Informācijas drošības apzināšanās sistēma ikdienas datorlietotājam

Ilze Murāne

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

zinātniskais vadītājs
prof. Juris Borzovs

ESF
EIROPAS SOCIĀLAIS FONDS
EIROPAS SAVIENĪBA
IEGULDĪJUMS TAVĀ NĀKOTNĒ
LATVIJAS UNIVERSITĀTE
ANNO 1919

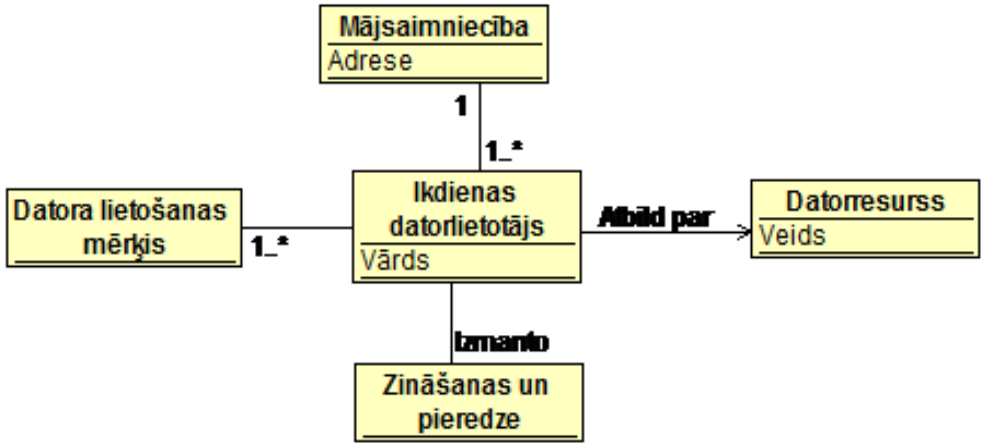
Tēmas aktualitāte un novitāte

- Tehnoloģiju progress (katra cilvēka dzīvē, ikdienā, mājās)
- Apdraudējumi (privātā vidē tie paši, kas citur)
- Cilvēkiem nav pieredzes elektroniskas informācijas aizsardzībā
- Grūtības saprasties tehnoloģiju speciālistiem un tehnoloģiju lietotājiem
- Drošību nepieciešams pārvaldīt nepārtraukti un sistemātiski

LATVIJAS UNIVERSITATE
ANNO 1919
UNIVERSITY OF LATVIA

Ikdienas datorlietotājs

- Persona, kas savā ikdienā, privātām vajadzībām
  - izmanto datoru vai planšeti un interneta iespējas
  - nav formālas izglītības vai ilgstošas pieredzes IT vai līdzīgā jomā
  - pats ir pilnībā atbildīgs par izmantojamo datoru vai planšeti un rīcību ar to



LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

Mērķis

- Izstrādāt pieeju, kā veicināt informācijas drošības apzināšanos privātā vidē
- Izstrādāt informācijas drošības risku novērtēšanas metodi un sistēmas prototipu (rīku), kas
  - palīdz uzņemties atbildību un īstenot drošības pārvaldību
  - sniedz praktiskus padomus, kas pielāgoti konkrēta ikdienas datorlietotāja vajadzībām

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

Uzdevumi (metodes)

- 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
- 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)

Informācijas (sistēmu) drošība

- Informācijas konfidencialitātes, integritātes un pieejamības saglabāšana
- Definīcijas pamatā vērstas uz biznesa informācijas drošību
- Privātums
  - Sākotnēji lielā mērā saistīts ar cilvēktiesībām
  - Fizisko personu datu aizsardzība
  - Lai izmantotu informācijas tehnoloģiju sniegtās ērtības, daļa privātuma ir jāziedo

Informācijas drošības apzināšanās

- Drošības apzināšanās veicināšanas mērķis ir veidot spēju intuitīvi rīkoties atbilstoši situācijai
- Būtiska sastāvdaļa organizācijas informācijas drošības programmā
- Informācijas drošības apzināšanās labās prakses attīstība
  - Starptautisku organizāciju vadlīnijas (OECD, ENISA, Microsoft)
  - Projekti Latvijā (Drošs internets, esidross.lv, bankas)
- Daudzveidīgi materiāli par katru apdraudējumu un risinājumu atsevišķi

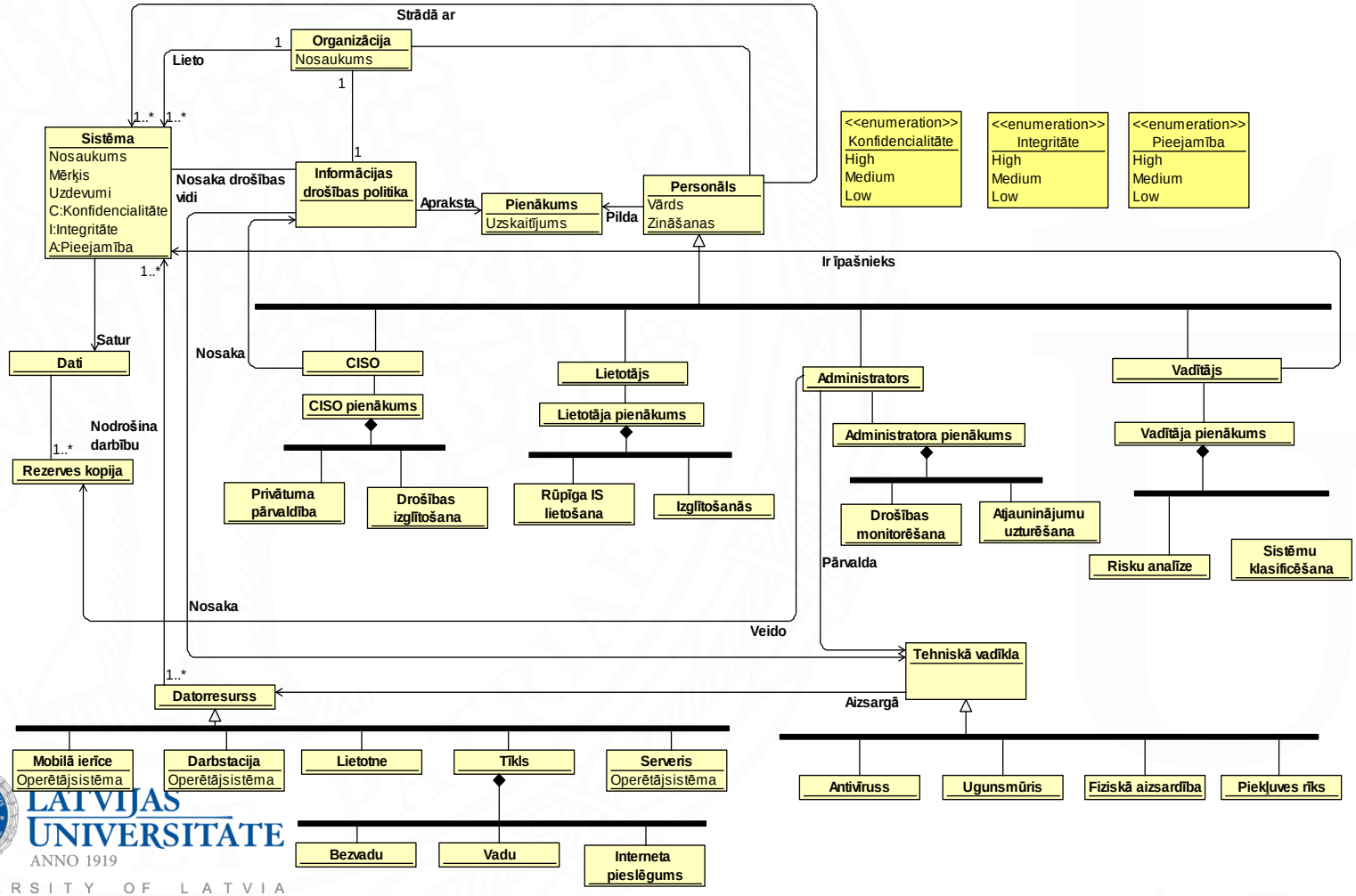
Citi pētījumi

- "Mūsdienās nozīmīga daļa datoruzbrukumu vairāk saistīta ar psiholoģisku metožu izmantošanu, tehnoloģijām atstājot tikai papildus rīka statusu" "R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems"
- "Starp riskiem, ko cilvēki nepietiekami novērtē, ir arī datora un elektroniskas informācijas izmantošanas riski" "B. Schneier, The Psychology of Security"
- "Efektīvi drošības risinājumi nav atkarīgi tikai no to matemātiskām un tehniskām īpašībām, bet arī no cilvēku spējām tos saprast un izmantot" "P. Dourish et al., Security in the wild: user strategies for managing security as an everyday, practical problem"
- "Konstatēta saistība starp pētījuma dalībnieku drošības uzvedību un drošības apzināšanās līmeni" "Grant, Gordon J., Ascertaining the relationship between security awareness and the security behavior of individuals"

Informācijas drošības standarti

- LVS ISO/IEC 27002:2013 “Informācijas tehnoloģija. Drošības metodika. Prakses kodekss informācijas drošības pārvaldībai”
- *ISF Standard of Good Practice for Information Security*
- *The Control Objectives for Information and related Technology*
  - Drošības pamatnostādnes (*Security Baseline*)
- Piekļuves vadības, konfidencialitātes un integritātes modeļi

Tradicionāls informācijas drošības pārvaldības modelis

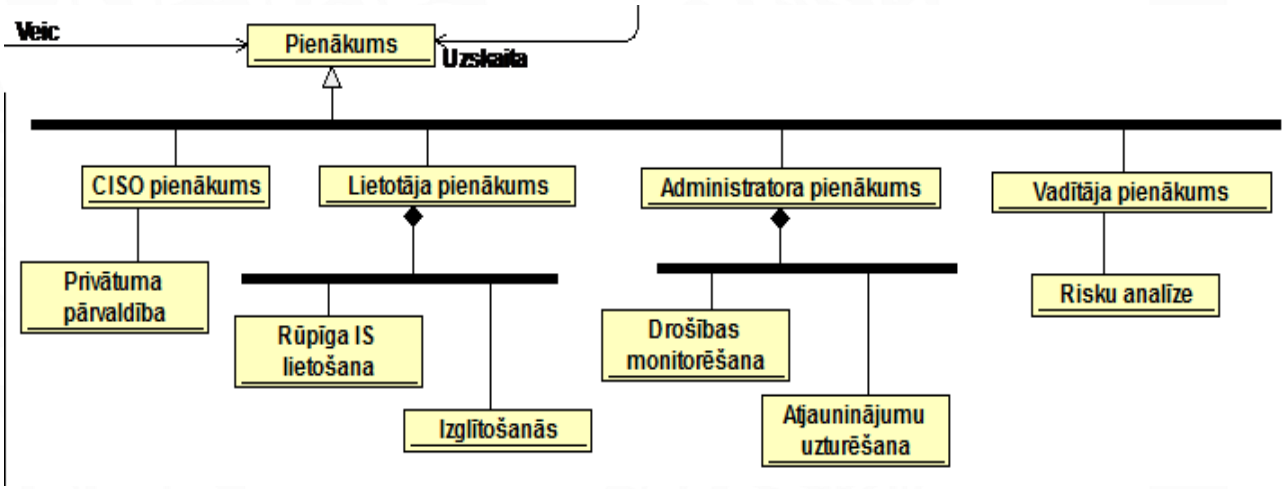


LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

Informācijas tehnoloģiju pielietojums mājsaimniecībā

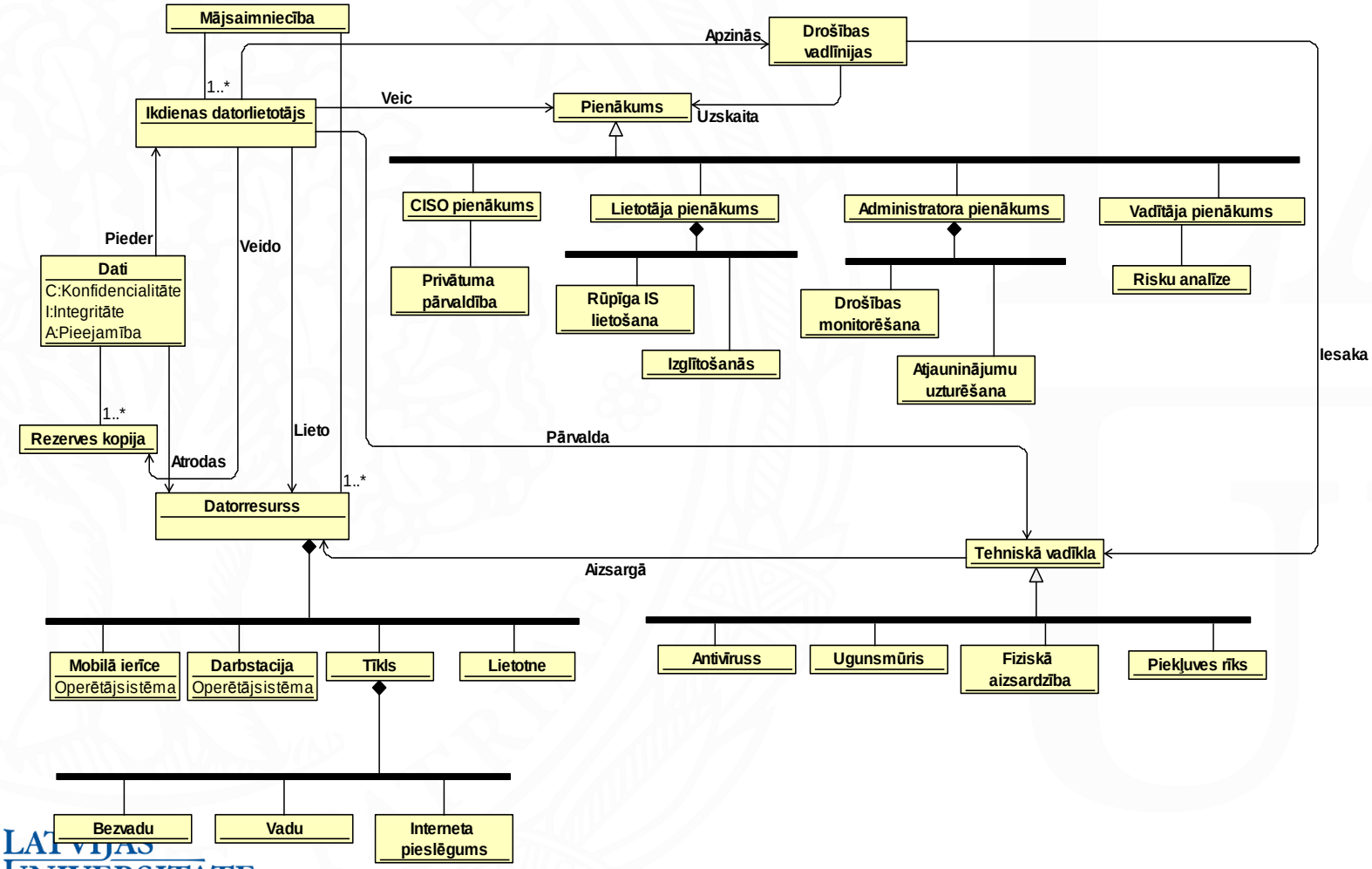
- Mājsaimniecībās pieejamas jaunākās tehnoloģijas (3. ātrākais internets pasaulē)
- Vairāk nekā 90% mājsaimniecību, kurās ir bērni, lieto internetu (2014)
- Lietošanas mērķi (2014)
  - e-pasta sūtīšana
  - informācijas iegūšana
  - internetbanka
  - paša izveidota satura augšupielādēšana
- Sociālie tīkli
- Dators = fotoalbums
- Apdraudējumi

Ikdienas datorlietotāja pienākumi



LATVIJAS UNIVERSITATE
ANNO 1919
UNIVERSITY OF LATVIA

Mājsaimniecības modelis



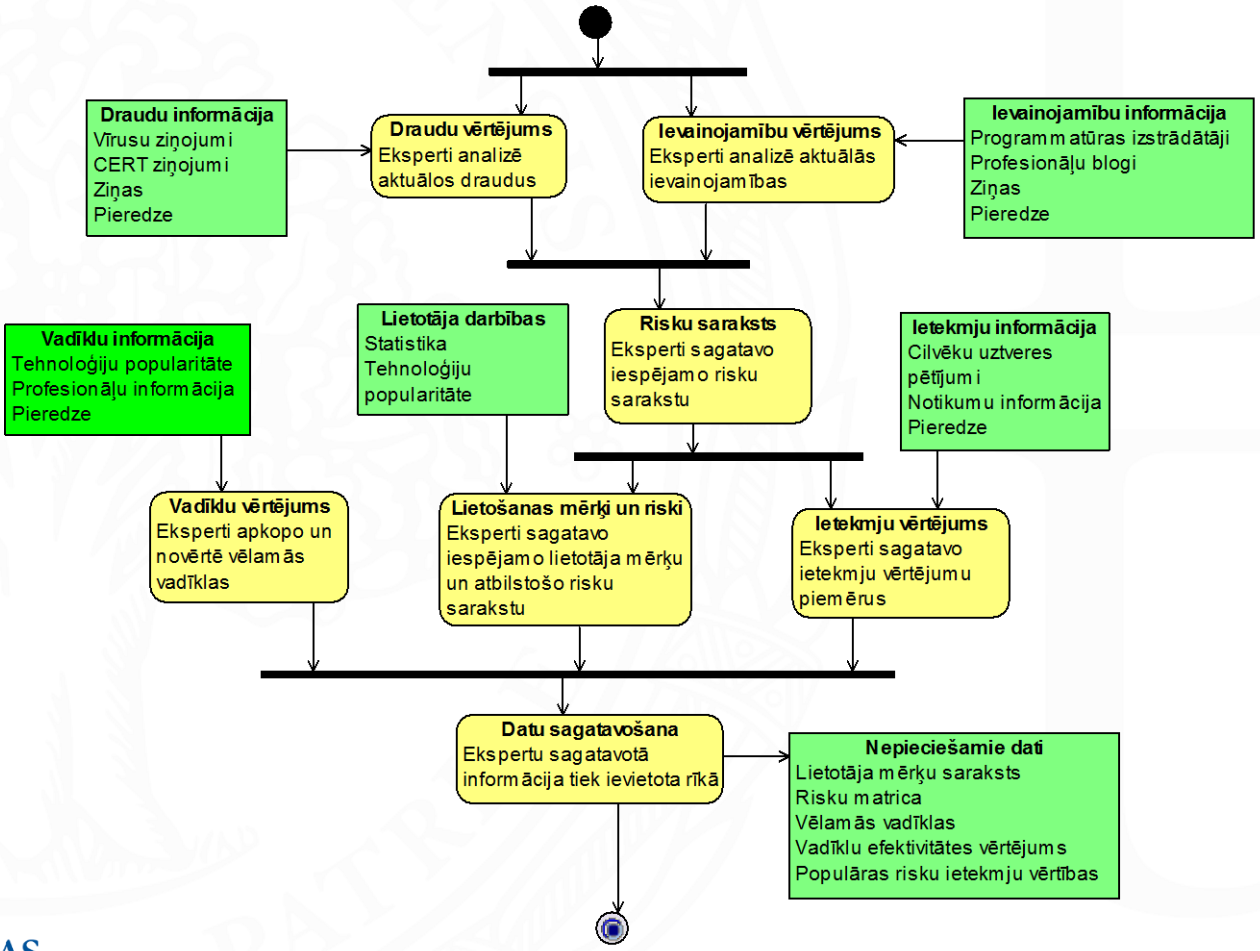
Informācijas drošības vadlīnijas mājsaimniecībā

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
SM3.1 Informācijas klasificēšana	Strukturēti visām sistēmām	Izpratne, kas ir svarīgi
SM3.3 Informācijas riska analīzes process	Strukturēti visām sistēmām	Vienkāršs
SM4.2 Informācijas privātums	Atbilstība tiesību aktiem	Drošības mērķis
SM5.2 Ļaunprogrammatūras aizsardzības programmatūra	Vairākas dažādiem mērķiem	Vienkārša, bet noteikti nepieciešama

Riska novērtēšanas metode

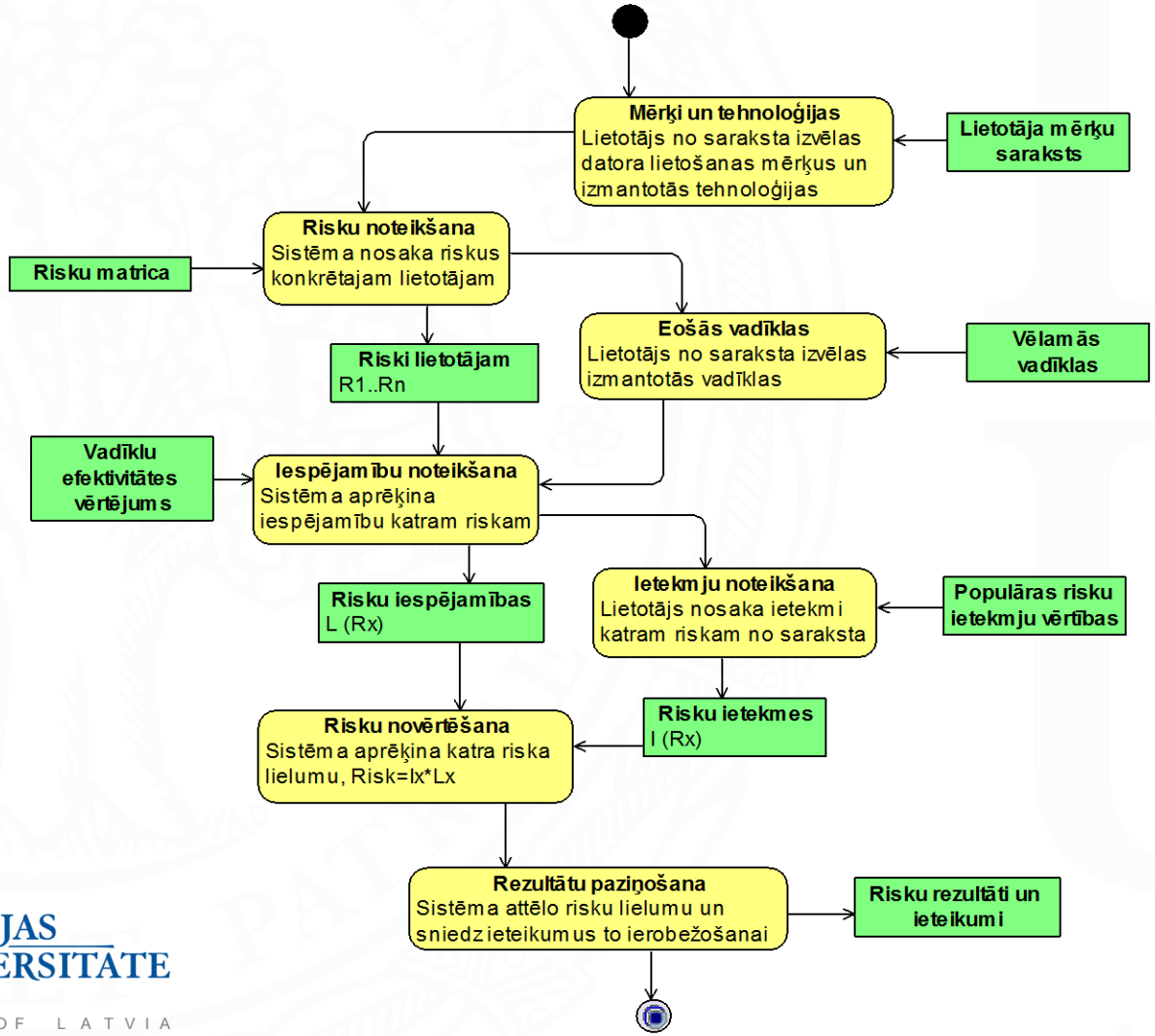
- NIST Ceļvedis informācijas tehnoloģiju sistēmu risku pārvaldīšanai
- Pielāgota lietošanai mājsaimniecībā
  - lietojama jebkuram datorlietotājam neatkarīgi no zināšanu līmeņa tehnoloģijās
  - lietojama interneta vidē
  - jautājumi ar atbilžu variantu izvēli
- Izmantoto datu kopums papildināms, attīstoties tehnoloģiju ierīču un apdraudējumu klāstam
  - speciālistu analītisks darbs

Ekspertu informācijas sagatavošana



LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

Metodes pielietošanas soļi



LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

Rīks IDRE

Informācijas Drošības Risku Eksperts

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, uT
- ☐ Internetbankas izmantošana, t.sk. rēķinu apmaksa citos portālos
- ☐ Iepirkšanās Internetā, t.sk. ceļojuma naktsmītņu rezervēšana, norādot maksājum
- ☐ Paša izveidota satura (t.sk. fotogrāfiju) augšupielādēšana jebkurā tīmekļa vietnē facebook.com)
- ☐ Fotogrāfiju/video failu glabāšana un apstrāde savā datorā
- ☐ Dokumentu rakstīš
- ☐ Mūzikas klausīšan

Kāda operētājsistēm

- ○ Windows (Vista, 7
- ○ Windows XP
- ○ OS X (Apple dator
- ○ Linux (piem. Ubun
- ○ iOS (Apple iPhone
- ○ Android

Vai programmatūra tiek regulāri atjaunota?

- ○ Programmatūras atjauninājumi pēc regulāras procedūr
- ○ 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

9 **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/

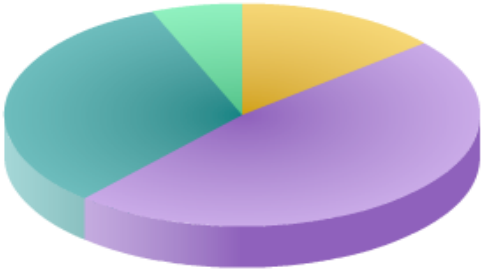
6 **Neapdomīgi publicētas informācijas dēļ, atteikts pieņemt darbā vai radusies cita nepatīkama situācija**

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/

LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

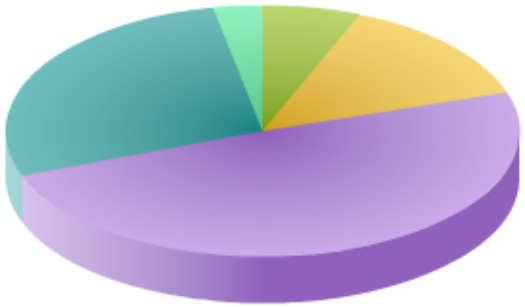
Rīka IDRE novērtējums

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 (0%)
- Sniegtie padomi ir interesanti, bet ne īpaši noderīgi (13.9%)
- Balstoties uz ieteikumiem, mēģināšu pārskatīt savus datora lietošanas paradumus (47.7%)
- Priecājos, ka mani datora lietošanas paradumi nerada lielus riskus manas informācijas drošībai (32.4%)
- Cits (6.2%)

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 (6.2%)
- Kaut kas ir jādara ar manu datoru, meklēšu tālāku padomu pie speciālistiem (13.9%)
- Dažus pasākumus veikt ir pavisam vienkārši, to drīzumā darīšu (49.3%)
- Priecājos, ka mana datora aizsardzības līmenis ir pietiekami labs (27.7%)
- Cits (3.1%)

LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

Riska novērtēšanas metodes uzturēšana

esi drošs

Mēs atbildam par savu drošību informācijas tehnoloģiju laikmetā

Mek

Mājās | Darbā | Publiskās vietās | Ieteikumi | Par drošību | Bezmaksas risinājumi | Pasākumi | Notikumi pasaulē

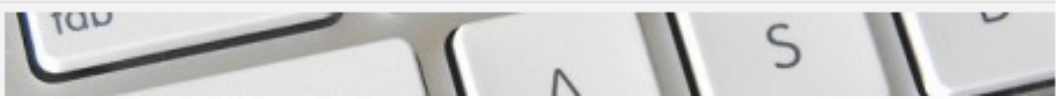
Tēmas

- Ap un par drošību (86)
- Bezmaksas risinājumi (16)
- Darbā (27)
- Datora drošība (9)
- Datorologs (2)
- Ieteikumu lāde (66)

Izaicini savu drošības sajūtu

AUTORS: **ILZE MURĀNE** 2015. gada 18. septembris

SADAĻAS: IETEIKUMU LĀDE, MĀJĀS, NOVĒRTĒ RISKUS, PĀRBAUDE



LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

Galvenie secinājumi

- 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

Darba rezultāts

- Jauna pieeja ikdienas datorlietotāja elektroniskās informācijas drošības apzināšanās veicināšanai un pārvaldībai, kas sastāv no
  - informācijas drošības pārvaldības modeļa un vadlīnijām mājsaimniecībai
  - informācijas drošības risku novērtēšanas metodes, kas aprobēta kā tīmekļa lietojumprogrammas prototips (rīks)
- Darbam ir gan teorētiska, gan praktiska nozīme
- Darba novitāte ir risku novērtēšanas metodes pielietošana ikdienas datorlietotāja informācijas drošības pārvaldībai
- Promocijas darba izstrādes gaitā izvirzītās tēzes apstiprinātas

LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

Konferences

- 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
- *Panel on capabilities building and education in National Cyber Security Strategies, 2nd ENISA National Cyber Security Strategies workshop, Riga, May 13, 2015*

LATVIJAS UNIVERSITATE
ANNO 1919
UNIVERSITY OF LATVIA

Publikācijas

- (*) 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.
- 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.
- 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.
- (*) (**) 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.
- 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.

(*) - SCOPUS, (**) - Web of Science

LATVIJAS UNIVERSITATE
ANNO 1919
UNIVERSITY OF LATVIA

Rezultātu nozīmība Latvijā

- Nacionālās drošības koncepcija un Latvijas kiberdrošības stratēģija 2014.–2018. gadam nosaka nepieciešamību izglītot lietotājus
- Papildinājums CERT.LV uzturētam izglītojošam portālam esidross.lv

LATVIJAS UNIVERSITĀTE
ANNO 1919
UNIVERSITY OF LATVIA

Paldies!

LATVIJAS UNIVERSITATE
ANNO 1919
UNIVERSITY OF LATVIA