	CB5.4 Drošības audits/apskats
CB6 Special Topics	*CB6 Īpašas tēmas*

CB6.1 Third party agreements	CB6.1 Trešo pušu līgumi
CB6.2 Cryptographic key management	CB6.2 Kriptogrāfisko atslēgu pārvaldība
CB6.3 Public key infrastructure	CB6.3 Publisko atslēgu infrastruktūra
CB6.4 Web-enabled applications	CB6.4 Tīmekļa lietojumprogrammas
Computer Installations	**Datoru iekārtas**
CI1 Installation Management	*CI1 Iekārtu pārvaldība*
CI1.1 Roles and responsibilities	CI1.1 Lomas un pienākumi
CI1.2 Service agreements	CI1.2 Pakalpojumu līgumi
CI1.3 Asset management	CI1.3 Vērtību pārvaldība
CI1.4 System monitoring	CI1.4 Sistēmu monitorings
CI2 Live Environment	*CI2 Dzīvā vide*
CI2.1 Installation design	CI2.1 Instalāciju dizains
CI2.2 Security event logging	CI2.2 Drošības notikumu reģistrēšana
CI2.3 Host system configuration	CI2.3 Saimnieksistēmas konfigurēšana
CI2.4 Workstation protection	CI2.4 Darbstaciju aizsardzība
CI2.5 Resilience	CI2.5 Elastīgums
CI2.6 Hazard protection	CI2.6 Briesmu aizsardzība
CI2.7 Power supplies	CI2.7 Barošanas bloki
CI2.8 Physical access	CI2.8 Fiziskā piekļuve
CI3 System Operation	*CI3 Sistēmu darbināšana*
CI3.1 Handling computer media	CI3.1 Darbs ar datoru ārējām ierīcēm
CI3.2 Back-up	CI3.2 Rezerves kopēšana
CI3.3 Change management	CI3.3 Pārmaiņu pārvaldība
CI3.4 Information security incident management	CI3.4 Informācijas drošības incidentu pārvaldība
CI3.5 Emergency fixes	CI3.5 Avārijas labojumi
CI3.6 Patch management	CI3.6 Ielāpu pārvaldība
CI4 Access Control	*CI4 Piekļuves kontrole*
CI4.1 Access control arrangements	CI4.1 Piekļuves kontroles kārtība
CI4.2 User authorisation	CI4.2 Lietotāju atļaujas
CI4.3 Access privileges	CI4.3 Piekļuves privilēģijas
CI4.4 Sign-on process	CI4.4 Pierakstīšanās process
CI4.5 User authentication	CI4.5 Lietotāju autentifikācija
CI5 Local Security Management	*CI5 Vietējā drošības pārvaldība*
CI5.1 Local security co-ordination	CI5.1 Vietējā drošības koordinēšana
CI5.2 Security awareness	CI5.2 Drošības apzināšanās
CI5.3 Information classification	CI5.3 Informācijas klasificēšana
CI5.4 Information risk analysis	CI5.4 Informācijas risku analīze
CI5.5 Security audit / review	CI5.5 Drošības audits/apskats
CI6 Service Continuity	*CI6 Pakalpojumu nepārtrauktība*
CI6.1 Contingency plans	CI6.1 Ārkārtas situāciju rīcības plāni
CI6.2 Contingency arrangements	CI6.2 Ārkārtas pasākumi

CI6.3 Validation and maintenance	CI6.3 Validēšana un uzturēšana
Networks	**Datortīkli**
NW1 Network Management	*NW1 Datortīklu pārvaldība*
NW1.1 Roles and responsibilities	NW1.1 Lomas un pienākumi
NW1.2 Network design	NW1.2 Datortīkla dizains
NW1.3 Network resilience	NW1.3 Datortīkla elastība
NW1.4 Network documentation	NW1.4 Datortīkla dokumentācija
NW1.5 Service providers	NW1.5 Pakalpojumu sniedzēji
NW2 Traffic Management	*NW2 Datplūsmas vadība*
NW2.1 Configuring network devices	NW2.1 Tīkla ierīču konfigurēšana
NW2.2 Firewalls	NW2.2 Ugunsmūri
NW2.3 External access	NW2.3 Ārējās piekļuves
NW2.4 Wireless access	NW2.4 Bezvadu piekļuves
NW3 Network Operations	*NW3 Datortīkla darbināšana*
NW3.1 Network monitoring	NW3.1 Datortīkla monitorēšana
NW3.2 Change management	NW3.2 Pārmaiņu vadība
NW3.3 Information security incident management	NW3.3 Informācijas drošības incidentu pārvaldība
NW3.4 Physical security	NW3.4 Fiziskā drošība
NW3.5 Back-up	NW3.5 Rezerves kopēšana
NW3.6 Service continuity	NW3.6 Pakalpojumu nepārtrauktība
NW3.7 Remote maintenance	NW3.7 Attālināta uzturēšana
NW4 Local Security Management	*NW4 Vietējā drošības pārvaldība*
NW4.1 Local security co-ordination	NW4.1 Vietējās drošības koordinēšana
NW4.2 Security awareness	NW4.2 Drošības apzināšanās
NW4.3 Information classification	NW4.3 Informācijas klasificēšana
NW4.4 Information risk analysis	NW4.4 Informācijas risku analīze
NW4.5 Security audit / review	NW4.5 Drošības audits/apskats
NW5 Voice Networks	*NW5 Balss tīkli*
NW5.1 Voice network documentation	NW5.1 Balss tīklu dokumentācija
NW5.2 Resilience of voice networks	NW5.2 Elastīgums balss tīklos
NW5.3 Special voice network controls	NW5.3 Īpašā balss tīklu kontrole
NW5.4 Voice over IP (VoIP) networks	NW5.4 Balss IP tīklā
Systems Development	**Sistēmu attīstība**
SD1 Development Management	*SD1 Attīstības pārvaldība*
SD1.1 Roles and responsibilities	SD1.1 Lomas un pienākumi
SD1.2 Development methodology	SD1.2 Izstrādes metodes
SD1.3 Quality assurance	SD1.3 Kvalitātes nodrošināšana
SD1.4 Development environments	SD1.4 Izstrādes vides
SD2 Local Security Management	*SD2 Vietējā drošības pārvaldība*
SD2.1 Local security co-ordination	SD2.1 Vietējā drošības koordinēšana
SD2.2 Security awareness	SD2.2 Drošības apzināšanās

SD2.3 Security audit / review	SD2.3 Drošības audits/apskats
SD3 Business Requirements	*SD3 Biznesa prasības*
SD3.1 Specification of requirements	SD3.1 Prasību specifikācija
SD3.2 Confidentiality requirements	SD3.2 Konfidencialitātes prasības
SD3.3 Integrity requirements	SD3.3 Integritātes prasības
SD3.4 Availability requirements	SD3.4 Pieejamības prasības
SD3.5 Information risk analysis	SD3.5 Informācijas risku analīze
SD4 Design and Build	*SD4 Projektēšana un būvēšana*
SD4.1 System design	SD4.1 Sistēmu projektēšana
SD4.2 Application controls	SD4.2 Lietojumprogrammu vadīklas
SD4.3 General security controls	SD4.3 Vispārējās drošības vadīklas
SD4.4 Acquisition	SD4.4 Iegāde
SD4.5 System build	SD4.5 Sistēmu būvēšana
SD4.6 Web-enabled development	SD4.6 Tīmekļa bāzēta izstrāde
SD5 Testing	*SD5 Testēšana*
SD5.1 Testing process	SD5.1 Testēšanas process
SD5.2 Acceptance testing	SD5.2 Akcepttesti
SD6 Implementation	*SD6 Īstenošana*
SD6.1 System promotion criteria	SD6.1 Sistēmas veicināšanas kritēriji
SD6.2 Installation process	SD6.2 Instalācijas process
SD6.3 Post-implementation review	SD6.3 Pēcieviešanas pārskats
End User Environment	**Lietotāja Vide**
UE1 Local Security Management	*UE1 Vietējā drošības pārvaldība*
UE1.1 Roles and responsibilities	UE1.1 Lomas un pienākumi
UE1.2 Security awareness	UE1.2 Drošības apzināšanās
UE1.3 User training	UE1.3 Lietotāju apmācība
UE1.4 Local security co-ordination	UE1.4 Vietējās drošības koordinēšana
UE1.5 Information classification	UE1.5 Informācijas klasificešana
UE2 Corporate Business Applications	*UE2 Korporatīvās biznesa lietojumprogrammas*
UE2.1 Access control	UE2.1 Piekļuves kontrole
UE2.2 Application sign-on process	UE2.2 Lietojumprogrammu pierakstīšanās process
UE2.3 Change management	UE2.3 Pārmaiņu vadība
UE3 Desktop Applications	*UE3 Darbvirsmas lietojumprogrammas*
UE3.1 Inventory of desktop applications	UE3.1 Darbvirsmas lietojumprogrammu inventarizācija
UE3.2 Protection of spreadsheets	UE3.2 Izklājlapu aizsardzība
UE3.3 Protection of databases	UE3.3 Datubāzu aizsardzība
UE3.4 Desktop application development	UE3.4 Darbvirsmas lietojumprogrammu izstrāde
UE4 Computing Devices	*UE4 Datošanas ierīces*
UE4.1 Workstation protection	UE4.1 Darbstaciju aizsardzība

UE4.2 Hand-held devices	UE4.2 Rokas ierīces
UE4.3 Portable storage devices	UE4.3 Portatīvās glabāšanas ierīces
UE5 Electronic Communications	*UE5 Elektroniskie sakari*
UE5.1 General controls	UE5.1 Vispārēja vadība
UE5.2 E-mail	UE5.2 E-pasts
UE5.3 Instant messaging	UE5.3 Tūlītējā ziņapmaiņa
UE5.4 Internet access	UE5.4 Interneta piekļuve
UE5.5 Voice over IP (VoIP) networks	UE5.5 Balss IP tīklā
UE5.6 Wireless access	UE5.6 Bezvadu piekļuve
UE6 Environment Management	*UE6 Vides pārvaldība*
UE6.1 Information privacy	UE6.1 Informācijas privātums
UE6.2 Information security incident management	UE6.2 Informācijas drošības incidentu pārvaldība
UE6.3 Back-up	UE6.3 Rezerves kopēšana
UE6.4 Physical and environmental protection	UE6.4 Fiziskā un vides aizsardzība
UE6.5 Business continuity	UE6.5 Uzņēmējdarbības nepārtrauktība

2. Mājsaimniecības vajadzību atšķirības no uzņēmuma

ISF Standarta nodaļa	Uzņēmumam	Mājsaimniecībai
SM1.1 Vadības apņemšanās	Augstākās vadības apņemšanās	Mājsaimniecības izpratne par atbildību
SM1.2 Informācijas drošības politika	Dokumentēta un apstiprināta	Vispārēja izpratne
SM2.4 Drošības apzināšanās	Organizēts process	Pašam jādomā
SM2.5 Drošības izglītība/apmācības	Organizēts process	Ja nepieciešams, pašam jādomā
SM3.1 Informācijas klasificēšana	Strukturēti visām sistēmām	Izpratne, kas ir svarīgi
SM3.2 Īpašumtiesības	Strukturēti visām sistēmām	Vēlams, ja datoram vairāki lietotāji
SM3.3 Informācijas riska analīzes process	Strukturēti visām sistēmām	Vienkāršs
SM3.4 Informācijas riska analīzes metodes	Dažādas pēc vajadzības	Vienkārša, standartizēta
SM3.5 Tiesiskā un uzraudzības regulējuma atbilstība	Strukturēta, daudzveidīga	Vienkārša
SM4.2 Informācijas privātums	Atbilstība tiesību aktiem	Drošības mērķis
SM4.3 Vērtību pārvaldība	Precīza uzskaite	Priekšstats
SM4.5 Fiziskā aizsardzība	Organizēts process	Vienkārša
SM5.1 Vispārēja ļaunprogrammatūras aizsardzība	Organizēts process	Izpratne
SM5.2 Ļaunprogrammatūras aizsardzības programmatūra	Vairākas dažādiem mērķiem	Vienkārša, bet noteikti nepieciešama
SM5.6 Ielāpu pārvaldība	Organizēts process	Vienkārša, bet noteikti nepieciešama
SM6.1 Kriptogrāfijas risinājumi	Organizēts process	Pēc nepieciešamības
SM6.3 E-pasts	Sistēmas aizsardzība	Lietotāja kontu aizsardzība
SM6.4 Attālināts darbs	Organizēts process	Lietotājs citu sistēmām
CB1.1 Konfidencialitātes prasības	Strukturēti visām sistēmām	Izpratne
CB1.2 Integritātes prasības	Strukturēti visām sistēmām	Izpratne
CB1.3 Pieejamības prasības	Strukturēti visām sistēmām	Izpratne
CB3.1 Piekļuves kontrole	Organizēts process	Lietotājs citu sistēmām, izpratne
CB3.2 Lietojumprogrammu pierakstīšanās process	Organizēts process	Lietotājs citu sistēmām, izpratne

CB3.3 Darbstaciju aizsardzība	Organizēts process	Pašam jādomā
CB4.4 Rezerves kopēšana	Organizēts process	Izpratne, faktiskā rīcība
CI1.1 Lomas un pienākumi	Organizēts process	Vienošanās, faktiskā rīcība
CI3.1 Darbs ar datoru ārējām ierīcēm	Organizēts process	Izpratne, faktiskā rīcība
CI3.6 Ielāpu pārvaldība	Organizēts process	Izpratne, faktiskā rīcība
NW2.2 Ugunsmūri	Organizēts process	Faktiskā rīcība, izpratne
NW2.4 Bezvadu piekļuves	Organizēts process	Ja nepieciešams, pašam jādomā
UE3.1 Darbvirsmas lietojumprogrammu inventarizācija	Organizēts process	Izpratne
UE4.2 Rokas ierīces	Organizēts process	Telefonu utml. ierīču aizsardzība
UE4.3 Portatīvās glabāšanas ierīces	Organizēts process	Ārējo disku, USB atmiņu aizsardzība

3. Dati rīka IDRE pielietošanai

Datora izmantošanas mērķi

- M1 E-pasta nosūtīšana un saņemšana (piemēram, gmail.com, inbox.lv, Outlook, Thunderbird u.c.)
- M2 E-pakalpojumu izmantošana saziņai ar valsts iestādēm
- M3 Darbošanās sociālajā tīklā (piemēram, draugiem.lv. twitter.com)
- M4 Informācijas meklēšana, t.sk. ziņu lasīšana
- M5 Spēles dažādos portālos
- M6 Spēļu, attēlu, filmu vai mūzikas lejupielāde no Interneta
- M7 Apmaiņa ar filmām, mūziku utt., izmantojot speciālas programmas (piemēram, uTorrent, BitTorrent)
- M8 Maksājumi internetbankā
- M9 Iepirkšanās Internetā
- M10 Paša izveidota satura (t.sk. fotogrāfiju) augšupielādēšana jebkurā tīmekļa vietnē (arī draugiem.lv)
- M11 Fotogrāfiju/video failu glabāšana un apstrāde savā datorā
- M12 Dokumentu rakstīšana un noformēšana savā datorā
- M13 Mūzikas klausīšanās

Izmantotās tehnoloģijas

- OS1 Windows (Vista, 7, 8 vai jaunāka)
- OS2 Windows XP
- OS3 OS X (Apple datori)
- OS4 Linux (piem. Ubuntu)
- OS5 iOS (Apple iPhone, iPad)
- OS6 Android
- IP1 Bezvadu tīkls mājās
- IP2 Pieslēgums caur interneta vadu mājās
- IP3 Tīkls (arī bezvadu) publiskās vietās

Apdraudējumi

- A1 Datorvīrusi
- A2 Datora iesaistīšana botu tīklā
- A3 Datora tehnisks bojājums, t.sk. diska bojājums
- A4 Pazaudēts datu nesējs
- A5 Neapdomīga informācijas publiskošana
- A6 Pārāk vienkārši uzlaužama parole
- A7 Bezvadu tīkla neatļauta izmantošana

Ievainojamības

- I1 Neaizsargāts bezvadu tīkls
- I2 Datoram nav antivīrusa programmatūra vai līdzvērtīga aizsardzība
- I3 Datoram nav ugunsmūra vai līdzvērtīga aizsardzība

- I4 Programmatūra netiek atjaunota
- I5 Nav datu kopiju
- I6 Lietotājs slikti pārzina IT drošības pārvaldību
- I7 Lietotājs lieto sliktas paroles

Risku saraksts

- R1 Vīrusa darbības rezultātā lietotāja dati nokopēti nezināmā virzienā
- R2 Vīrusa darbības rezultātā sabojāti dati datorā
- R3 Dators iesaistīts botu tīklā (zombēts) ar nezināmu mērķi (lietotājam nemanāmi)
- R4 Dators iesaistīts botu tīklā (zombēts), lai izsūtītu mēstules, Interneta pakalpojumu sniedzējs atslēdz piekļuvi tīklam
- R5 Datora tehnisku bojājumu, t.sk. diska bojājuma dēļ, dati ir zuduši
- R6 Pazaudējot USB atmiņas karti, zaudēti dati
- R7 Neapdomīgi publiskota informācija tiek izmantota, lai izkrāptu naudu
- R8 Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā
- R9 Pārāk vienkāršas paroles dēļ, kāds iekļuvis internetbankas kontā un nozadzis naudu
- R10 Pārāk vienkāršas paroles dēļ, sociālā tīkla profilā kāds darbojies saimnieka vietā
- R11 Svešais izmanto bezvadu tīklu sliktiem mērķiem

Iespējamo risku matrica

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	IP1	IP3
R1	X						X			X					
R2	X	X	X	X	X	X	X	X	X	X	X	X			
R3	X	X	X	X	X	X	X	X	X	X					
R4	X	X	X	X	X	X	X	X	X	X					
R5											X	X	X		
R6											X	X			
R7	X		X						X	X					
R8	X		X							X					
R9								X							
R10			X												
R11														X	X

Drošības vadīklu saraksts

- V1 Parole bezvadu rūterim
- V2 Antivīrusa programmatūra datoram
- V3 Ugunsmūris datoram
- V4 Datu kopijas
- V5 Lietotāja zināšanas par IT drošības pārvaldību
- V6 Regulāra programmatūras atjaunināšana
- V7 Paroļu izveides un lietošanas paradumi

Drošības vadīklas, kas samazina riska iespējamību

	V1	V2	V3	V4	V5	V6	V7
R1		X				X	
R2		X				X	
R3			X			X	
R4			X			X	
R5				X			
R6				X			
R7					X		
R8					X		
R9							X
R10							X
R11	X						

Drošības vadīklu ietekmes vērtējums

- V1 Parole bezvadu rūterim
  - Jā – 2
  - Nē – 0
  - Nezinu – 0
- V2 Antivīrusa programmatūra datoram
  - Ir antivīrusa programmatūra un tā tiek regulāri atjaunota – 2
  - Ir antivīrusa programmatūra, bet tā netiek regulāri atjaunota – 1
  - Nav antivīrusa programmatūras – 0
  - Nezinu – 0
- V3 Ugunsmūris datoram
  - Jā, tiek izmantots specializēts ugunsmūris – 2
  - Jā, tiek izmantots operētājsistēmas iebūvētais ugunsmūris – 1
  - Nav ugunsmūra – 0
  - Nezinu – 0
- V4 Datu kopijas
  - Jā, tiek veidotas regulāri – 2
  - Jā, šad un tad – 1
  - Nē, netiek veiktas – 0
  - Nezinu – 0

- V5 Lietotāja zināšanas par IT drošības pārvaldību
  - Ir plašas zināšanas un pieredze – 2
  - Zinu pamatprincipus un vienkāršākās darbības – 1
  - Ne īpaši – 0
- V6 Regulāra programmatūras atjaunināšana
  - Programmatūras atjauninājumi pēc regulāras procedūras – 2
  - Programmatūras atjauninājumi šad un tad – 1
  - Netiek veikti atjauninājumi – 0
- V7 Paroļu izveides un lietošanas paradumi
  - Dažādās vietās tiek lietotas dažādas un pietiekami stipras paroles – 2

- Tiek lietotas pēc iespējas labas paroles, ievērojot drošības speciālistu rekomendācijas – 1
- Par to īpaši netiek domāts – 0

Sākotnējā riska ietekme

R1	3
R2	2
R3	2
R4	3
R5	3
R6	2
R7	3
R8	2
R9	3
R10	2
R11	2

4. Rīka IDRE pielietošanas paraugi

Rīku IDRE pielietoja 3 iedomāti lietotāji. Pirmais lietotājs norāda, ka datoru izmanto visiem mērķiem, ko rīks piedāvā, bet maz ko saprot no drošības pārvaldības. Lietotājs pieņem ekspertu ieteikumu risku sākotnējās ietekmes vērtējumam. Ņemot vērā, ka drošības darbības vai nu netiek veiktas vai pirmais lietotājs tajās neorientējas, risku iespējamība ir ar maksimālo vērtību. Līdz ar to arī daudz risku ar augstu līmeni.

Otrais lietotājs izmanto datoru 3 populārākajiem mērķiem saskaņā ar statistikas datiem. Šo lietotāju uztrauc visi riski, līdz ar to tiek norādītas maksimālās vērtības. Lietotājs cenšas veikt drošības darbības vismaz šad un tad. Otrais lietotājs veic tikai dažas darbības, tāpēc viņš pakļauts mazāk riskiem. 3 no tiem ir ar vidēju līmeni, jo lietotājs norādījis, ka ir tikai daļēji zinošs drošības pārvaldībā, bet risku ietekme viņam ir būtiska.

Trešais lietotājs pamatā izmanto datoru izklaidei, izmanto operētājsistēmu, kurai pēc šī brīža ieskatiem vīrusi nav bīstami, daļa risku līdz ar to viņam nav aktuāli. Lietotājs pieņem ekspertu ieteikumu risku sākotnējās ietekmes vērtējumam. Šim lietotājam ir 2 riski ar vidēju līmeni, kas saistīti ar paša lietotāja rīcību.

Rīka pielietošana parādīta, izmantojot rīka ekrānšāviņus, trešajam lietotājam – versija angļu valodā.

Pirmā lietotāja rezultāti

Datora un interneta izmantošanas mērķi

- ☑ E-pasta nosūtīšana un saņemšana (piemēram, gmail.com, inbox.lv, Outlook, Thunderbird u.c.)
- ☑ E-pakalpojumu izmantošana saziņai ar valsts iestādēm (piemēram, latvija.lv, eriga.lv)
- ☑ Darbošanās sociālajā tīklā (piemēram, draugiem.lv, facebook.com, twitter.com)
- ☑ Informācijas meklēšana, t.sk. ziņu lasīšana, video un TV skatīšanās, radio klausīšanās
- ☑ Spēles dažādos portālos, t.sk. tiešsaistē
- ☑ Spēļu, attēlu, filmu vai mūzikas lejupielāde no interneta
- ☑ Apmaiņa ar filmām, mūziku utt., izmantojot speciālas programmas (piemēram, uTorrent, BitTorrent)
- ☑ Internetbankas izmantošana, t.sk. rēķinu apmaksa citos portālos
- ☑ Iepirkšanās Internetā, t.sk. ceļojuma naktsmītņu rezervēšana, norādot maksājumu kartes datus
- ☑ Paša izveidota satura (t.sk. fotogrāfiju) augšupielādēšana jebkurā tīmekļa vietnē (piemēram, GoogleDocs, SkyDrive, arī draugiem.lv, facebook.com)
- ☑ Fotogrāfiju/video failu glabāšana un apstrāde savā datorā
- ☑ Dokumentu rakstīšana un noformēšana savā datorā
- ☑ Mūzikas klausīšanās

Kāda operētājsistēma darbina Tevis visbiežāk izmantoto ierīci?

- (•) Windows (Vista, 7, 8 vai jaunāku)
- ( ) Windows XP
- ( ) OS X (Apple datori)
- ( ) Linux (piem. Ubuntu)
- ( ) iOS (Apple iPhone, iPad)
- ( ) Android

Kādus interneta pieslēguma veidus Tu izmanto?

- [x] Bezvadu tīkls mājās
- [ ] Pieslēgums caur interneta vadu mājās
- [ ] Tīkls (arī bezvadu) publiskās vietās

Vai mājas bezvadu rūterim ir parole?

- ( ) Jā
- ( ) Nē
- (•) Nezinu

Vai datoram ir antivīrusa programmatūra?

- ( ) Ir antivīrusa programmatūra un tā tiek regulāri atjaunota
- ( ) Ir antivīrusa programmatūra, bet tā netiek regulāri atjaunota
- ( ) Nav antivīrusa programmatūras
- (•) Nezinu

Vai datoram ir ugunsmūris?

- ( ) Jā, tiek izmantots specializēts ugunsmūris
- ( ) Jā, tiek izmantots operētājsistēmas iebūvētais ugunsmūris
- ( ) Nav ugunsmūra
- (•) Nezinu

Vai tiek veidotas datu kopijas?

- ( ) Jā, tiek veidotas regulāri
- ( ) Jā, šad un tad
- ( ) Nē, netiek veiktas
- (•) Nezinu

Vai programmatūra tiek regulāri atjaunota?

- ( ) Programmatūras atjauninājumi pēc regulāras procedūras
- ( ) Programmatūras atjauninājumi šad un tad
- (•) Netiek veikti atjauninājumi

Cik informēts Tu esi par IT drošības pārvaldību?

- ( ) Ir plašas zināšanas un pieredze
- ( ) Zinu pamatprincipus un vienkāršākās darbības
- (•) Ne īpaši

Kādi ir paroļu izveides un lietošanas paradumi?

- ( ) Dažādās vietās tiek lietotas dažādas un pietiekami stipras paroles
- ( ) Tiek lietotas pēc iespējas labas paroles, ievērojot drošības speciālistu rekomendācijas
- (•) Par to īpaši netiek domāts

Iedomājies, ka zemāk minētais notikums būtu noticis.

Cik svarīga Tev ir tā negatīvā ietekme: (1 – nemaz neuztrauc, 2 – gan jau pārdzīvošu, 3 – būtiska negatīva ietekme)?

Speciālisti ir novērtējuši riskus, sniedzot ieteikumu, taču droši maini riska novērtējumu, ja Tava attieksme ir citāda.

Vīrusa darbības rezultātā lietotāja dati nokopēti nezināmā virzienā

1 2 **3**

Vīrusa darbības rezultātā sabojāti vai izdzēsti dati datorā

1 **2** 3

Dators iesaistīts botu tīklā (zombēts) ar nezināmu mērķi (lietotājam nemanāmi)

1 **2** 3

Dators iesaistīts botu tīklā (zombēts), Interneta pakalpojumu sniedzējs atslēdz piekļuvi tīklam

1 2 **3**

Datora tehnisku bojājumu, t.sk. diska bojājuma dēļ, dati ir zuduši

1 2 **3**

Pazaudējot USB atmiņas karti vai telefonu, zaudēti dati

1 **2** 3

Neapdomīgi publiskota vai sliktajiem nodota informācija tiek izmantota, lai izkrāptu vai nozagtu naudu

1 2 **3**

Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā vai radusies cita nepatīkama situācija

1 **2** 3

Pārāk vienkāršas paroles dēļ, kāds iekļuvis internetbankas kontā un nozadzis naudu

1 2 **3**

Pārāk vienkāršas paroles dēļ, sociālā tīkla profilā vai e-pastā kāds darbojies saimnieka vietā

1 **2** 3

Svešais izmanto bezvadu tīklu sliktiem mērķiem

1 **2** 3

Tu esi pakļauts šādiem riskiem ar šādu riska ietekmi (9 maks.):

9 **Vīrusa darbības rezultātā lietotāja dati nokopēti nezināmā virzienā**

Ieteikums: Pārliecinies, ka izmanto labu antivīrusa programmu, kas regulāri tiek atjaunināta. Uzlabot aizsardzību pret vīrusiem jāveic cik vien iespējams drīz. Vairāk lasi:
www.esidross.lv/2013/06/18/zonealarm-antiviruss-un-ugunsmuris/
www.esidross.lv/2012/11/07/antiviruss-avast-free-antivirus/

9 **Dators iesaistīts botu tīklā (zombēts), Interneta pakalpojumu sniedzējs atslēdz piekļuvi tīklam**

Ieteikums: Noziedznieki ne vienmēr uzreiz sabojā vai nozog datus no zombētiem datoriem, tomēr nekad nevar zināt, kad tas notiks. Turklāt ir iespējams, ka zombētais dators tiek iesaistīts uzbrukumā citiem datoriem, un izmeklēšanas gaitā var rasties problēmas tā īpašniekam. Noteikti jāpilnveido aizsardzības programmas (antivīrusu, ugunsmūra) un jāuzstāda labākas paroles, tas jāveic cik vien iespējams drīz. Vairāk lasi:
www.esidross.lv/2012/09/05/ko-laundaris-var-iegut-no-uzlauzta-datora/
www.esidross.lv/2011/03/29/paroles/
www.esidross.lv/2013/06/18/zonealarm-antiviruss-un-ugunsmuris/
www.esidross.lv/2012/11/07/antiviruss-avast-free-antivirus/

9 **Neapdomīgi publiskota vai sliktajiem nodota informācija tiek izmantota, lai izkrāptu vai nozagtu naudu**

Ieteikums: Nevienas darbības Internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, "parakstot" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par ieradumiem, hobijiem vtml., lai iegūtu uzticību un izkrāptu naudu. Ir vērts atcerēties parunu "septiņreiz nomēri pirms nogriez" arī attiecībā uz informācijas publicēšanu Internetā (sociālajos tīklos). Ja labprāt publisko daudz informācijas, uzmanies no nepazīstamiem saziņas partneriem, kas daudz zina par Tevi. Iespējams, ka būtu vērts izdzēst kaut daļu informācijas, lai tā nebūtu tik ērti pieejama. Vairāk lasi:
www.esidross.lv/2013/04/10/kapec-sociala-inzenierija-ir-efektiva/
www.esidross.lv/2014/01/22/visa-dzive-interneta-spoguli-2/
www.esidross.lv/2013/07/16/berna-izglitosana-datora-lietosana/
www.esidross.lv/2012/04/28/popularakie-krapsanas-veidi-interneta/

9 **Pārāk vienkāršas paroles dēļ, kāds iekļuvis internetbankas kontā un nozadzis naudu**

Ieteikums: Parolei jābūt pietiekami sarežģītai (vismaz 8 simboli, bet labāk vairāk, lielie un mazie burti, speciālie simboli, cipari utt.). Ja paroli grūti atcerēties, mājās tā var tikt arī pierakstīta un glabāta kādā sev vien zināmā drošā vietā ("zem spilvena"), rūpējies, lai tā nebūtu pieejama kopā ar lietotāja vārdu. Ja esi lietojis paroli nedrošā vietā (Interneta kafejnīcā vtml.), labāk to nomaini. Vairāk lasi:
www.esidross.lv/2012/06/29/ka-drosi-iepirkties-tiessaiste/
www.esidross.lv/2012/10/15/parolu-nebusanas-jeb-nomaini-savu-paroli-tagad/
www.esidross.lv/2011/03/29/paroles/

9 **Datora tehnisku bojājumu, t.sk. diska bojājuma dēļ, dati ir zuduši**

Ieteikums: Vislabākais līdzeklis pret datu zaudēšanu tehnisku problēmu dēļ ir savlaicīga un regulāra rezerves kopiju veidošana. Izveido savu risinājumu, un sāc veidot rezerves kopijas. Var izmantot gan CD, gan USB atmiņas kartes, gan citus risinājumus. Vairāk lasi:
www.esidross.lv/2013/11/15/informacija-glabasana-un-sinhronizacija-bezmaksas-kratuve-makoni/
www.esidross.lv/2012/11/12/backup-jeb-datu-rezerves-kopijas/

6 **Vīrusa darbības rezultātā sabojāti vai izdzēsti dati datorā**

Ieteikums: Pārliecinies, ka izmanto labu antivīrusa programmu, kas regulāri tiek atjaunināta. Uzlabot aizsardzību pret vīrusiem jāveic cik vien iespējams drīz. Vairāk lasi:
www.esidross.lv/2013/06/18/zonealarm-antiviruss-un-ugunsmuris/
www.esidross.lv/2012/11/07/antiviruss-avast-free-antivirus/

6 **Dators iesaistīts botu tīklā (zombēts) ar nezināmu mērķi (lietotājam nemanāmi)**

Ieteikums: Noziedznieki ne vienmēr uzreiz sabojā vai nozog datus no zombētiem datoriem, tomēr nekad nevar zināt, kad tas notiks. Turklāt ir iespējams, ka zombētais dators tiek iesaistīts uzbrukumā citiem datoriem, un izmeklēšanas gaitā var rasties problēmas tā īpašniekam. Noteikti jāpilnveido aizsardzības programmas (antivīrusu, ugunsmūra) un jāuzstāda labākas paroles, tas jāveic cik vien iespējams drīz. Vairāk lasi:
www.esidross.lv/2013/05/10/java-un-tas-drosiba/
www.esidross.lv/2012/09/05/ko-laundaris-var-iegut-no-uzlauzta-datora/
www.esidross.lv/2011/03/29/paroles/
www.esidross.lv/2013/06/18/zonealarm-antiviruss-un-ugunsmuris/
www.esidross.lv/2012/11/07/antiviruss-avast-free-antivirus/

6 **Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā vai radusies cita nepatīkama situācija**

Ieteikums: Nevienas darbības Internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, "parakstot" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par trakulīgām ballītēm, ne īpaši labiem ieradumiem vtml., lai veidotu priekšstatu. Ir vērts atcerēties parunu "septiņreiz nomēri pirms nogriez" arī attiecībā uz informācijas publicēšanu Internetā (sociālajos tīklos). Iespējams, ka būtu vērts izdzēst kaut daļu informācijas, lai tā nebūtu tik ērti pieejama. Vairāk lasi:
www.esidross.lv/2013/04/10/kapec-sociala-inzenierija-ir-efektiva/
www.esidross.lv/2014/01/22/visa-dzive-interneta-spoguli-2/
www.esidross.lv/2013/07/16/berna-izglitosana-datora-lietosana/
www.esidross.lv/2012/04/28/popularakie-krapsanas-veidi-interneta/

6 **Pārāk vienkāršas paroles dēļ, sociālā tīkla profilā vai e-pastā kāds darbojies saimnieka vietā**

Ieteikums: Parolei jābūt pietiekami sarežģītai (vismaz 8 simboli, bet labāk vairāk, lielie un mazie burti, speciālie simboli, cipari utt.). Ja paroli grūti atcerēties, mājās tā var tikt arī pierakstīta un glabāta kādā sev vien zināmā drošā vietā ("zem spilvena"), rūpējies, lai tā nebūtu pieejama kopā ar lietotāja vārdu. Ja esi lietojis paroli nedrošā vietā (Interneta kafejnīcā vtml.), labāk to nomaini. Vairāk lasi:
www.esidross.lv/2012/06/29/ka-drosi-iepirkties-tiessaiste/
www.esidross.lv/2012/10/15/parolu-nebusanas-jeb-nomaini-savu-paroli-tagad/
www.esidross.lv/2011/03/29/paroles/

6 **Pazaudējot USB atmiņas karti vai telefonu, zaudēti dati**

Ieteikums: Jāizvērtē, kādi dati tiek glabāti USB atmiņas kartē. Ja tie ir tikai daži faili, kam ir oriģināli datorā, kā arī neuztrauc datu nokļūšana pie svešiem, tad var pieņemt nelielas materiālas vērtības zudumu. Ja USB atmiņā tiek glabāti slēpjami dati, tad vajadzētu tos šifrēt. Šī riska augstais līmenis liecina, ka jāpārdomā, kā uzlabot datu drošību USB atmiņā. Vairāk lasi:
www.esidross.lv/2013/11/15/informacija-glabasana-un-sinhronizacija-bezmaksas-kratuve-makoni/

6 **Svešais izmanto bezvadu tīklu sliktiem mērķiem**

Ieteikums: Bezvadu tīkla maršrutētājam nekavējoties noteikti jāuzstāda pietiekami droša parole. Vairāk lasi:
www.esidross.lv/2012/08/29/drosa-majas-bezvadu-tikla-konfiguracija/
www.esidross.lv/2012/05/31/ka-lietot-bezvadu-internetu-majas/
www.esidross.lv/2012/05/31/ka-lietot-bezvadu-internetu-publiskas-vietas/

Otrā lietotāja rezultāti

Datora un interneta izmantošanas mērķi

- [x] E-pasta nosūtīšana un saņemšana (piemēram, gmail.com, inbox.lv, Outlook, Thunderbird u.c.)
- [ ] E-pakalpojumu izmantošana saziņai ar valsts iestādēm (piemēram, latvija.lv, eriga.lv)
- [ ] Darbošanās sociālajā tīklā (piemēram, draugiem.lv, facebook.com, twitter.com)
- [x] Informācijas meklēšana, t.sk. ziņu lasīšana, video un TV skatīšanās, radio klausīšanās
- [ ] Spēles dažādos portālos, t.sk. tiešsaistē
- [ ] Spēļu, attēlu, filmu vai mūzikas lejupielāde no interneta
- [ ] Apmaiņa ar filmām, mūziku utt., izmantojot speciālas programmas (piemēram, uTorrent, BitTorrent)
- [x] Internetbankas izmantošana, t.sk. rēķinu apmaksa citos portālos
- [ ] Iepirkšanās Internetā, t.sk. ceļojuma naktsmītņu rezervēšana, norādot maksājumu kartes datus
- [ ] Paša izveidota satura (t.sk. fotogrāfiju) augšupielādēšana jebkurā tīmekļa vietnē (piemēram, GoogleDocs, SkyDrive, arī draugiem.lv, facebook.com)
- [ ] Fotogrāfiju/video failu glabāšana un apstrāde savā datorā
- [ ] Dokumentu rakstīšana un noformēšana savā datorā
- [ ] Mūzikas klausīšanās

Kāda operētājsistēma darbina Tevis visbiežāk izmantoto ierīci?

- (•) Windows (Vista, 7, 8 vai jaunāku)
- ( ) Windows XP
- ( ) OS X (Apple datori)
- ( ) Linux (piem. Ubuntu)
- ( ) iOS (Apple iPhone, iPad)
- ( ) Android

Kādus interneta pieslēguma veidus Tu izmanto?

- [ ] Bezvadu tīkls mājās
- [x] Pieslēgums caur interneta vadu mājās
- [ ] Tīkls (arī bezvadu) publiskās vietās

Vai datoram ir antivīrusa programmatūra?

- (●) Ir antivīrusa programmatūra un tā tiek regulāri atjaunota
- ( ) Ir antivīrusa programmatūra, bet tā netiek regulāri atjaunota
- ( ) Nav antivīrusa programmatūras
- ( ) Nezinu

Vai datoram ir ugunsmūris?

- ( ) Jā, tiek izmantots specializēts ugunsmūris
- (●) Jā, tiek izmantots operētājsistēmas iebūvētais ugunsmūris
- ( ) Nav ugunsmūra
- ( ) Nezinu

Vai tiek veidotas datu kopijas?

- ( ) Jā, tiek veidotas regulāri
- (●) Jā, šad un tad
- ( ) Nē, netiek veiktas
- ( ) Nezinu

Vai programmatūra tiek regulāri atjaunota?

- (●) Programmatūras atjauninājumi pēc regulāras procedūras
- ( ) Programmatūras atjauninājumi šad un tad
- ( ) Netiek veikti atjauninājumi

Cik informēts Tu esi par IT drošības pārvaldību?

- ( ) Ir plašas zināšanas un pieredze
- (●) Zinu pamatprincipus un vienkāršākās darbības
- ( ) Ne īpaši

Kādi ir paroļu izveides un lietošanas paradumi?

- ( ) Dažādās vietās tiek lietotas dažādas un pietiekami stipras paroles
- (●) Tiek lietotas pēc iespējas labas paroles, ievērojot drošības speciālistu rekomendācijas
- ( ) Par to īpaši netiek domāts

Vīrusa darbības rezultātā lietotāja dati nokopēti nezināmā virzienā

1 2 3

Vīrusa darbības rezultātā sabojāti vai izdzēsti dati datorā

1 2 3

Dators iesaistīts botu tīklā (zombēts) ar nezināmu mērķi (lietotājam nemanāmi)

1 2 3

Dators iesaistīts botu tīklā (zombēts), Interneta pakalpojumu sniedzējs atslēdz piekļuvi tīklam

1 2 3

Neapdomīgi publiskota vai sliktajiem nodota informācija tiek izmantota, lai izkrāptu vai nozagtu naudu

1 2 3

Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā vai radusies cita nepatīkama situācija

1 2 3

Pārāk vienkāršas paroles dēļ, kāds iekļuvis internetbankas kontā un nozadzis naudu

1 2 3

Tu esi pakļauts šādiem riskiem ar šādu riska ietekmi (9 maks.):

6 **Neapdomīgi publiskota vai sliktajiem nodota informācija tiek izmantota, lai izkrāptu vai nozagtu naudu**

Ieteikums: Nevienas darbības Internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, "parakstot" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par ieradumiem, hobijiem vtml., lai iegūtu uzticību un izkrāptu naudu. Ir vērts atcerēties parunu "septiņreiz nomēri pirms nogriez" arī attiecībā uz informācijas publicēšanu Internetā (sociālajos tīklos). Ja labprāt publisko daudz informācijas, uzmanies no nepazīstamiem saziņas partneriem, kas daudz zina par Tevi. Iespējams, ka būtu vērts izdzēst kaut daļu informācijas, lai tā nebūtu tik ērti pieejama. Vairāk lasi:
www.esidross.lv/2013/04/10/kapec-sociala-inzenierija-ir-efektiva/
www.esidross.lv/2014/01/22/visa-dzive-interneta-spoguli-2/
www.esidross.lv/2013/07/16/berna-izglitosana-datora-lietosana/
www.esidross.lv/2012/04/28/popularakie-krapsanas-veidi-interneta/

6 **Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā vai radusies cita nepatīkama situācija**

Ieteikums: Nevienas darbības Internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, "parakstot" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par trakulīgām ballītēm, ne īpaši labiem ieradumiem vtml., lai veidotu priekšstatu. Ir vērts atcerēties parunu "septiņreiz nomēri pirms nogriez" arī attiecībā uz informācijas publicēšanu Internetā (sociālajos tīklos). Iespējams, ka būtu vērts izdzēst kaut daļu informācijas, lai tā nebūtu tik ērti pieejama. Vairāk lasi:
www.esidross.lv/2013/04/10/kapec-sociala-inzenierija-ir-efektiva/
www.esidross.lv/2014/01/22/visa-dzive-interneta-spoguli-2/
www.esidross.lv/2013/07/16/berna-izglitosana-datora-lietosana/
www.esidross.lv/2012/04/28/popularakie-krapsanas-veidi-interneta/

6 **Pārāk vienkāršas paroles dēļ, kāds iekļuvis internetbankas kontā un nozadzis naudu**

Ieteikums: Parolei jābūt pietiekami sarežģītai (vismaz 8 simboli, bet labāk vairāk, lielie un mazie burti, speciālie simboli, cipari utt.). Ja paroli grūti atcerēties, mājās tā var tikt arī pierakstīta un glabāta kādā sev vien zināmā drošā vietā ("zem spilvena"), rūpējies, lai tā nebūtu pieejama kopā ar lietotāja vārdu. Ja esi lietojis paroli nedrošā vietā (Interneta kafejnīcā vtml.), labāk to nomaini. Vairāk lasi:
www.esidross.lv/2012/06/29/ka-drosi-iepirkties-tiessaiste/
www.esidross.lv/2012/10/15/parolu-nebusanas-jeb-nomaini-savu-paroli-tagad/
www.esidross.lv/2011/03/29/paroles/

Tu esi minimāli pakļauts šādiem riskiem, taču to ietekme ir zema un papildus darbības no Tavas puses nav nepieciešamas:

3 Vīrusa darbības rezultātā lietotāja dati nokopēti nezināmā virzienā

3 Vīrusa darbības rezultātā sabojāti vai izdzēsti dati datorā

3 Dators iesaistīts botu tīklā (zombēts) ar nezināmu mērķi (lietotājam nemanāmi)

3 Dators iesaistīts botu tīklā (zombēts), Interneta pakalpojumu sniedzējs atslēdz piekļuvi tīklam

Trešā lietotāja rezultāti

Your usage of computers and internet

- [ ] Sending and receiving emails (for example - gmail.com, inbox.lv, Outlook, Thunderbird etc.)
- [ ] Using e-services for contacting government institution (for example - latvija.lv, eriga.lv)
- [x] Using social networks (for example - draugiem.lv, facebook.com, twitter.com)
- [ ] Searching for information, including reading news, watching TV and online videos, listening to radio
- [x] Playing web games
- [x] Downloading games images movies or music from internet
- [ ] Sharing movies music etc. using special software (for example - uTorrent BitTorrent)
- [ ] Using internet bank, including payments on other websites
- [ ] Shopping through internet, including booking hotels (and providing creditcard information)
- [x] Uploading original content (including photos) on any web page (for example - GoogleDocs, SkyDrive, draugiem.lv, facebook.com)
- [x] Storing Photo/video and processing on your computer
- [ ] Writing and formatting documents on your computer
- [x] Listening to music

What operating system controls your monstly used device?

- ○ Windows (Vista, 7, 8 or newer)
- ○ Windows XP
- ◉ OS X (Apple computers)
- ○ Linux (piem. Ubuntu)
- ○ iOS (Apple iPhone, iPad)
- ○ Android

What internet connection types are you using?

- [x] Wireless network at home
- [ ] Wired network at home
- [ ] Public (including wireless) networks

Is your home router password protected?

- (●) Yes
- ( ) No
- ( ) Don't know

Is data being backed up?

- ( ) Yes, regularly
- (●) Yes, now and then
- ( ) No, it isn't
- ( ) Don't know

Is software updated regularly?

- (●) Yes, software is updated regularly
- ( ) Software is updated now and then
- ( ) Software is not updated regularly

How well informed are you about IT safety management?

- ( ) Broad knowledge and experience
- (●) Informed about basic principles and simple procedures
- ( ) Not really

What are your password creation habits?

- ( ) Different passwords are used in different places and they are strong enough
- (●) Good passwords(according to recommendations by security specialists) are used as often as possible
- ( ) I don't pay attention to it

Imagine that events mentioned below really happened. Rank how important is its negative implications:
1 - doesn't bother, 2 - I'll get over it, 3 - substantial negative impact
Experts have rated these risks, giving advises, but change the rating if you feel differently.

Because of damaged computer, including damaged hard drive, data has been lost

1 2 **3**

Data has been lost because of lost mobile phone or flash drive

1 2 3

Lightmindedly published information is used to cheat out money

1 2 3

Job opportunity is denied because of lightmindedly published information or other unpleasant situation

1 2 3

Because of a weak password someone is using owner's email or social profile

1 2 **3**

Someone is using wireless network for bad purposes

1 **2** 3

You are affected by these risks with these implications (9 max):

6 **Because of a weak password someone is using owner's email or social profile**

Advice: Password must be complicated enough (at least 8 symbols (but more is better), uppercase and lowercase letter, special symbols, number etc.). If password is hard to remember, it can be stored home in a secret place ("under the pillow"), but make sure that it is not accessible with username. If you used password in unsafe environment (Internet café for example) you should change the password. Read more (in latvian):
www.esidross.lv/2012/06/29/ka-drosi-iepirkties-tiessaiste/
www.esidross.lv/2012/10/15/parolu-nebusanas-jeb-nomaini-savu-paroli-tagad/
www.esidross.lv/2011/03/29/paroles/

6 **Because of damaged computer, including damaged hard drive, data has been lost**

Advice: The best tool to prevent data loss because of computer technical problems is timely and on regular basis created data backups. Create your solution to this problem and start creating backups. Optical discs, USB flash memory and other storage solutions can be used for backup purposes. Read more (in latvian):
www.esidross.lv/2013/11/15/informacija-glabasana-un-sinhronizacija-bezmaksas-kratuve-makoni/
www.esidross.lv/2012/11/12/backup-jeb-datu-rezerves-kopijas/

You are affected by the following risks, but their possible implications ar less likely and additional actions are not necessary:

2 Lightmindedly published information is used to cheat out money

2 Job opportunity is denied because of lightmindedly published information or other unpleasant situation

2 Data has been lost because of lost mobile phone or flash drive

2 Someone is using wireless network for bad purposes

5. Rīka IDRE dati

```
var systemdata = {};

systemdata.questions = [
    {
        qid: 0,
        text: {
            lv: "Datora un interneta izmantošanas mērķi",
            en: "Your usage of computers and internet"
        },
        multiple: true,
        answers: [
            {
                aid: 0,
                risks: [0, 1, 2, 3, 6, 7],
                text: {
                    lv: "E-pasta nosūtīšana un saņemšana
(piemēram, gmail.com, inbox.lv, Outlook, Thunderbird u.c.)",
                    en: "Sending and receiving emails (for example
- gmail.com, inbox.lv, Outlook, Thunderbird etc.)"
                }
            },
            {
                aid: 1,
                risks: [1, 2, 3],
                text: {
                    lv: "E-pakalpojumu izmantošana saziņai ar
valsts iestādēm (piemēram, latvija.lv, eriga.lv)",
                    en: "Using e-services for contacting
government institution (for example - latvija.lv, eriga.lv)"
                }
            },
            {
                aid: 2,
                risks: [1, 2, 3, 6, 7, 9],
                text: {
                    lv: "Darbošanās sociālajā tīklā (piemēram,
draugiem.lv, facebook.com, twitter.com)",
                    en: "Using social networks (for example -
draugiem.lv, facebook.com, twitter.com)"
                }
            },
            {
                aid: 3,
                risks: [1, 2, 3],
                text: {
                    lv: "Informācijas meklēšana, t.sk. ziņu
lasīšana, video un TV skatīšanās, radio klausīšanās",
                    en: "Searching for information, including
reading news, watching TV and online videos, listening to radio"
                }
            },
            {
```

```
                aid: 4,
                risks: [1, 2, 3],
                text: {
                    lv: "Spēles dažādos portālos, t.sk.
tiešsaistē",
                    en: "Playing web games"
                }
            },
            {
                aid: 5,
                risks: [1, 2, 3],
                text: {
                    lv: "Spēļu, attēlu, filmu vai mūzikas
lejupielāde no interneta",
                    en: "Downloading games images movies or music
from internet"
                }
            },
            {
                aid: 6,
                risks: [0, 1, 2, 3],
                text: {
                    lv: "Apmaiņa ar filmām, mūziku utt.,
izmantojot speciālas programmas (piemēram, uTorrent, BitTorrent)",
                    en: "Sharing movies music etc. using special
software (for example - uTorrent BitTorrent)"
                }
            },
            {
                aid: 7,
                risks: [1, 2, 3, 8],
                text: {
                    lv: "Internetbankas izmantošana, t.sk. rēķinu
apmaksa citos portālos",
                    en: "Using internet bank, including payments
on other websites"
                }
            },
            {
                aid: 8,
                risks: [1, 2, 3, 6],
                text: {
                    lv: "Iepirkšanās Internetā, t.sk. ceļojuma
naktsmītņu rezervēšana, norādot maksājumu kartes datus",
                    en: "Shopping through internet, including
booking hotels (and providing creditcard information)"
                }
            },
            {
                aid: 9,
                risks: [0, 1, 2, 3, 6, 7],
                text: {
                    lv: "Paša izveidota satura (t.sk. fotogrāfiju)
augšupielādēšana jebkurā tīmekļa vietnē (piemēram, GoogleDocs,
SkyDrive, arī draugiem.lv, facebook.com)",
```

```
                    en: "Uploading original content (including
photos) on any web page (for example - GoogleDocs, SkyDrive,
draugiem.lv, facebook.com)"
                }
            },
            {
                aid: 10,
                risks: [1, 4, 5],
                text: {
                    lv: "Fotogrāfiju/video failu glabāšana un
apstrāde savā datorā",
                    en: "Storing Photo/video and processing on
your computer"
                }
            },
            {
                aid: 11,
                risks: [1, 4, 5],
                text: {
                    lv: "Dokumentu rakstīšana un noformēšana savā
datorā",
                    en: "Writing and formatting documents on your
computer"
                }
            },
            {
                aid: 12,
                risks: [4],
                text: {
                    lv: "Mūzikas klausīšanās",
                    en: "Listening to music"
                }
            }
        ]
    },
    {
        qid: 1,
        text: {
            lv: "Kāda operētājsistēma darbina Tevis visbiežāk
izmantoto ierīci?",
            en: "What operating system controls your monstly used
device?"
        },
        multiple: false,
        answers: [
            {
                aid: 0,
                text: {
                    lv: "Windows (Vista, 7, 8 vai jaunāku)",
                    en: "Windows (Vista, 7, 8 or newer)"
                }
            },
            {
                aid: 1,
                text: {
```

```
                lv: "Windows XP",
                en: "Windows XP"
            }
        },
        {
            aid: 2,
            text: {
                lv: "OS X (Apple datori)",
                en: "OS X (Apple computers)"
            }
        },
        {
            aid: 3,
            text: {
                lv: "Linux (piem. Ubuntu)",
                en: "Linux (piem. Ubuntu)"
            }
        },
        {
            aid: 4,
            text: {
                lv: "iOS (Apple iPhone, iPad)",
                en: "iOS (Apple iPhone, iPad)"
            }
        },
        {
            aid: 5,
            text: {
                lv: "Android",
                en: "Android"
            }
        }
    ]
},
{
    qid: 2,
    text: {
        lv: "Kādus interneta pieslēguma veidus Tu izmanto?",
        en: "What internet connection types are you using?"
    },
    multiple: true,
    answers: [
        {
            aid: 0,
            risks: [10],
            text: {
                lv: "Bezvadu tīkls mājās",
                en: "Wireless network at home"
            }
        },
        {
            aid: 1,
            text: {
                lv: "Pieslēgums caur interneta vadu mājās",
                en: "Wired network at home"
```

```
                }
            },
            {
                aid: 2,
                risks: [10],
                text: {
                    lv: "Tīkls (arī bezvadu) publiskās vietās",
                    en: "Public (including wireless) networks"
                }
            }
        ]
    },
    {
        qid: 3,
        text: {
            lv: "Vai mājas bezvadu rūterim ir parole?",
            en: "Is your home router password protected?"
        },
        multiple: false,
        answers: [
            {
                aid: 0,
                adjust_risk: { 10: -2 },
                text: {
                    lv: "Jā",
                    en: "Yes"
                }
            },
            {
                aid: 1,
                text: {
                    lv: "Nē",
                    en: "No"
                }
            },
            {
                aid: 2,
                text: {
                    lv: "Nezinu",
                    en: "Don't know"
                }
            }
        ]
    },
    {
        qid: 4,
        text: {
            lv: "Vai datoram ir antivīrusa programmatūra?",
            en: "Is your computer protected with antivirus
software?"
        },
        multiple: false,
        answers: [
            {
                aid: 0,
```

```
                adjust_risk: { 0: -2, 1: -2 },
                text: {
                    lv: "Ir antivīrusa programmatūra un tā tiek
regulāri atjaunota",
                    en: "Yes and it is updated regularly"
                }
            },
            {
                aid: 1,
                adjust_risk: { 0: -1, 1: -1 },
                text: {
                    lv: "Ir antivīrusa programmatūra, bet tā
netiek regulāri atjaunota",
                    en: "Yes, but it is not updated regularly"
                }
            },
            {
                aid: 2,
                text: {
                    lv: "Nav antivīrusa programmatūras",
                    en: "No"
                }
            },
            {
                aid: 3,
                text: {
                    lv: "Nezinu",
                    en: "Don't know"
                }
            }
        ]
    },
    {
        qid: 5,
        text: {
            lv: "Vai datoram ir ugunsmūris?",
            en: "Is your computer protected with firewall?"
        },
        multiple: false,
        answers: [
            {
                aid: 0,
                adjust_risk: { 2: -2, 3: -2 },
                text: {
                    lv: "Jā, tiek izmantots specializēts
ugunsmūris",
                    en: "Yes, with special third party firewall"
                }
            },
            {
                aid: 1,
                adjust_risk: { 2: -1, 3: -1 },
                text: {
                    lv: "Jā, tiek izmantots operētājsistēmas
iebūvētais ugunsmūris",
```

```
                    en: "Yes, with operating system’s built-in
firewall"
                }
            },
            {
                aid: 2,
                text: {
                    lv: "Nav ugunsmūra",
                    en: "No"
                }
            },
            {
                aid: 3,
                text: {
                    lv: "Nezinu",
                    en: "Don't know"
                }
            }
        ]
    },
    {
        qid: 6,
        text: {
            lv: "Vai tiek veidotas datu kopijas?",
            en: "Is data being backed up?"
        },
        multiple: false,
        answers: [
            {
                aid: 0,
                adjust_risk: { 4: -2, 5: -2 },
                text: {
                    lv: "Jā, tiek veidotas regulāri",
                    en: "Yes, regularly"
                }
            },
            {
                aid: 1,
                adjust_risk: { 4: -1, 5: -1 },
                text: {
                    lv: "Jā, šad un tad",
                    en: "Yes, now and then"
                }
            },
            {
                aid: 2,
                text: {
                    lv: "Nē, netiek veiktas",
                    en: "No, it isn’t"
                }
            },
            {
                aid: 3,
                text: {
                    lv: "Nezinu",
```

```
                    en: "Don't know"
                }
            }
        ]
    },
    {
        qid: 7,
        text: {
            lv: "Vai programmatūra tiek regulāri atjaunota?",
            en: "Is software updated regularly?"
        },
        multiple: false,
        answers: [
            {
                aid: 0,
                adjust_risk: { 0: -2, 1: -2, 2: -2, 3: -2 },
                text: {
                    lv: "Programmatūras atjauninājumi pēc
regulāras procedūras",
                    en: "Yes, software is updated regularly"
                }
            },
            {
                aid: 1,
                adjust_risk: { 0: -1, 1: -1, 2: -1, 3: -1 },
                text: {
                    lv: "Programmatūras atjauninājumi šad un tad",
                    en: "Software is updated now and then"
                }
            },
            {
                aid: 2,
                text: {
                    lv: "Netiek veikti atjauninājumi",
                    en: "Software is not updated regularly"
                }
            }
        ]
    },
    {
        qid: 8,
        text: {
            lv: "Cik informēts Tu esi par IT drošības
pārvaldību?",
            en: "How well informed are you about IT safety
management?"
        },
        multiple: false,
        answers: [
            {
                aid: 0,
                adjust_risk: { 6: -2, 7: -2 },
                text: {
                    lv: "Ir plašas zināšanas un pieredze",
                    en: "Broad knowledge and experience"
```

```
                }
            },
            {
                aid: 1,
                adjust_risk: { 6: -1, 7: -1 },
                text: {
                    lv: "Zinu pamatprincipus un vienkāršākās
darbības",
                    en: "Informed about basic principles and
simple procedures"
                }
            },
            {
                aid: 2,
                text: {
                    lv: "Ne īpaši",
                    en: "Not really"
                }
            }
        ]
    },
    {
        qid: 9,
        text: {
            lv: "Kādi ir paroļu izveides un lietošanas paradumi?",
            en: "What are your password creation habits?"
        },
        multiple: false,
        answers: [
            {
                aid: 0,
                adjust_risk: { 8: -2, 9: -2 },
                text: {
                    lv: "Dažādās vietās tiek lietotas dažādas un
pietiekami stipras paroles",
                    en: "Different passwords are used in different
places and they are strong enough"
                }
            },
            {
                aid: 1,
                adjust_risk: { 8: -1, 9: -1 },
                text: {
                    lv: "Tiek lietotas pēc iespējas labas paroles,
ievērojot drošības speciālistu rekomendācijas",
                    en: "Good passwords(according to
recommendations by security specialists) are used as often as
possible"
                }
            },
            {
                aid: 2,
                text: {
                    lv: "Par to īpaši netiek domāts",
                    en: "I don’t pay attention to it"
```

```
                }
            }
        ]
    }
];

systemdata.risks = [
    {
        rid: 0,
        checked: 3,
        text: {
            lv: "Vīrusa darbības rezultātā lietotāja dati nokopēti
nezināmā virzienā",
            en: "Data copied to unknown place because of virus"
        },
        links: ["www.esidross.lv/2013/06/18/zonealarm-antiviruss-
un-ugunsmuris/", "www.esidross.lv/2012/11/07/antiviruss-avast-
free-antivirus/"],
        suggestion_high: {
            lv: "Pārliecinies, ka izmanto labu antivīrusa
programmu, kas regulāri tiek atjaunināta. Uzlabot aizsardzību pret
vīrusiem jāveic cik vien iespējams drīz.",
            en: "Check that there is as a good antivirus program
and that it is being updated on regular basis. Protection against
viruses must be improved as soon as possible."
        },
        suggestion_medium: {
            lv: "Iespējams, ka antivīrusa programma netiek
regulāri atjaunināta, būtu ļoti vēlams uzlabot situāciju.",
            en: "Maybe antivirus program is not being updated on
regular basis - this situation should be improved."
        }
    },
    {
        rid: 1,
        checked: 2,
        text: {
            lv: "Vīrusa darbības rezultātā sabojāti vai izdzēsti
dati datorā",
            en: "Data has been corrupted because of a virus."
        },
        links: ["www.esidross.lv/2013/06/18/zonealarm-antiviruss-
un-ugunsmuris/", "www.esidross.lv/2012/11/07/antiviruss-avast-
free-antivirus/"],
        suggestion_high: {
            lv: "Pārliecinies, ka izmanto labu antivīrusa
programmu, kas regulāri tiek atjaunināta. Uzlabot aizsardzību pret
vīrusiem jāveic cik vien iespējams drīz.",
            en: "Check that there is as a good antivirus program
and that it is being updated on regular basis. Protection against
viruses must be improved as soon as possible.",
        },
        suggestion_medium: {
            lv: "Iespējams, ka antivīrusa programma netiek
regulāri atjaunināta, būtu ļoti vēlams uzlabot situāciju.",
```

```
            en: "Maybe antivirus program is not being updated on
regular basis – this situation should be improved."
        }
    },
    {
        rid: 2,
        checked: 2,
        text: {
            lv: "Dators iesaistīts botu tīklā (zombēts) ar
nezināmu mērķi (lietotājam nemanāmi)",
            en: "Computer is involved in botnet with unknown
objective"
        },
        links: ["www.esidross.lv/2013/05/10/java-un-tas-drosiba/",
"www.esidross.lv/2012/09/05/ko-laundaris-var-iegut-no-uzlauzta-
datora/", "www.esidross.lv/2011/03/29/paroles/",
"www.esidross.lv/2013/06/18/zonealarm-antiviruss-un-ugunsmuris/",
"www.esidross.lv/2012/11/07/antiviruss-avast-free-antivirus/"],
        suggestion_high: {
            lv: "Noziedznieki ne vienmēr uzreiz sabojā vai nozog
datus no zombētiem datoriem, tomēr nekad nevar zināt, kad tas
notiks. Turklāt ir iespējams, ka zombētais dators tiek iesaistīts
uzbrukumā citiem datoriem, un izmeklēšanas gaitā var rasties
problēmas tā īpašniekam. Noteikti jāpilnveido aizsardzības
programmas (antivīrusu, ugunsmūra) un jāuzstāda labākas paroles,
tas jāveic cik vien iespējams drīz.",
            en: "Criminals not always corrupt or steal data from
botnet computers, but it is not possible when that may happen. In
addition, there is a possibility that computer will be involved in
attack on other computers and that could create legal problems for
the owner. Protection programs (antivirus, firewall) must be
improved and better passwords should be used – this should be done
as soon as possible.",
        },
        suggestion_medium: {
            lv: "Noziedznieki ne vienmēr uzreiz sabojā vai nozog
datus no zombētiem datoriem, tomēr nekad nevar zināt, kad tas
notiks. Turklāt ir iespējams, ka zombētais dators tiek iesaistīts
uzbrukumā citiem datoriem, un izmeklēšanas gaitā var rasties
problēmas tā īpašniekam. Jāpārdomā un nepieciešamības gadījumā
jāpilnveido aizsardzības programmas (antivīrusu, ugunsmūra) un
jāuzstāda labākas paroles.', 'Computer is involved in botnet with
unknown goal (not visible to user).",
            en: "Criminals not always corrupt or steal data from
botnet computers, but it is not possible when that may happen. In
addition, there is a possibility that computer will be involved in
attack on other computers and that could create legal problems for
the owner. The question of improving protection programs
(antivirus, firewall) and using better passwords should be
addressed and in case of need – implemented.",
        }
    },
    {
        rid: 3,
        checked: 3,
```

```
        text: {
            lv: "Dators iesaistīts botu tīklā (zombēts), Interneta
pakalpojumu sniedzējs atslēdz piekļuvi tīklam",
            en: "Computer is involved in botnet to send spam
email, internet service provider disconnects computer from
internet"
        },
        links: ["www.esidross.lv/2012/09/05/ko-laundaris-var-
iegut-no-uzlauzta-datora/", "www.esidross.lv/2011/03/29/paroles/",
"www.esidross.lv/2013/06/18/zonealarm-antiviruss-un-ugunsmuris/",
"www.esidross.lv/2012/11/07/antiviruss-avast-free-antivirus/"],
        suggestion_high: {
            lv: "Noziedznieki ne vienmēr uzreiz sabojā vai nozog
datus no zombētiem datoriem, tomēr nekad nevar zināt, kad tas
notiks. Turklāt ir iespējams, ka zombētais dators tiek iesaistīts
uzbrukumā citiem datoriem, un izmeklēšanas gaitā var rasties
problēmas tā īpašniekam. Noteikti jāpilnveido aizsardzības
programmas (antivīrusu, ugunsmūra) un jāuzstāda labākas paroles,
tas jāveic cik vien iespējams drīz.",
            en: "Criminals not always corrupt or steal data from
botnet computers, but it is not possible when that may happen. In
addition, there is a possibility that computer will be involved in
attack on other computers and that could create legal problems for
the owner. Protection programs (antivirus, firewall) must be
improved and better passwords should be used – this should be done
as soon as possible.",
        },
        suggestion_medium: {
            lv: "Noziedznieki ne vienmēr uzreiz sabojā vai nozog
datus no zombētiem datoriem, tomēr nekad nevar zināt, kad tas
notiks. Turklāt ir iespējams, ka zombētais dators tiek iesaistīts
uzbrukumā citiem datoriem, un izmeklēšanas gaitā var rasties
problēmas tā īpašniekam. Jāpārdomā un nepieciešamības gadījumā
jāpilnveido aizsardzības programmas (antivīrusu, ugunsmūra) un
jāuzstāda labākas paroles.",
            en: "Criminals not always corrupt or steal data from
botnet computers, but it is not possible when that may happen. In
addition, there is a possibility that computer will be involved in
attack on other computers and that could create legal problems for
the owner. The question of improving protection programs
(antivirus, firewall) and using better passwords should be
addressed and in case of need – implemented."
        }
    },
    {
        rid: 4,
        checked: 3,
        text: {
            lv: "Datora tehnisku bojājumu, t.sk. diska bojājuma
dēļ, dati ir zuduši",
            en: "Because of damaged computer, including damaged
hard drive, data has been lost"
        },
```

```
        links: ["www.esidross.lv/2013/11/15/informacija-glabasana-
un-sinhronizacija-bezmaksas-kratuve-makoni/",
"www.esidross.lv/2012/11/12/backup-jeb-datu-rezerves-kopijas/"],
        suggestion_high: {
            lv: "Vislabākais līdzeklis pret datu zaudēšanu
tehnisku problēmu dēļ ir savlaicīga un regulāra rezerves kopiju
veidošana. Izveido savu risinājumu, un sāc veidot rezerves
kopijas. Var izmantot gan CD, gan USB atmiņas kartes, gan citus
risinājumus.",
            en: "The best tool to prevent data loss because of
computer technical problems is timely and on regular basis created
data backups. Create your solution to this problem and start
creating backups. Optical discs, USB flash memory and other
storage solutions can be used for backup purposes.",
        },
        suggestion_medium: {
            lv: "Vislabākais līdzeklis pret datu zaudēšanu
tehnisku problēmu dēļ ir savlaicīga un regulāra rezerves kopiju
veidošana. Tomēr privātā vidē ir iespējams uz datu (piemēram,
fotogrāfiju kolekcija) zaudējumu raudzīties filozofiski, un
pieņemt, ja pazudīs, tad nekas. Tomēr, ja glabājamie dati ir ar
ilgtermiņa nozīmi, padomā par rezerves kopijām.",
            en: "The best tool to prevent data loss because of
computer technical problems is timely and on regular basis created
data backups. For private purposes there is a way to look
philosophically at data (for example photo collection) loss and
think that this is not the end of the world."
        }
    },
    {
        rid: 5,
        checked: 2,
        text: {
            lv: "Pazaudējot USB atmiņas karti vai telefonu,
zaudēti dati",
            en: "Data has been lost because of lost mobile phone
or flash drive"
        },
        links: ["www.esidross.lv/2013/11/15/informacija-glabasana-
un-sinhronizacija-bezmaksas-kratuve-makoni/"],
        suggestion_high: {
            lv: "Jāizvērtē, kādi dati tiek glabāti USB atmiņas
kartē. Ja tie ir tikai daži faili, kam ir oriģināli datorā, kā arī
neuztrauc datu nokļūšana pie svešiem, tad var pieņemt nelielas
materiālas vērtības zudumu. Ja USB atmiņā tiek glabāti slēpjami
dati, tad vajadzētu tos šifrēt. Šī riska augstais līmenis liecina,
ka jāpārdomā, kā uzlabot datu drošību USB atmiņā.",
            en: "It should be evaluated what data is stored on USB
flash drive. If those are only few files, which are copies of
original files on computer, and it is not a concern if those files
become accessible by unknown people, then it can be accepted as a
small loss of material value. If flash drive contains secret data,
then it should be encrypted. The highest level of this risk shows
that flash drive security should be improved.",
        },
```

```
        suggestion_medium: {
            lv: "Jāizvērtē, kādi dati tiek glabāti USB atmiņas
kartē. Ja tie ir tikai daži faili, kam ir oriģināli datorā, kā arī
neuztrauc datu nokļūšana pie svešiem, tad var pieņemt nelielas
materiālas vērtības zudumu. Ja USB atmiņā tiek glabāti slēpjami
dati, tad vajadzētu tos šifrēt. Privātā vidē ir iespējams uz datu
zaudējumu raudzīties filozofiski, un pieņemt, ja pazudīs, tad
nekas.",
            en: "It should be evaluated what data is stored on USB
flash drive. If those are only few files, which are copies of
original files on computer, and it is not a concern if those files
become accessible by unknown people, then it can be accepted as a
small loss of material value. If flash drive contains secret data,
then it should be encrypted. For private purposes there is a way
to look philosophically at data loss and think that this is not
the end of the world."
        }
    },
    {
        rid: 6,
        checked: 3,
        text: {
            lv: "Neapdomīgi publiskota vai sliktajiem nodota
informācija tiek izmantota, lai izkrāptu vai nozagtu naudu",
            en: "Lightmindedly published information is used to
cheat out money"
        },
        links: ["www.esidross.lv/2013/04/10/kapec-sociala-
inzenierija-ir-efektiva/", "www.esidross.lv/2014/01/22/visa-dzive-
interneta-spoguli-2/", "www.esidross.lv/2013/07/16/berna-
izglitosana-datora-lietosana/",
"www.esidross.lv/2012/04/28/popularakie-krapsanas-veidi-
interneta/"],
        suggestion_high: {
            lv: "Nevienas darbības Internetā nav anonīmas un pēdas
paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki
publisko informāciju, \"parakstot\" to ar savu vārdu. Ir iespējams
izmantot informāciju, ko pats esi publicējis, piemēram, par
ieradumiem, hobijiem vtml., lai iegūtu uzticību un izkrāptu naudu.
Ir vērts atcerēties parunu \"septiņreiz nomēri pirms nogriez\" arī
attiecībā uz informācijas publicēšanu Internetā (sociālajos
tīklos). Ja labprāt publisko daudz informācijas, uzmanies no
nepazīstamiem saziņas partneriem, kas daudz zina par Tevi.
Iespējams, ka būtu vērts izdzēst kaut daļu informācijas, lai tā
nebūtu tik ērti pieejama.",
            en: "Actions on the internet are not anonymous and
trace is left even for deleted information, but more and more
commonly information, which is “signed” with one’s name, is
published. It is possible to use information, which you are
published, for example, about your habits, \r\nhobbies etc., to
gain trust and cheat out money. It is useful to remember the
saying – “Measure seven times and cut one” in the context of
publishing information on the internet (social sites). If you
willingly publish a lot of information, watch out of unknown
communication partners, who know a lot about you. Maybe it could
```

be a good idea to delete some information, to make in less easy to obtain.",
        },
        suggestion_medium: {
            lv: "Nevienas darbības Internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, \"parakstot\" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par ieradumiem, hobijiem vtml., lai iegūtu uzticību un izkrāptu naudu. Ir vērts atcerēties parunu \"septiņreiz nomēri pirms nogriez\" arī attiecībā uz informācijas publicēšanu Internetā (sociālajos tīklos). Ja labprāt publisko daudz informācijas, uzmanies no nepazīstamiem saziņas partneriem, kas daudz zina par Tevi.",
            en: "Actions on the internet are not anonymous and trace is left even for deleted information, but more and more commonly information, which is “signed” with one’s name, is published. It is possible to use information, which you are published, for example, about your habits, hobbies etc., to gain trust and cheat out money. It is useful to remember the saying – “Measure seven times and cut one” in the context of publishing information on the internet (social sites). If you willingly publish a lot of information, watch out of unknown communication partners, who know a lot about you."
        }
    },
    {
        rid: 7,
        checked: 2,
        text: {
            lv: "Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā vai radusies cita nepatīkama situācija",
            en: "Job opportunity is denied because of lightmindedly published information or other unpleasant situation"
        },
        links: ["www.esidross.lv/2013/04/10/kapec-sociala-inzenierija-ir-efektiva/", "www.esidross.lv/2014/01/22/visa-dzive-interneta-spoguli-2/", "www.esidross.lv/2013/07/16/berna-izglitosana-datora-lietosana/", "www.esidross.lv/2012/04/28/popularakie-krapsanas-veidi-interneta/"],
        suggestion_high: {
            lv: "Nevienas darbības Internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, \"parakstot\" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par trakulīgām ballītēm, ne īpaši labiem ieradumiem vtml., lai veidotu priekšstatu. Ir vērts atcerēties parunu \"septiņreiz nomēri pirms nogriez\" arī attiecībā uz informācijas publicēšanu Internetā (sociālajos tīklos). Iespējams, ka būtu vērts izdzēst kaut daļu informācijas, lai tā nebūtu tik ērti pieejama.",
            en: "Actions on the internet are not anonymous and trace is left even for deleted information, but more and more commonly information, which is \"signed\" with one’s name, is published. It is possible to use information, which you are published, for example, about some crazy party or bad habits etc.,

to make an impression. It is useful to remember the saying – \"Measure seven times and cut one\" in the context of publishing information on the internet (social sites). Maybe it could be a good idea to delete some information, to make in less easy to obtain.",
        },
        suggestion_medium: {
            lv: "Nevienas darbības Internetā nav anonīmas un pēdas paliek arī izdzēstai informācijai, bet aizvien biežāk cilvēki publisko informāciju, \"parakstot\" to ar savu vārdu. Ir iespējams izmantot informāciju, ko pats esi publicējis, piemēram, par trakulīgām ballītēm, ne īpaši labiem ieradumiem vtml., lai veidotu priekšstatu. Ir vērts atcerēties parunu \"septiņreiz nomēri pirms nogriez\" arī attiecībā uz informācijas publicēšanu Internetā (sociālajos tīklos).",
            en: "Actions on the internet are not anonymous and trace is left even for deleted information, but more and more commonly information, which is \"signed\" with one's name, is published. It is possible to use information, which you are published, for example, about some crazy party or bad habits etc., to make an impression. It is useful to remember the saying – \"Measure seven times and cut one\" in the context of publishing information on the internet (social sites)."
        }
    },
    {
        rid: 8,
        checked: 3,
        text: {
            lv: "Pārāk vienkāršas paroles dēļ, kāds iekļuvis internetbankas kontā un nozadzis naudu",
            en: "Because of weak a password someone broke in your bank account and stole money"
        },
        links: ["www.esidross.lv/2012/06/29/ka-drosi-iepirkties-tiessaiste/", "www.esidross.lv/2012/10/15/parolu-nebusanas-jeb-nomaini-savu-paroli-tagad/", "www.esidross.lv/2011/03/29/paroles/"],
        suggestion_high: {
            lv: "Parolei jābūt pietiekami sarežģītai (vismaz 8 simboli, bet labāk vairāk, lielie un mazie burti, speciālie simboli, cipari utt.). Ja paroli grūti atcerēties, mājās tā var tikt arī pierakstīta un glabāta kādā sev vien zināmā drošā vietā (\"zem spilvena\"), rūpējies, lai tā nebūtu pieejama kopā ar lietotāja vārdu. Ja esi lietojis paroli nedrošā vietā (Interneta kafejnīcā vtml.), labāk to nomaini.",
            en: "Password must be complicated enough (at least 8 symbols (but more is better), uppercase and lowercase letter, special symbols, number etc.). If password is hard to remember, it can be stored home in a secret place (\"under the pillow\"), but make sure that it is not accessible with username. If you used password in unsafe environment (Internet café for example) you should change the password.",
        },
        suggestion_medium: {

```
            lv: "Parolei jābūt pietiekami sarežģītai (vismaz 8
simboli, bet labāk vairāk, lielie un mazie burti, speciālie
simboli, cipari utt.). Ja paroli grūti atcerēties, mājās tā var
tikt arī pierakstīta un glabāta kādā sev vien zināmā drošā vietā
(\"zem spilvena\"), rūpējies, lai tā nebūtu pieejama kopā ar
lietotāja vārdu.",
            en: "Password must be complicated enough (at least 8
symbols (but more is better), uppercase and lowercase letter,
special symbols, number etc.). If password is hard to remember, it
can be stored home in a secret place (\"under the pillow\"), but
make sure that it is not accessible with username."
        }
    },
    {
        rid: 9,
        checked: 2,
        text: {
            lv: "Pārāk vienkāršas paroles dēļ, sociālā tīkla
profilā vai e-pastā kāds darbojies saimnieka vietā",
            en: "Because of a weak password someone is using
owner's email or social profile"
        },
        links: ["www.esidross.lv/2012/06/29/ka-drosi-iepirkties-
tiessaiste/", "www.esidross.lv/2012/10/15/parolu-nebusanas-jeb-
nomaini-savu-paroli-tagad/",
"www.esidross.lv/2011/03/29/paroles/"],
        suggestion_high: {
            lv: "Parolei jābūt pietiekami sarežģītai (vismaz 8
simboli, bet labāk vairāk, lielie un mazie burti, speciālie
simboli, cipari utt.). Ja paroli grūti atcerēties, mājās tā var
tikt arī pierakstīta un glabāta kādā sev vien zināmā drošā vietā
(\"zem spilvena\"), rūpējies, lai tā nebūtu pieejama kopā ar
lietotāja vārdu. Ja esi lietojis paroli nedrošā vietā (Interneta
kafejnīcā vtml.), labāk to nomaini.",
            en: "Password must be complicated enough (at least 8
symbols (but more is better), uppercase and lowercase letter,
special symbols, number etc.). If password is hard to remember, it
can be stored home in a secret place (“under the pillow”), but
make sure that it is not accessible with username. If you used
password in unsafe environment (Internet café for example) you
should change the password.",
        },
        suggestion_medium: {
            lv: "Parolei jābūt pietiekami sarežģītai (vismaz 8
simboli, bet labāk vairāk, lielie un mazie burti, speciālie
simboli, cipari utt.). Ja paroli grūti atcerēties, mājās tā var
tikt arī pierakstīta un glabāta kādā sev vien zināmā drošā vietā
(\"zem spilvena\"), rūpējies, lai tā nebūtu pieejama kopā ar
lietotāja vārdu.",
            en: "'Password must be complicated enough (at least 8
symbols (but more is better), uppercase and lowercase letter,
special symbols, number etc.). If password is hard to remember, it
can be stored home in a secret place (“under the pillow”), but
make sure that it is not accessible with username."
        }
```

```
    },
    {
        rid: 10,
        checked: 2,
        text: {
            lv: "Svešais izmanto bezvadu tīklu sliktiem mērķiem",
            en: "Someone is using wireless network for bad
purposes"
        },
        links: ["www.esidross.lv/2012/08/29/drosa-majas-bezvadu-
tikla-konfiguracija/", "www.esidross.lv/2012/05/31/ka-lietot-
bezvadu-internetu-majas/", "www.esidross.lv/2012/05/31/ka-lietot-
bezvadu-internetu-publiskas-vietas/"],
        suggestion_high: {
            lv: "Bezvadu tīkla maršrutētājam nekavējoties noteikti
jāuzstāda pietiekami droša parole.",
            en: "Wireless router password must be immediately set
to a stronger password.",
        },
        suggestion_medium: {
            lv: "Bezvadu tīkla maršrutētājam noteikti jāuzstāda
pietiekami droša parole. To var nedarīt, ja dzīvo meža vidū, kur
sveši neieklīst :)",
            en: "Wireless router password must be immediately set
to a stronger password. It is not as critical, if you live in the
middle of a forest, where strangers don’t enter :)"
        }
    }
];

systemdata.ui = {
    'sysname': {
        lv: "Informācijas Drošības Risku Eksperts",
        en: "Information Security Risk Expert"
    },
    'descr1': {
        lv: "Datoru drošība nereti tiek uzskatīta par tikai
atbilstošās jomas speciālistiem saprotamu un svarīgu tēmu. Tomēr
par informācijas un datora drošību ir iespējams un nepieciešams
rūpēties katram pašam.",
        en: "Computer security pretty often is considered as fully
understood and an important topic only by security specialists.
However it is possible and essential to think about security of
your computers and digital information."
    },
    'descr2': {
        lv: "Atbildi uz jautājumiem par datora lietošanas
paradumiem un noskaidro sev būtiskākos riskus, kas ar tiem
saistīti. Ja Tavu datoru izmanto vairāki lietotāji vai Tu pats
lieto vairākus datorus, tad jautājumi jāatbild katram un par katru
datoru atsevišķi. Noslēgumā saņemsi ieteikumus, ko varētu vai
vajadzētu darīt, ja šobrīd īstenotie drošības pasākumi neatbilst
Tavām vēlmēm būt pasargātam elektroniskā vidē.",
        en: "Answer questions about your computer usage and
evaluate the most crucial risks, which are asociated with your
```

```
habits. If your computer is shared with other people or you use
several computers, then questions should be answered by everybody
and about every computer in distinct. In the end You will receive
recomendations which you should or must take into account if your
current security policy does not fulfil your expectations of
secure electronic environment."
    },
    'start': {
        lv: "Sākt aptauju",
        en: "Start inquiry"
    },
    'changelang': {
        lv: "English",
        en: "Latviski"
    },
    'continue': {
        lv: "Turpināt",
        en: "Continue"
    },
    'back': {
        lv: "Atpakaļ",
        en: "Back"
    },
    'riskpage1': {
        lv: "Iedomājies, ka zemāk minētie notikumi būtu notikuši.
Novērtē cik svarīga Tev ir to negatīvā ietekme:",
        en: "Imagine that events mentioned below really happened.
Rank how important is its negative implications:"
    },
    'riskpage2': {
        lv: "1 - nemaz neuztrauc, 2 - gan jau pārdzīvošu, 3 -
būtiska negatīva ietekme",
        en: "1 - doesn't bother, 2 - I'll get over it, 3 -
substantial negative impact"
    },
    'riskpage3': {
        lv: "Speciālisti ir novērtējuši riskus, sniedzot
ieteikumu, taču droši maini riska novērtējumu, ja Tava attieksme
ir citāda.",
        en: "Experts have rated these risks, giving advises, but
change the rating if you feel differently."
    },
    'highrisks': {
        lv: "Tu esi pakļauts šādiem riskiem ar šādu riska ietekmi
(9 maks.):",
        en: "You are affected by these risks with these
implications (9 max):"
    },
    'lowrisks': {
        lv: "Tu esi minimāli pakļauts šādiem riskiem, taču to
ietekme ir zema un papildus darbības no Tavas puses nav
nepieciešamas:",
        en: "You are affected by the following risks, but their
possible implications ar less likely and additional actions are
not necessary:"
```

```
    },
    'advice': {
        lv: "Ieteikums:",
        en: "Advice:"
    },
    'backtostart': {
        lv: "Uz sākumu",
        en: "Back to start"
    },
    'feedback': {
        lv: "Atstāt atsauksmi",
        en: "Leave feedback"
    },
    'send': {
        lv: "Nosūtīt",
        en: "Send"
    },
    'thanks': {
        lv: "Paldies!",
        en: "Thank you!"
    },
    'readmore': {
        lv: "Vairāk lasi: ",
        en: "Read more (in latvian): "
    }
};
```

6. Rīka IDRE lietotāju aptaujas anketas jautājumi

Kā saņemt padomu par drošību elektroniskā vidē

Aptaujas mērķis ir novērtēt iespaidus par informācijas drošības risku novērtēšanas rīka paraugu un gūt idejas tā tālākai attīstībai. Atbildes prasa tikai dažas minūtes Tava laika.

1. Tavs vecums?

- ☐ 15 gadi vai mazāk
- ☐ 16-23
- ☐ 24-45
- ☐ 46-65
- ☐ 66 gadi vai vairāk

2. Kāds ir Tavs IT lietotāja pieredzes līmenis?

- ☐ Esmu šo jomu mācījies un strādāju kā IT speciālists
- ☐ Datoru lietoju ikdienā darba vietā, ir pieejamas datora lietošanas apmācības
- ☐ Datoru lietoju ikdienā darba vietā, jaunas prasmes apgūstu pats
- ☐ Datoru lietoju vismaz pāris reizes nedēļā, pārsvarā personīgām vajadzībām
- ☐ Datoru lietoju retāk nekā reizi nedēļā

3. Kur Tu visbiežāk meklē padomu, ja saskaries ar problēmu personīgā datora darbībā vai jautājumos par rīcību ar personīgo elektronisko informāciju?

- ☐ Nekur, – pats visu saprotu
- ☐ Datoru remonta darbnīcā
- ☐ Prasu padomu draugiem
- ☐ Meklēju padomu specializētās Interneta vietnēs
- ☐ Man ir savs uzticams datorspeciālists

☐ Interneta sarunu forumos

☐ Tā ir problēma, īsti nezinu, kam varētu uzticēties

☐ Cits ____

4. Kas ir kritēriji, lai Tu uzticētos Interneta mājas lapas sniegtajai informācijai? (vairākas atbildes iespējamas)

☐ Uzticos savai intuīcijai

☐ Draugu ieteikumi

☐ Zināmas datoru kompānijas mājas lapa

☐ Valsts iestādes mājas lapa

☐ Atzītas nevalstiskas organizācijas, asociācijas mājas lapa

☐ Reklāma iecienītā Interneta portālā

☐ Cits ____

5. Vai informācijas drošības risku novērtēšanas rīks lika aizdomāties par savas elektroniskās informācijas drošību?

☐ Mani neuztrauc manas elektroniskās informācijas drošība, un nekas neliks man savas domas mainīt

☐ Sniegtie padomi ir interesanti, bet ne īpaši noderīgi

☐ Balstoties uz ieteikumiem, mēģināšu pārskatīt savus datora lietošanas paradumus

☐ Priecājos, ka mani datora lietošanas paradumi nerada lielus riskus manas informācijas drošībai

☐ Cits ____

6. Vai risku novērtēšanas rīks palīdzēs veikt sava datora aizsardzības pilnveidi?

☐ Kaut rīks uzrāda lielus riskus, kamēr dators strādā tā, kā man nepieciešams, neredzu vajadzību kaut ko papildus darīt

☐ Kaut kas ir jādara ar manu datoru, meklēšu tālāku padomu pie speciālistiem

☐ Dažus pasākumus veikt ir pavisam vienkārši, to drīzumā darīšu

☐ Priecājos, ka mana datora aizsardzības līmenis ir pietiekami labs

☐ Cits

7. Kāds jautājums Tev pietrūka Informācijas drošības risku novērtēšanas rīkā?